►**B**

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 juin 2024

établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

(Texte présentant de l'intérêt pour l'EEE)

(JO L 1689 du 12.7.2024, p. 1)

Rectifié par:

►**C1** Rectificatif, JO L 90802 du 9.10.2025, p. 1 (2024/1689)

▼B

RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 13 juin 2024

établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle)

(Texte présentant de l'intérêt pour l'EEE)

CHAPITRE I

DISPOSITIONS GÉNÉRALES

Article premier

Objet

1. L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur et de promouvoir l'adoption d'une intelligence artificielle (IA) axée sur l'humain et digne de confiance, tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, notamment la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation.

2. Le présent règlement établit:

a) des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation de systèmes d'IA dans l'Union;

b) l'interdiction de certaines pratiques en matière d'IA;

c) des exigences spécifiques applicables aux systèmes d'IA à haut risque et des obligations imposées aux opérateurs de ces systèmes;

d) des règles harmonisées en matière de transparence applicables à certains systèmes d'IA;

e) des règles harmonisées pour la mise sur le marché de modèles d'IA à usage général;

f) des règles relatives au suivi du marché, à la surveillance du marché, à la gouvernance et à l'application des règles;

g) des mesures visant à soutenir l'innovation, en mettant particulièrement l'accent sur les PME, y compris les jeunes pousses.

Article 2

Champ d'application

1. Le présent règlement s'applique:

a) aux fournisseurs établis ou situés dans l'Union ou dans un pays tiers qui mettent sur le marché ou mettent en service des systèmes d'IA ou qui mettent sur le marché des modèles d'IA à usage général dans l'Union;

b) aux déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans l'Union;

▼B

c) aux fournisseurs et aux déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans un pays tiers, lorsque les sorties produites par le système d'IA sont utilisées dans l'Union;

d) aux importateurs et aux distributeurs de systèmes d'IA;

e) aux fabricants de produits qui mettent sur le marché ou mettent en service un système d'IA en même temps que leur produit et sous leur propre nom ou leur propre marque;

f) aux mandataires des fournisseurs qui ne sont pas établis dans l'Union;

g) aux personnes concernées qui sont situées dans l'Union.

2. En ce qui concerne les systèmes d'IA classés à haut risque conformément à l'article 6, paragraphe 1, liés aux produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, seuls l'article 6, paragraphe 1, les articles 102 à 109 et l'article 112 s'appliquent. L'article 57 ne s'applique que dans la mesure où les exigences applicables aux systèmes d'IA à haut risque au titre du présent règlement ont été intégrées dans ladite législation d'harmonisation de l'Union.

3. Le présent règlement ne s'applique pas aux domaines qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, ne porte pas atteinte aux compétences des États membres en matière de sécurité nationale, quel que soit le type d'entité chargée par les États membres d'exécuter des tâches liées à ces compétences.

Le présent règlement ne s'applique pas aux systèmes d'IA si et dans la mesure où ils sont mis sur le marché, mis en service ou utilisés avec ou sans modifications exclusivement à des fins militaires, de défense ou de sécurité nationale, quel que soit le type d'entité exerçant ces activités.

Le présent règlement ne s'applique pas aux systèmes d'IA qui ne sont pas mis sur le marché ou mis en service dans l'Union, lorsque les sorties sont utilisées dans l'Union exclusivement à des fins militaires, de défense ou de sécurité nationale, quel que soit le type d'entité exerçant ces activités.

4. Le présent règlement ne s'applique ni aux autorités publiques d'un pays tiers ni aux organisations internationales relevant du champ d'application du présent règlement en vertu du paragraphe 1, lorsque ces autorités ou organisations utilisent des systèmes d'IA dans le cadre de la coopération internationale ou d'accords internationaux de coopération des services répressifs et judiciaires avec l'Union ou avec un ou plusieurs États membres, à condition que ce pays tiers ou cette organisation internationale fournisse des garanties adéquates en ce qui concerne la protection des droits fondamentaux et des libertés des personnes.

5. Le présent règlement n'affecte pas l'application des dispositions relatives à la responsabilité des prestataires intermédiaires énoncées au chapitre II du règlement (UE) 2022/2065.

6. Le présent règlement ne s'applique pas aux systèmes d'IA ou aux modèles d'IA spécifiquement développés et mis en service uniquement à des fins de recherche et développement scientifiques, ni à leurs sorties.

▼B

7. Le droit de l'Union en matière de protection des données à caractère personnel, de respect de la vie privée et de confidentialité des communications s'applique aux données à caractère personnel traitées en lien avec les droits et obligations énoncés dans le présent règlement. Le présent règlement n'a pas d'incidence sur le règlement (UE) 2016/679 ou le règlement (UE) 2018/1725, ni sur la directive 2002/58/CE ou la directive (UE) 2016/680, sans préjudice de l'article 10, paragraphe 5, et de l'article 59 du présent règlement.

8. Le présent règlement ne s'applique pas aux activités de recherche, d'essai et de développement relatives aux systèmes d'IA ou modèles d'IA avant leur mise sur le marché ou leur mise en service. Ces activités sont menées conformément au droit de l'Union applicable. Les essais en conditions réelles ne sont pas couverts par cette exclusion.

9. Le présent règlement s'entend sans préjudice des règles établies par d'autres actes juridiques de l'Union relatifs à la protection des consommateurs et à la sécurité des produits.

10. Le présent règlement ne s'applique pas aux obligations incombant aux déployeurs qui sont des personnes physiques utilisant des systèmes d'IA dans le cadre d'une activité strictement personnelle à caractère non professionnel.

11. Le présent règlement n'empêche pas l'Union ou les États membres de maintenir ou d'introduire des dispositions législatives, réglementaires ou administratives plus favorables aux travailleurs quant à la protection de leurs droits en ce qui concerne l'utilisation de systèmes d'IA par les employeurs, ou d'encourager ou de permettre l'application de conventions collectives plus favorables aux travailleurs.

12. Le présent règlement ne s'applique pas aux systèmes d'IA publiés dans le cadre de licences libres et ouvertes, sauf s'ils sont mis sur le marché ou mis en service en tant que systèmes d'IA à haut risque ou en tant que systèmes d'IA qui relèvent de l'article 5 ou de l'article 50.

Article 3

Définitions

Aux fins du présent règlement, on entend par:

1) «système d'IA», un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels;

2) «risque», la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci;

3) «fournisseur», une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et le met sur le marché ou met le système d'IA en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit;

▼B

4) «déployeur», une personne physique ou morale, une autorité publique, une agence ou un autre organisme utilisant sous sa propre autorité un système d'IA sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel;

5) «mandataire», une personne physique ou morale située ou établie dans l'Union ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA ou de modèle d'IA à usage général pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement;

6) «importateur», une personne physique ou morale située ou établie dans l'Union qui met sur le marché un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers;

7) «distributeur», une personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union;

8) «opérateur», un fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur;

9) «mise sur le marché», la première mise à disposition d'un système d'IA ou d'un modèle d'IA à usage général sur le marché de l'Union;

10) «mise à disposition sur le marché», la fourniture d'un système d'IA ou d'un modèle d'IA à usage général destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

11) «mise en service», la fourniture d'un système d'IA en vue d'une première utilisation directement au déployeur ou pour usage propre dans l'Union, conformément à la destination du système d'IA;

12) «destination», l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, tels qu'ils sont précisés dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique;

13) «mauvaise utilisation raisonnablement prévisible», l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction raisonnablement prévisible avec d'autres systèmes, y compris d'autres systèmes d'IA;

14) «composant de sécurité», un composant d'un produit ou d'un système d'IA qui remplit une fonction de sécurité pour ce produit ou ce système d'IA, ou dont la défaillance ou le dysfonctionnement met en danger la santé et la sécurité des personnes ou des biens;

15) «notice d'utilisation», les indications communiquées par le fournisseur pour informer le déployeur, en particulier, de la destination et de l'utilisation correcte d'un système d'IA;

▼B

16) «rappel d'un système d'IA», toute mesure visant à assurer le retour au fournisseur d'un système d'IA mis à la disposition de déployeurs ou à le mettre hors service ou à désactiver son utilisation;

17) «retrait d'un système d'IA», toute mesure visant à empêcher qu'un système d'IA se trouvant dans la chaîne d'approvisionnement ne soit mis à disposition sur le marché;

18) «performance d'un système d'IA», la capacité d'un système d'IA à remplir sa destination;

19) «autorité notifiante», l'autorité nationale chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle;

20) «évaluation de la conformité», la procédure permettant de démontrer que les exigences relatives à un système d'IA à haut risque énoncées au chapitre III, section 2, ont été respectées;

21) «organisme d'évaluation de la conformité», un organisme en charge des activités d'évaluation de la conformité par un tiers, y compris la mise à l'essai, la certification et l'inspection;

22) «organisme notifié», un organisme d'évaluation de la conformité notifié en application du présent règlement et d'autres actes législatifs d'harmonisation de l'Union pertinents;

23) «modification substantielle», une modification apportée à un système d'IA après sa mise sur le marché ou sa mise en service, qui n'est pas prévue ou planifiée dans l'évaluation initiale de la conformité réalisée par le fournisseur et qui a pour effet de nuire à la conformité de ce système aux exigences énoncées au chapitre III, section 2, ou qui entraîne une modification de la destination pour laquelle le système d'IA a été évalué;

24) «marquage CE», un marquage par lequel le fournisseur indique qu'un système d'IA est conforme aux exigences du chapitre III, section 2, et d'autres actes législatifs d'harmonisation de l'Union applicables qui en prévoient l'apposition;

25) «système de surveillance après commercialisation», l'ensemble des activités réalisées par les fournisseurs de systèmes d'IA pour recueillir et analyser les données issues de l'expérience d'utilisation des systèmes d'IA qu'ils mettent sur le marché ou mettent en service de manière à repérer toute nécessité d'appliquer immédiatement une mesure préventive ou corrective;

26) «autorité de surveillance du marché», l'autorité nationale assurant la mission et prenant les mesures prévues par le règlement (UE) 2019/1020;

27) «norme harmonisée», une norme harmonisée au sens de l'article 2, paragraphe 1, point c), du règlement (UE) n° 1025/2012;

▼B

28) «spécification commune», un ensemble de spécifications techniques au sens de l'article 2, point 4), du règlement (UE) n° 1025/2012 qui permettent de satisfaire à certaines exigences établies en vertu du présent règlement;

29) «données d'entraînement», les données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînables;

30) «données de validation», les données utilisées pour fournir une évaluation du système d'IA entraîné et pour régler ses paramètres non entraînables ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement;

31) «jeu de données de validation», un jeu de données distinct ou une partie du jeu de données d'entraînement, sous la forme d'une division variable ou fixe;

32) «données de test», les données utilisées pour fournir une évaluation indépendante du système d'IA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service;

33) «données d'entrée», les données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit une sortie;

34) «données biométriques», les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, telles que des images faciales ou des données dactyloscopiques;

35) «identification biométrique», la reconnaissance automatisée de caractéristiques physiques, physiologiques, comportementales ou psychologiques humaines aux fins d'établir l'identité d'une personne physique en comparant ses données biométriques à des données biométriques de personnes stockées dans une base de données;

36) «vérification biométrique», la vérification «un à un» automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données biométriques à des données biométriques précédemment fournies;

37) «catégories particulières de données à caractère personnel», les catégories de données à caractère personnel visées à l'article 9, paragraphe 1, du règlement (UE) 2016/679, à l'article 10 de la directive (UE) 2016/680 et à l'article 10, paragraphe 1, du règlement (UE) 2018/1725;

38) «données opérationnelles sensibles», les données opérationnelles relatives à des activités de prévention et de détection des infractions pénales, ainsi que d'enquête ou de poursuites en la matière, dont la divulgation pourrait compromettre l'intégrité des procédures pénales;

39) «système de reconnaissance des émotions», un système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques;

40) «système de catégorisation biométrique», un système d'IA destiné à affecter des personnes physiques à des catégories spécifiques sur la base de leurs données biométriques, à moins que cela ne soit accessoire à un autre service commercial et strictement nécessaire pour des raisons techniques objectives;

▼B

41) «système d'identification biométrique à distance», un système d'IA destiné à identifier des personnes physiques sans leur participation active, généralement à distance, en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données;

42) «système d'identification biométrique à distance en temps réel», un système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel important et qui comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles;

43) «système d'identification biométrique à distance a posteriori», un système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance en temps réel;

44) «espace accessible au public», tout espace physique de propriété publique ou privée, accessible à un nombre indéterminé de personnes physiques, indépendamment de l'existence de conditions d'accès à cet espace qui puissent s'appliquer, et indépendamment d'éventuelles restrictions de capacité;

45) «autorités répressives»,

a) toute autorité publique compétente pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces; ou

b) tout autre organisme ou entité à qui le droit d'un État membre confie l'exercice de l'autorité publique et des prérogatives de puissance publique à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

46) «activités répressives», des activités menées par les autorités répressives ou pour leur compte pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces;

47) «Bureau de l'IA», la fonction de la Commission consistant à contribuer à la mise en œuvre, au suivi et à la surveillance des systèmes d'IA et de modèles d'IA à usage général et de la gouvernance de l'IA, établi par la décision de la Commission du 24 janvier 2024; les références faites au Bureau de l'IA dans le présent règlement s'entendent comme faites à la Commission;

48) «autorité nationale compétente», une autorité notifiante ou une autorité de surveillance du marché; en ce qui concerne les systèmes d'IA mis en service ou utilisés par les institutions, organes ou organismes de l'Union, les références aux autorités nationales compétentes ou aux autorités de surveillance du marché dans le présent règlement s'entendent comme une référence au Contrôleur européen de la protection des données;

▼B

49) «incident grave», un incident ou dysfonctionnement d'un système d'IA entraînant directement ou indirectement:

a) le décès d'une personne ou une atteinte grave à la santé d'une personne;

b) une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques;

c) la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux;

d) un dommage grave à des biens ou à l'environnement;

50) «données à caractère personnel», les données à caractère personnel définies à l'article 4, point 1), du règlement (UE) 2016/679;

51) «données à caractère non personnel», les données autres que les données à caractère personnel au sens de l'article 4, point 1), du règlement (UE) 2016/679;

52) «profilage», le profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679;

53) «plan d'essais en conditions réelles», un document décrivant les objectifs, la méthode, la population et le champ d'application géographique et la portée dans le temps, le suivi, l'organisation et la conduite des essais en conditions réelles;

54) «plan du bac à sable», un document adopté conjointement entre le fournisseur participant et l'autorité compétente, qui décrit les objectifs, les conditions, les délais, la méthodologie et les exigences applicables aux activités réalisées au sein du bac à sable;

55) «bac à sable réglementaire de l'IA», un cadre contrôlé mis en place par une autorité compétente qui offre aux fournisseurs ou fournisseurs potentiels de systèmes d'IA la possibilité de développer, d'entraîner, de valider et de tester, lorsqu'il y a lieu en conditions réelles, un système d'IA innovant, selon un plan du bac à sable pour une durée limitée sous surveillance réglementaire;

56) «maîtrise de l'IA», les compétences, les connaissances et la compréhension qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le contexte du présent règlement, de procéder à un déploiement des systèmes d'IA en toute connaissance de cause, ainsi que de prendre conscience des possibilités et des risques que comporte l'IA, ainsi que des préjudices potentiels qu'elle peut causer;

57) «essais en conditions réelles», les essais temporaires d'un système d'IA aux fins de sa destination en conditions réelles en dehors d'un laboratoire ou d'un environnement simulé d'une autre manière, visant à recueillir des données fiables et solides et à évaluer et vérifier la conformité du système d'IA aux exigences du présent règlement; les essais en conditions réelles ne remplissent pas les conditions pour constituer une mise sur le marché ni une mise en service du système d'IA au sens du présent règlement, pour autant que toutes les conditions prévues à l'article 57 ou à l'article 60 soient remplies;

58) «participant», aux fins des essais en conditions réelles, une personne physique qui participe à des essais en conditions réelles;

▼B

59) «consentement éclairé», l'expression libre, spécifique, univoque et volontaire, par un participant, de sa volonté de participer à un essai en conditions réelles particulier, après avoir été informé de tous les éléments de l'essai qui lui permettent de prendre sa décision concernant sa participation;

60) «hypertrucage», une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux, des entités ou événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques;

61) «infraction de grande ampleur», tout acte ou toute omission contraire au droit de l'Union en matière de protection des intérêts des personnes, qui:

a) a porté ou est susceptible de porter atteinte aux intérêts collectifs des personnes résidant dans au moins deux États membres autres que celui:

i) où l'acte ou l'omission en question a son origine ou a eu lieu;

ii) où le fournisseur concerné ou, le cas échéant, son mandataire, est situé ou établi; ou

iii) où le déployeur est établi, lorsque l'infraction est commise par le déployeur;

b) a porté, porte ou est susceptible de porter atteinte aux intérêts collectifs des personnes, qui présente des caractéristiques communes, notamment la même pratique illégale ou la violation du même intérêt, et qui se produit simultanément, commise par le même opérateur, dans au moins trois États membres;

62) «infrastructure critique», une infrastructure critique au sens de l'article 2, point 4), de la directive (UE) 2022/2557;

63) «modèle d'IA à usage général», un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes, indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval, à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché;

64) «capacités à fort impact», des capacités égales ou supérieures aux capacités enregistrées dans les modèles d'IA à usage général les plus avancés;

65) «risque systémique», un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûreté, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur;

▼B

66) «système d'IA à usage général», un système d'IA qui est fondé sur un modèle d'IA à usage général et qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA;

67) «opération en virgule flottante», toute opération ou assignation mathématique impliquant des nombres en virgule flottante, qui constituent un sous-ensemble des nombres réels généralement représentés sur un ordinateur par un entier de précision fixe suivi d'un exposant entier d'une base fixe;

68) «fournisseur en aval», un fournisseur d'un système d'IA, y compris d'un système d'IA à usage général, qui intègre un modèle d'IA, que le modèle d'IA soit fourni par lui-même ou non, et verticalement intégré ou fourni par une autre entité sur la base de relations contractuelles.

Article 4

Maîtrise de l'IA

Les fournisseurs et les déployeurs de systèmes d'IA prennent des mesures pour garantir, dans toute la mesure du possible, un niveau suffisant de maîtrise de l'IA pour leur personnel et les autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte, en prenant en considération leurs connaissances techniques, leur expérience, leur éducation et leur formation, ainsi que le contexte dans lequel les systèmes d'IA sont destinés à être utilisés, et en tenant compte des personnes ou des groupes de personnes à l'égard desquels les systèmes d'IA sont destinés à être utilisés.

CHAPITRE II

PRATIQUES INTERDITES EN MATIÈRE D'IA

Article 5

Pratiques interdites en matière d'IA

1. Les pratiques en matière d'IA suivantes sont interdites:

a) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales, au-dessous du seuil de conscience d'une personne, ou à des techniques délibérément manipulatrices ou trompeuses, avec pour objectif ou effet d'altérer substantiellement le comportement d'une personne ou d'un groupe de personnes en portant considérablement atteinte à leur capacité à prendre une décision éclairée, amenant ainsi la personne à prendre une décision qu'elle n'aurait pas prise autrement, d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne, à une autre personne ou à un groupe de personnes;

b) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite les éventuelles vulnérabilités dues à l'âge, au handicap ou à la situation sociale ou économique spécifique d'une personne physique ou d'un groupe de personnes donné avec pour objectif ou effet d'altérer substantiellement le comportement de cette personne ou d'un membre de ce groupe d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à un tiers;

▼B

c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA pour l'évaluation ou la classification de personnes physiques ou de groupes de personnes au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites, la note sociale conduisant à l'une ou l'autre des situations suivantes, ou aux deux:

   i) le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes de personnes dans des contextes sociaux dissociés du contexte dans lequel les données ont été générées ou collectées à l'origine;

   ii) le traitement préjudiciable ou défavorable de certaines personnes ou de groupes de personnes, qui est injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci;

d) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation d'un système d'IA pour mener des évaluations des risques des personnes physiques visant à évaluer ou à prédire le risque qu'une personne physique commette une infraction pénale, uniquement sur la base du profilage d'une personne physique ou de l'évaluation de ses traits de personnalité ou caractéristiques; cette interdiction ne s'applique pas aux systèmes d'IA utilisés pour étayer l'évaluation humaine de l'implication d'une personne dans une activité criminelle, qui est déjà fondée sur des faits objectifs et vérifiables, directement liés à une activité criminelle;

e) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance;

f) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA pour inférer les émotions d'une personne physique sur le lieu de travail et dans les établissements d'enseignement, sauf lorsque l'utilisation du système d'IA est destinée à être mise en place ou mise sur le marché pour des raisons médicales ou de sécurité;

g) la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes de catégorisation biométrique qui catégorisent individuellement les personnes physiques sur la base de leurs données biométriques afin d'arriver à des déductions ou des inférences concernant leur race, leurs opinions politiques, leur affiliation à une organisation syndicale, leurs convictions religieuses ou philosophiques, leur vie sexuelle ou leur orientation sexuelle; cette interdiction ne couvre pas l'étiquetage ou le filtrage d'ensembles de données biométriques acquis légalement, tels que des images, fondés sur des données biométriques ou la catégorisation de données biométriques dans le domaine répressif;

h) l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, sauf si et dans la mesure où cette utilisation est strictement nécessaire eu égard à l'un des objectifs suivants:

   i) la recherche ciblée de victimes spécifiques d'enlèvement, de la traite ou de l'exploitation sexuelle d'êtres humains, ainsi que la recherche de personnes disparues;

▼B

ii) la prévention d'une menace spécifique, substantielle et imminente pour la vie ou la sécurité physique de personnes physiques ou d'une menace réelle et actuelle ou réelle et prévisible d'attaque terroriste;

iii) la localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale, aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'annexe II et punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'une durée maximale d'au moins quatre ans.

Le premier alinéa, point h), est sans préjudice de l'article 9 du règlement (UE) 2016/679 pour le traitement des données biométriques à des fins autres que répressives.

2. L'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), n'est déployée aux fins énoncées audit point, que pour confirmer l'identité de la personne spécifiquement ciblée et tient compte des éléments suivants:

a) la nature de la situation donnant lieu à un éventuel recours au système, en particulier la gravité, la probabilité et l'ampleur du préjudice qui serait causé si le système n'était pas utilisé;

b) les conséquences de l'utilisation du système sur les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de ces conséquences.

En outre, l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives en vue de la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), du présent article respecte les garanties et conditions nécessaires et proportionnées en ce qui concerne cette utilisation, conformément au droit national qui l'autorise, notamment eu égard aux limitations temporelles, géographiques et relatives aux personnes. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public n'est autorisée que si l'autorité répressive a réalisé une analyse d'impact sur les droits fondamentaux conformément à l'article 27 et a enregistré le système dans la base de données de l'UE prévue par l'article 49. Toutefois, dans des cas d'urgence dûment justifiés, il est possible de commencer à utiliser ces systèmes sans enregistrement dans la base de données de l'UE, à condition que cet enregistrement soit effectué sans retard injustifié.

3. Aux fins du paragraphe 1, premier alinéa, point h), et du paragraphe 2, chaque utilisation à des fins répressives d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public est subordonnée à une autorisation préalable octroyée par une autorité judiciaire ou une autorité administrative indépendante dont la décision est contraignante de l'État membre dans lequel cette utilisation doit avoir lieu, délivrée sur demande motivée et conformément aux règles détaillées du droit national visées au paragraphe 5. Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser ce système sans autorisation à condition que cette autorisation soit demandée sans retard injustifié, au plus tard dans les 24 heures. Si cette autorisation est rejetée, il est mis fin à l'utilisation avec effet immédiat, et toutes les données, ainsi que les résultats et sorties de cette utilisation, sont immédiatement mis au rebut et supprimés.

▼B

L'autorité judiciaire compétente ou une autorité administrative indépendante dont la décision est contraignante n'accorde l'autorisation que si elle estime, sur la base d'éléments objectifs ou d'indications claires qui lui sont présentés, que l'utilisation du système d'identification biométrique à distance en temps réel concerné est nécessaire et proportionnée à la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), tels qu'indiqués dans la demande et, en particulier, que cette utilisation reste limitée au strict nécessaire dans le temps et du point de vue de la portée géographique et personnelle. Lorsqu'elle statue sur la demande, cette autorité tient compte des éléments visés au paragraphe 2. Aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne peut être prise sur la seule base de la sortie du système d'identification biométrique à distance «en temps réel».

4. Sans préjudice du paragraphe 3, toute utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives est notifiée à l'autorité de surveillance du marché concernée et à l'autorité nationale chargée de la protection des données, conformément aux règles nationales visées au paragraphe 5. Cette notification contient, au minimum, les informations visées au paragraphe 6 et n'inclut pas de données opérationnelles sensibles.

5. Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, dans les limites et les conditions énumérées au paragraphe 1, premier alinéa, point h), et aux paragraphes 2 et 3. Les États membres concernés établissent dans leur droit national les règles détaillées nécessaires à la demande, à la délivrance et à l'exercice des autorisations visées au paragraphe 3, ainsi qu'à la surveillance et à l'établissement de rapports y afférents. Ces règles précisent également pour quels objectifs énumérés au paragraphe 1, premier alinéa, point h), et notamment pour quelles infractions pénales visées au point h), iii), les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives. Les États membres notifient ces règles à la Commission au plus tard 30 jours après leur adoption. Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance.

6. Les autorités nationales de surveillance du marché et les autorités nationales chargées de la protection des données des États membres qui ont été notifiées de l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, conformément au paragraphe 4, soumettent à la Commission des rapports annuels sur cette utilisation. À cette fin, la Commission fournit aux États membres et aux autorités nationales en matière de surveillance du marché et de protection des données un modèle comprenant des informations sur le nombre de décisions prises par les autorités judiciaires compétentes ou par une autorité administrative indépendante dont la décision est contraignante en ce qui concerne les demandes d'autorisation conformément au paragraphe 3, ainsi que sur leur résultat.

7. La Commission publie des rapports annuels sur l'utilisation de systèmes d'identification biométriques à distance en temps réel dans des espaces accessibles au public à des fins répressives, fondés sur des données agrégées dans les États membres sur la base des rapports annuels visés au paragraphe 6. Ces rapports annuels n'incluent pas de données opérationnelles sensibles sur les activités répressives connexes.

▼B

8. Le présent article ne porte pas atteinte aux interdictions qui s'appliquent lorsqu'une pratique en matière d'IA enfreint d'autres dispositions du droit de l'Union.

CHAPITRE III

SYSTÈMES D'IA À HAUT RISQUE

SECTION 1

Classification de systèmes d'IA comme systèmes à haut risque

Article 6

Règles relatives à la classification de systèmes d'IA comme systèmes à haut risque

1. Un système d'IA mis sur le marché ou mis en service, qu'il soit ou non indépendant des produits visés aux points a) et b), est considéré comme étant à haut risque lorsque les deux conditions suivantes sont remplies:

a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou le système d'IA constitue lui-même un tel produit;

b) le produit dont le composant de sécurité visé au point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de conformité par un tiers en vue de la mise sur le marché ou de la mise en service de ce produit conformément à la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.

2. Outre les systèmes d'IA à haut risque visés au paragraphe 1, les systèmes d'IA visés à l'annexe III sont considérés comme étant à haut risque.

3. Par dérogation au paragraphe 2, un système d'IA visé à l'annexe III n'est pas considéré comme étant à haut risque lorsqu'il ne présente pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques, y compris en n'ayant pas d'incidence significative sur le résultat de la prise de décision.

Le premier alinéa s'applique lorsqu'une des conditions suivantes est remplie:

a) le système d'IA est destiné à accomplir un tâche procédurale étroite;

b) le système d'IA est destiné à améliorer le résultat d'une activité humaine préalablement réalisée;

c) le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures et n'est pas destiné à se substituer à l'évaluation humaine préalablement réalisée, ni à influencer celle-ci, sans examen humain approprié; ou

d) le système d'IA est destiné à exécuter une tâche préparatoire en vue d'une évaluation pertinente aux fins des cas d'utilisation visés à l'annexe III.

▼B

Nonobstant le premier alinéa, un système d'IA visé à l'annexe III est toujours considéré comme étant à haut risque lorsqu'il effectue un profilage de personnes physiques.

4. Un fournisseur qui considère qu'un système d'IA visé à l'annexe III n'est pas à haut risque documente son évaluation avant que ce système ne soit mis sur le marché ou mis en service. Ce fournisseur est soumis à l'obligation d'enregistrement visée à l'article 49, paragraphe 2. À la demande des autorités nationales compétentes, le fournisseur fournit la documentation de l'évaluation.

5. Après consultation du Comité européen de l'intelligence artificielle (ci-après dénommé «Comité IA»), et au plus tard le 2 février 2026, la Commission fournit des lignes directrices précisant la mise en œuvre pratique du présent article, conformément à l'article 96, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier le paragraphe 3, deuxième alinéa, du présent article en ajoutant de nouvelles conditions à celles qui y sont énoncées, ou en les modifiant, lorsqu'il existe des preuves concrètes et fiables de l'existence de systèmes d'IA qui relèvent du champ d'application de l'annexe III, mais qui ne présentent pas de risque important de préjudice pour la santé, la sécurité ou les droits fondamentaux des personnes physiques.

7. La Commission adopte des actes délégués conformément à l'article 97 afin de modifier le paragraphe 3, deuxième alinéa, du présent article en supprimant l'une des conditions qui y est établie, lorsqu'il existe des preuves concrètes et fiables attestant que cela est nécessaire pour maintenir le niveau de protection de la santé, de la sécurité et des droits fondamentaux prévu par le présent règlement.

8. Toute modification des conditions établies au paragraphe 3, deuxième alinéa, adoptée conformément aux paragraphe 6 et 7 du présent article ne diminue pas le niveau global de protection de la santé, de la sécurité et des droits fondamentaux prévu par le présent règlement et veille à la cohérence avec les actes délégués adoptés conformément à l'article 7, paragraphe 1, et tient compte des évolutions du marché et des technologies.

Article 7

Modifications de l'annexe III

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe III en y ajoutant des cas d'utilisation de systèmes d'IA à haut risque, ou en les modifiant, lorsque les deux conditions suivantes sont remplies:

a) les systèmes d'IA sont destinés à être utilisés dans l'un des domaines énumérés à l'annexe III;

b) les systèmes d'IA présentent un risque de préjudice pour la santé et la sécurité, ou un risque d'incidence négative sur les droits fondamentaux, et ce risque est équivalent ou supérieur au risque de préjudice ou d'incidence négative que présentent les systèmes d'IA à haut risque déjà visés à l'annexe III.

▼B

2. Lorsqu'elle évalue les conditions visées au paragraphe 1, point b), la Commission tient compte des critères suivants:

a) la destination du système d'IA;

b) la mesure dans laquelle un système d'IA a été utilisé ou est susceptible de l'être;

c) la nature et la quantité des données traitées et utilisées par le système d'IA, en particulier le traitement ou l'absence de traitement des catégories particulières de données à caractère personnel;

d) la mesure dans laquelle le système d'IA agit de manière autonome et la mesure dans laquelle l'homme peut intervenir pour annuler une décision ou des recommandations susceptibles de causer un préjudice potentiel;

e) la mesure dans laquelle l'utilisation d'un système d'IA a déjà causé un préjudice à la santé et à la sécurité, a eu une incidence négative sur les droits fondamentaux ou a suscité de graves préoccupations quant à la probabilité de ce préjudice ou de cette incidence négative, tel que cela ressort, par exemple, des rapports ou allégations documentées soumis aux autorités nationales compétentes ou d'autres rapports, le cas échéant;

f) l'ampleur potentielle d'un tel préjudice ou d'une telle incidence négative, notamment en ce qui concerne son intensité et sa capacité d'affecter plusieurs personnes ou d'affecter un groupe particulier de personnes de manière disproportionnée;

g) la mesure dans laquelle les personnes ayant potentiellement subi un préjudice ou une incidence négative dépendent des résultats obtenus au moyen d'un système d'IA, notamment parce qu'il n'est pas raisonnablement possible, pour des raisons pratiques ou juridiques, de s'affranchir de ces résultats;

h) la mesure dans laquelle il existe un déséquilibre de pouvoir, ou les personnes ayant potentiellement subi un préjudice ou une incidence négative se trouvent dans une situation vulnérable par rapport au déployeur d'un système d'IA, notamment en raison du statut, de l'autorité, de connaissances, de circonstances économiques ou sociales ou de l'âge;

i) la mesure dans laquelle les résultats obtenus en utilisant un système d'IA sont facilement corrigibles ou réversibles, compte tenu des solutions techniques disponibles pour les corriger ou les inverser, les résultats qui ont une incidence négative sur la santé, la sécurité ou les droits fondamentaux ne devant pas être considérés comme facilement corrigibles ou réversibles;

j) la probabilité que le déploiement du système d'IA présente des avantages pour certaines personnes, certains groupes de personnes ou la société dans son ensemble et la portée de ces avantages, y compris les améliorations éventuelles quant à la sécurité des produits;

k) la mesure dans laquelle le droit existant de l'Union prévoit:

   i) des mesures de réparation efficaces en ce qui concerne les risques posés par un système d'IA, à l'exclusion des réclamations en dommages-intérêts;

   ii) des mesures efficaces destinées à prévenir ou à réduire substantiellement ces risques.

▼B

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier la liste figurant à l'annexe III en supprimant des systèmes d'IA à haut risque lorsque les deux conditions suivantes sont remplies:

a) le système d'IA à haut risque concerné ne présente plus de risques substantiels pour les droits fondamentaux, la santé ou la sécurité, compte tenu des critères énumérés au paragraphe 2;

b) la suppression ne diminue pas le niveau global de protection de la santé, de la sécurité et des droits fondamentaux en vertu du droit de l'Union.

SECTION 2

Exigences applicables aux systèmes d'IA à haut risque

Article 8

Respect des exigences

1. Les systèmes d'IA à haut risque respectent les exigences énoncées dans la présente section, en tenant compte de leur destination ainsi que de l'état de la technique généralement reconnu en matière d'IA et de technologies liées à l'IA. Pour garantir le respect de ces exigences, il est tenu compte du système de gestion des risques prévu à l'article 9.

2. Lorsqu'un produit contient un système d'IA auquel s'appliquent les exigences du présent règlement ainsi que les exigences de la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, les fournisseurs sont chargés de veiller à ce que leur produit soit pleinement conforme à toutes les exigences en vertu de la législation d'harmonisation de l'Union applicable. Pour garantir que les systèmes d'IA à haut risque visés au paragraphe 1 sont conformes aux exigences énoncées dans la présente section, et afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les processus d'essai et de déclaration nécessaires, les informations et la documentation qu'ils fournissent concernant leur produit dans la documentation et les procédures qui existent déjà et qui sont requises en vertu de la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I.

Article 9

Système de gestion des risques

1. Un système de gestion des risques est établi, mis en œuvre, documenté et tenu à jour en ce qui concerne les systèmes d'IA à haut risque.

2. Ce système de gestion des risques s'entend comme étant un processus itératif continu qui est planifié et se déroule sur l'ensemble du cycle de vie d'un système d'IA à haut risque et qui doit périodiquement faire l'objet d'un examen et d'une mise à jour méthodiques. Il comprend les étapes suivantes:

a) l'identification et l'analyse des risques connus et raisonnablement prévisibles que le système d'IA à haut risque peut poser pour la santé, la sécurité ou les droits fondamentaux lorsque le système d'IA à haut risque est utilisé conformément à sa destination;

▼B

b) l'estimation et l'évaluation des risques susceptibles d'apparaître lorsque le système d'IA à haut risque est utilisé conformément à sa destination et dans des conditions de mauvaise utilisation raisonnablement prévisible;

c) l'évaluation d'autres risques susceptibles d'apparaître, sur la base de l'analyse des données recueillies au moyen du système de surveillance après commercialisation visé à l'article 72;

d) l'adoption de mesures appropriées et ciblées de gestion des risques, conçues pour répondre aux risques identifiés en vertu du point a).

3. Les risques visés au présent article ne concernent que ceux qui peuvent être raisonnablement atténués ou éliminés dans le cadre du développement ou de la conception du système d'IA à haut risque, ou par la fourniture d'informations techniques appropriées.

4. Les mesures de gestion des risques visées au paragraphe 2, point d), tiennent dûment compte des effets et de l'interaction possibles résultant de l'application combinée des exigences énoncées dans la présente section, en vue de prévenir les risques plus efficacement tout en parvenant à un bon équilibre dans le cadre de la mise en œuvre des mesures visant à répondre à ces exigences.

5. Les mesures de gestion des risques visées au paragraphe 2, point d), sont telles que le risque résiduel pertinent associé à chaque danger ainsi que le risque résiduel global lié aux systèmes d'IA à haut risque sont jugés acceptables.

Pour déterminer les mesures de gestion des risques les plus adaptées, il convient de veiller à:

a) éliminer ou réduire les risques identifiés et évalués conformément au paragraphe 2 autant que la technologie le permet grâce à une conception et à un développement appropriés du système d'IA à haut risque;

b) mettre en œuvre, le cas échéant, des mesures adéquates d'atténuation et de contrôle répondant aux risques impossibles à éliminer;

c) fournir aux déployeurs les informations requises conformément à l'article 13 et, éventuellement, une formation.

En vue de l'élimination ou de la réduction des risques liés à l'utilisation du système d'IA à haut risque, il est dûment tenu compte des connaissances techniques, de l'expérience, de l'éducation et de la formation pouvant être attendues du déployeur, ainsi que du contexte prévisible dans lequel le système est destiné à être utilisé.

6. Les systèmes d'IA à haut risque sont soumis à des essais afin de déterminer les mesures de gestion des risques les plus appropriées et les plus ciblées. Les essais garantissent que les systèmes d'IA à haut risque fonctionnent de manière conforme à leur destination et qu'ils sont conformes aux exigences énoncées dans la présente section.

7. Les procédures d'essai peuvent comprendre des essais en conditions réelles conformément à l'article 60.

8. Les tests des systèmes d'IA à haut risque sont effectués, selon les besoins, à tout moment pendant le processus de développement et, en tout état de cause, avant leur mise sur le marché ou leur mise en service. Les tests sont effectués sur la base d'indicateurs et de seuils probabilistes préalablement définis, qui sont adaptés à la destination du système d'IA à haut risque.

▼B

9. Lors de la mise en œuvre du système de gestion des risques prévu aux paragraphes 1 à 7, les fournisseurs prennent en considération la probabilité que, compte tenu de sa destination, le système d'IA à haut risque puisse avoir une incidence négative sur des personnes âgées de moins de 18 ans et, le cas échéant, sur d'autres groupes vulnérables.

10. En ce qui concerne les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des exigences concernant les processus internes de gestion des risques en vertu d'autres dispositions pertinentes du droit de l'Union, les aspects présentés aux paragraphes 1 à 9 peuvent faire partie des procédures de gestion des risques établies conformément à ladite législation, ou être combinées à celles-ci.

Article 10

Données et gouvernance des données

1. Les systèmes d'IA à haut risque faisant appel à des techniques qui impliquent l'entraînement de modèles d'IA au moyen de données sont développés sur la base de jeux de données d'entraînement, de validation et de test qui satisfont aux critères de qualité visés aux paragraphes 2 à 5 chaque fois que ces jeux de données sont utilisés.

▼C1

2. Les jeux de données d'entraînement, de validation et de test sont soumis à des pratiques en matière de gouvernance et de gestion des données appropriées à la destination du système d'IA à haut risque. Ces pratiques concernent en particulier:

▼B

a) les choix de conception pertinents;

b) les processus de collecte de données et l'origine des données, ainsi que, dans le cas des données à caractère personnel, la finalité initiale de la collecte de données;

c) les opérations de traitement pertinentes pour la préparation des données, telles que l'annotation, l'étiquetage, le nettoyage, la mise à jour, l'enrichissement et l'agrégation;

d) la formulation d'hypothèses, notamment en ce qui concerne les informations que les données sont censées mesurer et représenter;

e) une évaluation de la disponibilité, de la quantité et de l'adéquation des jeux de données nécessaires;

f) un examen permettant de repérer d'éventuels biais qui sont susceptibles de porter atteinte à la santé et à la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de se traduire par une discrimination interdite par le droit de l'Union, en particulier lorsque les données de sortie influencent les entrées pour les opérations futures;

g) les mesures appropriées visant à détecter, prévenir et atténuer les éventuels biais repérés conformément au point f);

h) la détection de lacunes ou déficiences pertinentes dans les données qui empêchent l'application du présent règlement, et la manière dont ces lacunes ou déficiences peuvent être comblées.

3. Les jeux de données d'entraînement, de validation et de test sont pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination. Ils possèdent les propriétés statistiques appropriées, y compris, le cas

▼B

échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le système d'IA à haut risque est destiné à être utilisé. Ces caractéristiques des jeux de données peuvent être remplies au niveau des jeux de données pris individuellement ou d'une combinaison de ceux-ci.

4. Les jeux de données tiennent compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé.

5. Dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, conformément au paragraphe 2, points f) et g), du présent article, les fournisseurs de ces systèmes peuvent exceptionnellement traiter des catégories particulières de données à caractère personnel, sous réserve de garanties appropriées pour les droits et libertés fondamentaux des personnes physiques. Outre les dispositions des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680, toutes les conditions suivantes doivent être réunies pour que ce traitement puisse avoir lieu:

a) la détection et la correction des biais ne peuvent être satisfaites de manière efficace en traitant d'autres données, y compris des données synthétiques ou anonymisées;

b) les catégories particulières de données à caractère personnel sont soumises à des limitations techniques relatives à la réutilisation des données à caractère personnel, ainsi qu'aux mesures les plus avancées en matière de sécurité et de protection de la vie privée, y compris la pseudonymisation;

c) les catégories particulières de données à caractère personnel font l'objet de mesures visant à garantir que les données à caractère personnel traitées sont sécurisées, protégées et soumises à des garanties appropriées, y compris des contrôles stricts et une documentation de l'accès, afin d'éviter toute mauvaise utilisation et de veiller à ce que seules les personnes autorisées ayant des obligations de confidentialité appropriées aient accès à ces données à caractère personnel;

d) les catégories particulières de données à caractère personnel ne doivent pas être transmises, transférées ou consultées d'une autre manière par d'autres parties;

e) les catégories particulières de données à caractère personnel sont supprimées une fois que le biais a été corrigé ou que la période de conservation des données à caractère personnel a expiré, selon celle de ces deux échéances qui arrive en premier;

f) les registres des activités de traitement visés dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680 comprennent les raisons pour lesquelles le traitement des catégories particulières de données à caractère personnel était strictement nécessaire pour détecter et corriger les biais, ainsi que la raison pour laquelle cet objectif n'a pas pu être atteint par le traitement d'autres données.

6. En ce qui concerne le développement de systèmes d'IA à haut risque qui ne font pas appel à des techniques qui impliquent l'entraînement de modèles d'IA, les paragraphes 2 à 5 s'appliquent uniquement aux jeux de données de test.

▼B

Article 11

Documentation technique

1. La documentation technique relative à un système d'IA à haut risque est établie avant que ce système ne soit mis sur le marché ou mis en service et est tenue à jour.

La documentation technique est établie de manière à démontrer que le système d'IA à haut risque satisfait aux exigences énoncées dans la présente section et à fournir aux autorités nationales compétentes et aux organismes notifiés les informations nécessaires sous une forme claire et intelligible pour évaluer la conformité du système d'IA avec ces exigences. Elle contient, au minimum, les éléments énoncés à l'annexe IV. Les PME, y compris les jeunes pousses, peuvent fournir des éléments de la documentation technique spécifiée à l'annexe IV d'une manière simplifiée. À cette fin, la Commission établit un formulaire de documentation technique simplifié ciblant les besoins des petites entreprises et des microentreprises. Lorsqu'une PME, y compris une jeune pousse, choisit de fournir les informations requises à l'annexe IV de manière simplifiée, elle utilise le formulaire visé au présent paragraphe. Les organismes notifiés acceptent le formulaire aux fins de l'évaluation de la conformité.

2. Lorsqu'un système d'IA à haut risque lié à un produit couvert par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I est mis sur le marché ou mis en service, un seul ensemble de documentation technique est établi, contenant toutes les informations visées au paragraphe 1, ainsi que les informations requises en vertu de ces actes juridiques.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe IV, lorsque cela est nécessaire, afin de garantir que, compte tenu du progrès technique, la documentation technique fournit toutes les informations requises pour évaluer la conformité du système avec les exigences énoncées dans la présente section.

Article 12

Enregistrement

1. Les systèmes d'IA à haut risque permettent, techniquement, l'enregistrement automatique des événements (journaux) tout au long de la durée de vie du système.

2. Afin de garantir un degré de traçabilité du fonctionnement d'un système d'IA qui soit adapté à la destination du système, les fonctionnalités de journalisation permettent l'enregistrement des événements pertinents pour:

a) repérer les situations susceptibles d'avoir pour effet que le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, ou d'entraîner une modification substantielle;

b) faciliter la surveillance après commercialisation visée à l'article 72; et

▼B

c) surveiller le fonctionnement du système d'IA à haut risque comme prévu à l'article 26, paragraphe 5.

3. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les fonctionnalités de journalisation fournissent, au minimum:

a) l'enregistrement de la période de chaque utilisation du système (date et heure de début et de fin pour chaque utilisation);

b) la base de données de référence utilisée par le système pour vérifier les données d'entrée;

c) les données d'entrée pour lesquelles la recherche a abouti à une correspondance;

d) l'identification des personnes physiques participant à la vérification des résultats, visées à l'article 14, paragraphe 5.

Article 13

Transparence et fourniture d'informations aux déployeurs

1. La conception et le développement des systèmes d'IA à haut risque sont tels que le fonctionnement de ces systèmes est suffisamment transparent pour permettre aux déployeurs d'interpréter les sorties d'un système et de les utiliser de manière appropriée. Un type et un niveau adéquats de transparence sont garantis afin de veiller au respect des obligations pertinentes incombant au fournisseur et au déployeur énoncées à la section 3.

2. Les systèmes d'IA à haut risque sont accompagnés d'une notice d'utilisation dans un format numérique approprié ou autre, contenant des informations concises, complètes, exactes et claires, qui soient pertinentes, accessibles et compréhensibles pour les déployeurs.

3. La notice d'utilisation contient au moins les informations suivantes:

a) l'identité et les coordonnées du fournisseur et, le cas échéant, de son mandataire;

b) les caractéristiques, les capacités et les limites de performance du système d'IA à haut risque, notamment:

   i) sa destination;

   ii) le niveau d'exactitude, y compris les indicateurs utilisés, de robustesse et de cybersécurité visé à l'article 15 qui a servi de référence pour les tests et la validation du système d'IA à haut risque et qui peut être attendu, ainsi que toutes circonstances connues et prévisibles susceptibles d'avoir une incidence sur le niveau attendu d'exactitude, de robustesse et de cybersécurité;

   iii) toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé et la sécurité ou pour les droits fondamentaux visés à l'article 9, paragraphe 2;

   iv) le cas échéant, les capacités et caractéristiques techniques du système d'IA à haut risque à fournir des informations pertinentes pour expliquer ses sorties;

▼B

v) le cas échéant, sa performance en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé;

vi) le cas échéant, les spécifications relatives aux données d'entrée, ou toute autre information pertinente concernant les jeux de données d'entraînement, de validation et de test utilisés, compte tenu de la destination du système d'IA à haut risque;

vii) le cas échéant, les informations permettant aux déployeurs d'interpréter les sorties du système d'IA à haut risque et de les utiliser de manière appropriée;

c) les modifications du système d'IA à haut risque et de sa performance qui ont été prédéterminées par le fournisseur au moment de l'évaluation initiale de la conformité, le cas échéant;

d) les mesures de contrôle humain visées à l'article 14, notamment les mesures techniques mises en place pour faciliter l'interprétation des sorties des systèmes d'IA à haut risque par les déployeurs;

e) les ressources informatiques et matérielles nécessaires, la durée de vie attendue du système d'IA à haut risque et toutes les mesures de maintenance et de suivi, y compris leur fréquence, nécessaires pour assurer le bon fonctionnement de ce système d'IA, notamment en ce qui concerne les mises à jour logicielles;

f) le cas échéant, une description des mécanismes compris dans le système d'IA à haut risque qui permet aux déployeurs de collecter, stocker et interpréter correctement les journaux, conformément à l'article 12.

Article 14

Contrôle humain

1. La conception et le développement des systèmes d'IA à haut risque permettent, notamment au moyen d'interfaces homme-machine appropriées, un contrôle effectif par des personnes physiques pendant leur période d'utilisation.

2. Le contrôle humain vise à prévenir ou à réduire au minimum les risques pour la santé, la sécurité ou les droits fondamentaux qui peuvent apparaître lorsqu'un système d'IA à haut risque est utilisé conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, en particulier lorsque de tels risques persistent malgré l'application d'autres exigences énoncées dans la présente section.

3. Les mesures de contrôle sont proportionnées aux risques, au niveau d'autonomie et au contexte d'utilisation du système d'IA à haut risque, et sont assurées au moyen d'un ou des deux types de mesures suivants:

a) des mesures identifiées et, lorsque cela est techniquement possible, intégrées par le fournisseur dans le système d'IA à haut risque avant la mise sur le marché ou la mise en service de ce dernier;

b) des mesures identifiées par le fournisseur avant la mise sur le marché ou la mise en service du système d'IA à haut risque et qui se prêtent à une mise en œuvre par le déployeur.

▼B

4. Aux fins de la mise en œuvre des dispositions des paragraphes 1, 2 et 3, le système d'IA à haut risque est fourni au déployeur de telle manière que les personnes physiques chargées d'effectuer un contrôle humain, dans la mesure où cela est approprié et proportionné, ont la possibilité:

a) de comprendre correctement les capacités et les limites pertinentes du système d'IA à haut risque et d'être en mesure de surveiller correctement son fonctionnement, y compris en vue de détecter et de traiter les anomalies, les dysfonctionnements et les performances inattendues;

b) d'avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux sorties produites par un système d'IA à haut risque (biais d'automatisation), en particulier pour les systèmes d'IA à haut risque utilisés pour fournir des informations ou des recommandations concernant les décisions à prendre par des personnes physiques;

c) d'interpréter correctement les sorties du système d'IA à haut risque, compte tenu par exemple des outils et méthodes d'interprétation disponibles;

d) de décider, dans une situation particulière, de ne pas utiliser le système d'IA à haut risque ou d'ignorer, remplacer ou inverser la sortie du système d'IA à haut risque;

e) d'intervenir dans le fonctionnement du système d'IA à haut risque ou d'interrompre le système au moyen d'un bouton d'arrêt ou d'une procédure similaire permettant au système de s'arrêter de manière sécurisée.

5. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les mesures prévues au paragraphe 3 du présent article sont de nature à garantir que, en outre, aucune mesure ou décision n'est prise par le déployeur sur la base de l'identification résultant du système sans vérification et confirmation distinctes de cette identification par au moins deux personnes physiques disposant des compétences, de la formation et de l'autorité nécessaires.

L'exigence d'une vérification distincte par au moins deux personnes physiques ne s'applique pas aux systèmes d'IA à haut risque utilisés à des fins répressives ou dans les domaines de la migration, des contrôles aux frontières ou de l'asile, lorsque le droit de l'Union ou le droit national considère que l'application de cette exigence est disproportionnée.

Article 15

Exactitude, robustesse et cybersécurité

1. La conception et le développement des systèmes d'IA à haut risque sont tels qu'ils leur permettent d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de façon constante à cet égard tout au long de leur cycle de vie.

2. Pour examiner les aspects techniques de la manière de mesurer les niveaux appropriés d'exactitude et de robustesse visés au paragraphe 1 et tout autre indicateur de performance pertinent, la Commission, en coopération avec les parties prenantes et organisations concernées, telles que les autorités de métrologie et d'étalonnage des performances, encourage, le cas échéant, l'élaboration de critères de référence et de méthodes de mesure.

▼B

3. Les niveaux d'exactitude et les indicateurs de l'exactitude des systèmes d'IA à haut risque sont indiqués dans la notice d'utilisation jointe.

4. Les systèmes d'IA à haut risque font preuve d'autant de résilience que possible en cas d'erreurs, de défaillances ou d'incohérences pouvant survenir au sein des systèmes eux-mêmes ou de l'environnement dans lequel ils fonctionnent, notamment en raison de leur interaction avec des personnes physiques ou d'autres systèmes. Des mesures techniques et organisationnelles sont prises à cet égard.

Des solutions techniques redondantes, telles que des plans de sauvegarde ou des mesures de sécurité après défaillance, peuvent permettre de garantir la robustesse des systèmes d'IA à haut risque.

Les systèmes d'IA à haut risque qui continuent leur apprentissage après leur mise sur le marché ou leur mise en service sont développés de manière à éliminer ou à réduire dans la mesure du possible le risque que des sorties éventuellement biaisées n'influencent les entrées pour les opérations futures (boucles de rétroaction) et à veiller à ce que ces boucles de rétroaction fassent l'objet d'un traitement adéquat au moyen de mesures d'atténuation appropriées.

5. Les systèmes d'IA à haut risque résistent aux tentatives de tiers non autorisés visant à modifier leur utilisation, leurs sorties ou leur performance en exploitant les vulnérabilités du système.

Les solutions techniques visant à garantir la cybersécurité des systèmes d'IA à haut risque sont adaptées aux circonstances pertinentes et aux risques.

Les solutions techniques destinées à remédier aux vulnérabilités spécifiques à l'IA comprennent, au besoin, des mesures ayant pour but de prévenir, de détecter, de contrer, de résoudre et de maîtriser les attaques visant à manipuler le jeu de données d'entraînement (empoisonnement des données) ou les composants préentraînés utilisés en entraînement (empoisonnement de modèle), les entrées destinées à induire le modèle d'IA en erreur (exemples contradictoires ou invasion de modèle), les attaques visant la confidentialité ou les défauts du modèle.

SECTION 3

Obligations incombant aux fournisseurs et aux déployeurs de systèmes d'IA à haut risque et à d'autres parties

Article 16

Obligations incombant aux fournisseurs de systèmes d'IA à haut risque

Les fournisseurs de systèmes d'IA à haut risque:

a) veillent à ce que leurs systèmes d'IA à haut risque soient conformes aux exigences énoncées à la section 2;

b) indiquent sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur son emballage ou dans la documentation l'accompagnant, selon le cas, leur nom, raison sociale ou marque déposée, l'adresse à laquelle ils peuvent être contactés;

▼B

c) mettent en place un système de gestion de la qualité conforme à l'article 17;

d) assurent la conservation de la documentation visée à l'article 18;

e) assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, lorsque ces journaux se trouvent sous leur contrôle, conformément à l'article 19;

f) veillent à ce que le système d'IA à haut risque soit soumis à la procédure d'évaluation de la conformité applicable visée à l'article 43, avant sa mise sur le marché ou sa mise en service;

g) élaborent une déclaration UE de conformité conformément à l'article 47;

h) apposent le marquage CE sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur son emballage ou dans la documentation l'accompagnant, selon le cas, afin d'indiquer la conformité avec le présent règlement, conformément à l'article 48;

i) respectent les obligations en matière d'enregistrement prévues à l'article 49, paragraphe 1;

j) prennent les mesures correctives nécessaires et fournissent les informations requises à l'article 20;

k) à la demande motivée d'une autorité nationale compétente, prouvent la conformité du système d'IA à haut risque avec les exigences énoncées à la section 2;

l) veillent à ce que le système d'IA à haut risque soit conforme aux exigences en matière d'accessibilité conformément aux directives (UE) 2016/2102 et (UE) 2019/882.

Article 17

Système de gestion de la qualité

1. Les fournisseurs de systèmes d'IA à haut risque mettent en place un système de gestion de la qualité garantissant le respect du présent règlement. Ce système est documenté de manière méthodique et ordonnée sous la forme de politiques, de procédures et d'instructions écrites, et comprend au moins les aspects suivants:

a) une stratégie de respect de la réglementation, notamment le respect des procédures d'évaluation de la conformité et des procédures de gestion des modifications apportées aux systèmes d'IA à haut risque;

b) des techniques, procédures et actions systématiques destinées à la conception des systèmes d'IA à haut risque ainsi qu'au contrôle et à la vérification de cette conception;

c) des techniques, procédures et actions systématiques destinées au développement des systèmes d'IA à haut risque ainsi qu'au contrôle et à l'assurance de leur qualité;

d) des procédures d'examen, de test et de validation à exécuter avant, pendant et après le développement du système d'IA à haut risque, ainsi que la fréquence à laquelle elles doivent être réalisées;

▼B

e) des spécifications techniques, notamment des normes, à appliquer et, lorsque les normes harmonisées pertinentes ne sont pas appliquées intégralement, ou ne couvrent pas toutes les exigences pertinentes énoncées à la section 2, les moyens à utiliser pour faire en sorte que le système d'IA à haut risque satisfasse auxdites exigences;

f) les systèmes et procédures de gestion des données, notamment l'acquisition, la collecte, l'analyse, l'étiquetage, le stockage, la filtration, l'exploration, l'agrégation, la conservation des données et toute autre opération concernant les données qui est effectuée avant la mise sur le marché ou la mise en service de systèmes d'IA à haut risque et aux fins de celles-ci;

g) le système de gestion des risques prévu à l'article 9;

h) l'élaboration, la mise en œuvre et le fonctionnement d'un système de surveillance après commercialisation conformément à l'article 72;

i) les procédures relatives au signalement d'un incident grave conformément à l'article 73;

j) la gestion des communications avec les autorités nationales compétentes, les autres autorités compétentes, y compris celles fournissant ou facilitant l'accès aux données, les organismes notifiés, les autres opérateurs, les clients ou d'autres parties intéressées;

k) les systèmes et procédures de conservation de tous les documents et informations pertinents;

l) la gestion des ressources, y compris les mesures liées à la sécurité d'approvisionnement;

m) un cadre de responsabilisation définissant les responsabilités de l'encadrement et des autres membres du personnel en ce qui concerne tous les aspects énumérés dans le présent paragraphe.

2. La mise en œuvre des aspects visés au paragraphe 1 est proportionnée à la taille de l'organisation du fournisseur. Les fournisseurs respectent, en tout état de cause, le degré de rigueur et le niveau de protection requis afin de garantir que leurs systèmes d'IA à haut risque sont conformes au présent règlement.

3. Les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des obligations relatives aux systèmes de gestion de la qualité, ou liées à l'exercice d'une fonction équivalente en vertu de la législation sectorielle pertinente de l'Union peuvent inclure les aspects énumérés au paragraphe 1 dans les systèmes de gestion de la qualité conformément à ladite législation.

4. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, la conformité avec les règles relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues dans la législation pertinente de l'Union sur les services financiers vaut respect de l'obligation de mettre en place un système de gestion de la qualité, à l'exception du paragraphe 1, points g), h) et i) du présent article. À cette fin, toute norme harmonisée visée à l'article 40 est prise en considération.

▼B

Article 18

Conservation des documents

1. Pendant une période prenant fin 10 ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, le fournisseur tient à la disposition des autorités nationales compétentes:

a) la documentation technique visée à l'article 11;

b) la documentation concernant le système de gestion de la qualité visé à l'article 17;

c) la documentation concernant les modifications approuvées par les organismes notifiés, le cas échéant;

d) les décisions et autres documents émis par les organismes notifiés, le cas échéant;

e) la déclaration UE de conformité visée à l'article 47.

2. Chaque État membre détermine les conditions dans lesquelles la documentation visée au paragraphe 1 reste à la disposition des autorités nationales compétentes pendant la période indiquée audit paragraphe dans le cas où un fournisseur ou son mandataire établi sur son territoire fait faillite ou met un terme à ses activités avant la fin de cette période.

3. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour la documentation technique dans le cadre de la documentation conservée en vertu de la législation pertinente de l'Union sur les services financiers.

Article 19

Journaux générés automatiquement

1. Les fournisseurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous leur contrôle. Sans préjudice du droit de l'Union ou du droit national applicable, les journaux sont conservés pendant une période adaptée à la destination du système d'IA à haut risque, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.

2. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour les journaux générés automatiquement par leurs systèmes d'IA à haut risque dans le cadre de la documentation conservée en vertu de la législation pertinente sur les services financiers.

Article 20

Mesures corrective et devoir d'information

1. Les fournisseurs de systèmes d'IA à haut risque qui considèrent ou ont des raisons de considérer qu'un système d'IA à haut risque qu'ils ont mis sur le marché ou mis en service n'est pas conforme au présent règlement prennent immédiatement les mesures correctives

▼B

nécessaires pour le mettre en conformité, le retirer, le désactiver ou le rappeler, selon le cas. Ils informent les distributeurs du système d'IA à haut risque concerné et, le cas échéant, les déployeurs, le mandataire et les importateurs en conséquence.

2. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, et que le fournisseur prend conscience de ce risque, celui-ci recherche immédiatement les causes, en collaboration avec le déployeur à l'origine du signalement, le cas échéant, et informe les autorités de surveillance du marché compétentes pour le système d'IA à haut risque concerné et, le cas échéant, l'organisme notifié qui a délivré un certificat pour ce système d'IA à haut risque, conformément à l'article 44, en précisant en particulier la nature du cas de non-conformité et les éventuelles mesures correctives pertinentes prises.

Article 21

Coopération avec les autorités compétentes

1. À la demande motivée d'une autorité compétente, les fournisseurs de systèmes d'IA à haut risque fournissent à ladite autorité toutes les informations et tous les documents nécessaires pour démontrer la conformité du système d'IA à haut risque avec les exigences énoncées à la section 2, dans une langue aisément compréhensible par l'autorité dans l'une des langues officielles des institutions de l'Union, telle qu'indiquée par l'État membre concerné.

2. À la demande motivée d'une autorité compétente, les fournisseurs accordent également à l'autorité compétente à l'origine de la demande, le cas échéant, l'accès aux journaux générés automatiquement par le système d'IA à haut risque visés à l'article 12, paragraphe 1, dans la mesure où ces journaux sont sous leur contrôle.

3. Les informations obtenues par une autorité compétente en application du présent article sont traitées conformément aux obligations de confidentialité énoncées à l'article 78.

Article 22

Mandataires des fournisseurs de systèmes d'IA à haut risque

1. Avant de mettre leurs systèmes d'IA à haut risque à disposition sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le fournisseur autorise son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.

3. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Il fournit une copie du mandat aux autorités de surveillance du marché à leur demande, dans l'une des langues officielles des institutions de l'Union, indiquée par l'autorité compétente. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter les tâches suivantes:

a) vérifier que la déclaration UE de conformité visée à l'article 47 et la documentation technique visée à l'article 11 ont été établies et que le fournisseur a suivi une procédure appropriée d'évaluation de la conformité;

▼B

b) tenir à la disposition des autorités compétentes et des autorités ou organismes nationaux visés à l'article 74, paragraphe 10, pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les coordonnées du fournisseur ayant désigné le mandataire, une copie de la déclaration UE de conformité visée à l'article 47, la documentation technique et, le cas échéant, le certificat délivré par l'organisme notifié;

c) à la demande motivée d'une autorité compétente, communiquer à cette dernière toutes les informations et tous les documents, y compris ceux visés au point b) du présent alinéa, nécessaires pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, et notamment lui donner accès aux journaux générés automatiquement par le système d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous le contrôle du fournisseur;

d) à la demande motivée des autorités compétentes, coopérer avec elles à toute mesure prise par ces dernières à l'égard du système d'IA à haut risque, en particulier pour réduire et atténuer les risques posés par le système d'IA à haut risque;

e) le cas échéant, respecter les obligations en matière d'enregistrement visées à l'article 49, paragraphe 1, ou, si l'enregistrement est effectué par le fournisseur lui-même, vérifier que les informations visées à l'annexe VIII, section A, point 3, sont correctes.

Le mandat habilite le mandataire à servir d'interlocuteur, en plus ou à la place du fournisseur, aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.

4. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent en vertu du présent règlement. Dans ce cas, il informe immédiatement l'autorité de surveillance du marché concernée et, selon le cas, l'organisme notifié pertinent de la cessation du mandat et des motifs qui la sous-tendent.

Article 23

Obligations des importateurs

1. Avant de mettre sur le marché un système d'IA à haut risque, les importateurs s'assurent que le système est conforme au présent règlement en vérifiant que:

a) le fournisseur du système d'IA à haut risque a suivi la procédure pertinente d'évaluation de la conformité visée à l'article 43;

b) le fournisseur a établi la documentation technique conformément à l'article 11 et à l'annexe IV;

c) le système porte le marquage CE requis et est accompagné de la déclaration UE de conformité visée à l'article 47 et de la notice d'utilisation;

d) le fournisseur a désigné un mandataire conformément à l'article 22, paragraphe 1.

▼B

2. Lorsqu'un importateur a des raisons suffisantes de considérer qu'un système d'IA à haut risque n'est pas conforme au présent règlement, ou a été falsifié ou s'accompagne de documents falsifiés, il ne met le système sur le marché qu'après sa mise en conformité. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, l'importateur en informe le fournisseur du système, les mandataires et les autorités de surveillance du marché.

3. Les importateurs indiquent leur nom, raison sociale ou marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés, sur le système d'IA à haut risque et sur son emballage ou dans la documentation l'accompagnant, selon le cas.

4. Les importateurs s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport, le cas échéant, ne compromettent pas sa conformité avec les exigences énoncées à la section 2.

5. Pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les importateurs conservent une copie du certificat délivré par l'organisme notifié, selon le cas, de la notice d'utilisation et de la déclaration UE de conformité visée à l'article 47.

6. À la demande motivée des autorités compétentes concernées, les importateurs communiquent à ces dernières toutes les informations et tous les documents nécessaires, y compris ceux visés au paragraphe 5, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, dans une langue aisément compréhensible par les autorités nationales compétentes. À cette fin, ils veillent également à ce que la documentation technique puisse être mise à la disposition de ces autorités.

7. Les importateurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un système d'IA à haut risque mis sur le marché par les importateurs, en particulier pour réduire et atténuer les risques qu'il présente.

Article 24

Obligations des distributeurs

1. Avant de mettre un système d'IA à haut risque à disposition sur le marché, les distributeurs vérifient qu'il porte le marquage CE requis, qu'il est accompagné d'une copie de la déclaration UE de conformité visée à l'article 47 et de la notice d'utilisation, et que le fournisseur et l'importateur dudit système, selon le cas, ont respecté leurs obligations respectives en vertu de l'article 16, points b) et c), et de l'article 23, paragraphe 3.

2. Lorsqu'un distributeur considère ou a des raisons de considérer, sur la base des informations en sa possession, qu'un système d'IA à haut risque n'est pas conforme aux exigences énoncées à la section 2, il ne met le système à disposition sur le marché qu'après la mise en conformité de celui-ci avec lesdites exigences. De plus, lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, le distributeur en informe le fournisseur ou l'importateur du système, selon le cas.

▼B

3. Les distributeurs s'assurent, lorsqu'un système d'IA à haut risque est sous leur responsabilité, que les conditions de stockage ou de transport, le cas échéant, ne compromettent pas sa conformité avec les exigences énoncées à la section 2.

4. Lorsqu'un distributeur considère ou a des raisons de considérer, sur la base des informations en sa possession, qu'un système d'IA à haut risque qu'il a mis à disposition sur le marché n'est pas conforme aux exigences énoncées à la section 2, il prend les mesures correctives nécessaires pour mettre ce système en conformité avec lesdites exigences, le retirer ou le rappeler ou veille à ce que le fournisseur, l'importateur ou tout opérateur concerné, selon le cas, prenne ces mesures correctives. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 79, paragraphe 1, le distributeur en informe immédiatement le fournisseur ou l'importateur du système ainsi que les autorités compétentes pour le système d'IA à haut risque concerné et précise, notamment, le cas de non-conformité et les éventuelles mesures correctives prises.

5. À la demande motivée d'une autorité compétente concernée, les distributeurs d'un système d'IA à haut risque communiquent à cette autorité toutes les informations et tous les documents concernant les mesures qu'ils ont prises en vertu des paragraphes 1 à 4, nécessaires pour démontrer la conformité de ce système avec les exigences énoncées à la section 2.

6. Les distributeurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard d'un système d'IA à haut risque mis à disposition sur le marché par les distributeurs, en particulier pour réduire et atténuer les risques qu'il présente.

Article 25

Responsabilités tout au long de la chaîne de valeur de l'IA

1. Tout distributeur, importateur, déployeur ou autre tiers est considéré comme un fournisseur d'un système d'IA à haut risque aux fins du présent règlement et est soumis aux obligations incombant au fournisseur au titre de l'article 16 dans toutes les circonstances suivantes:

a) il commercialise sous son propre nom ou sa propre marque un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles prévoyant une autre répartition des obligations;

b) il apporte une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service de telle manière qu'il reste un système d'IA à haut risque en application de l'article 6;

c) il modifie la destination d'un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé à haut risque et a déjà été mis sur le marché ou mis en service de telle manière que le système d'IA concerné devient un système d'IA à haut risque conformément l'article 6.

2. Lorsque les circonstances visées au paragraphe 1, se produisent, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA n'est plus considéré comme un fournisseur de ce système d'IA spécifique aux fins du présent règlement. Ce fournisseur initial coopère étroitement avec les nouveaux fournisseurs et met à disposition

▼B

les informations nécessaires et fournit l'accès technique raisonnablement attendu et toute autre assistance nécessaire au respect des obligations énoncées dans le présent règlement, en particulier en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque. Le présent paragraphe ne s'applique pas dans les cas où le fournisseur initial a clairement précisé que son système d'IA ne doit pas être transformé en un système d'IA à haut risque et ne relève donc pas de l'obligation relative à la remise de la documentation.

3. Lorsque des systèmes d'IA à haut risque constituent des composants de sécurité de produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, le fabricant de ces produits est considéré comme étant le fournisseur du système d'IA à haut risque et est soumis aux obligations visées à l'article 16 dans l'un des deux cas suivants:

a) le système d'IA à haut risque est mis sur le marché avec le produit sous le nom ou la marque du fabricant du produit;

b) le système d'IA à haut risque est mis en service sous le nom ou la marque du fabricant du produit après que le produit a été mis sur le marché.

4. Le fournisseur d'un système d'IA à haut risque et le tiers qui fournit un système d'IA, des outils, services, composants ou processus qui sont utilisés ou intégrés dans un système d'IA à haut risque précisent, par accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaire, sur la base de l'état de la technique généralement reconnu, pour permettre au fournisseur du système d'IA à haut risque de se conformer pleinement aux obligations prévues dans le présent règlement. Le présent paragraphe ne s'applique pas aux tiers qui rendent accessibles au public des outils, services, processus ou composants, autres que des modèles d'IA à usage général, dans le cadre d'une licence libre et ouverte.

Le Bureau de l'IA peut élaborer et recommander des clauses types volontaires pour les contrats entre les fournisseurs de systèmes d'IA à haut risque et les tiers qui fournissent des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans les systèmes d'IA à haut risque. Lorsqu'il élabore des clauses types volontaires, le Bureau de l'IA tient compte des éventuelles exigences contractuelles applicables dans des secteurs ou des activités spécifiques. Les clauses types volontaires sont publiées et mises à disposition gratuitement dans un format électronique facile d'utilisation.

5. Les paragraphes 2 et 3 sont sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle, les informations confidentielles de nature commerciale et les secrets d'affaires conformément au droit de l'Union et au droit national.

Article 26

Obligations incombant aux déployeurs de systèmes d'IA à haut risque

1. Les déployeurs de systèmes d'IA à haut risque prennent des mesures techniques et organisationnelles appropriées afin de garantir qu'ils utilisent ces systèmes conformément aux notices d'utilisation accompagnant les systèmes, conformément aux paragraphes 3 et 6.

▼B

2. Les déployeurs confient le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires ainsi que du soutien nécessaire.

3. Les obligations énoncées aux paragraphes 1 et 2 sont sans préjudice des autres obligations du déployeur prévues par le droit de l'Union ou le droit national et de la faculté du déployeur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de contrôle humain indiquées par le fournisseur.

4. Sans préjudice des paragraphes 1 et 2, pour autant que le déployeur exerce un contrôle sur les données d'entrée, il veille à ce que ces dernières soient pertinentes et suffisamment représentatives au regard de la destination du système d'IA à haut risque.

5. Les déployeurs surveillent le fonctionnement du système d'IA à haut risque sur la base de la notice d'utilisation et, le cas échéant, informent les fournisseurs conformément à l'article 72. Lorsque les déployeurs ont des raisons de considérer que l'utilisation du système d'IA à haut risque conformément à la notice d'utilisation pourrait conduire à ce que le système d'IA présente un risque au sens de l'article 79, paragraphe 1, ils en informent, sans retard injustifié, le fournisseur ou le distributeur ainsi que l'autorité de surveillance du marché concernée, et suspendent l'utilisation de ce système. Lorsque les déployeurs ont détecté un incident grave, ils informent également immédiatement d'abord le fournisseur, puis l'importateur ou le distributeur et les autorités de surveillance du marché concernées de cet incident. Si le déployeur n'est pas en mesure de joindre le fournisseur, l'article 73 s'applique mutatis mutandis. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs de systèmes d'IA qui sont des autorités répressives.

Si les déployeurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, la conformité avec les règles relatives à la gouvernance, aux dispositifs, aux processus et aux mécanismes internes prévues dans la législation sur les services financiers vaut respect de l'obligation de surveillance énoncée au premier alinéa.

6. Les déployeurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par ce système d'IA à haut risque dans la mesure où ces journaux se trouvent sous leur contrôle, pendant une période adaptée à la destination du système d'IA à haut risque, d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicable, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.

Si les déployeurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs ou à leurs processus internes prévues par la législation de l'Union sur les services financiers, ils tiennent à jour les journaux dans le cadre de la documentation conservée en vertu de la législation pertinente de l'Union sur les services financiers.

7. Avant de mettre en service ou d'utiliser un système d'IA à haut risque sur le lieu de travail, les déployeurs qui sont des employeurs informent les représentants des travailleurs et les travailleurs concernés qu'ils seront soumis à l'utilisation du système d'IA à haut risque. Ces informations sont fournies, le cas échéant, conformément aux règles et procédures prévues par le droit de l'Union et le droit national et aux pratiques en matière d'information des travailleurs et de leurs représentants.

▼B

8. Les déployeurs de systèmes d'IA à haut risque qui sont des autorités publiques ou des institutions, organes ou organismes de l'Union, respectent les obligations en matière d'enregistrement prévues à l'article 49. Dans le cas où ces déployeurs constatent que le système d'IA à haut risque qu'ils envisagent d'utiliser n'a pas été enregistré dans la base de données de l'UE visée à l'article 71, ils n'utilisent pas ce système et informent le fournisseur ou le distributeur.

9. Le cas échéant, les déployeurs de systèmes d'IA à haut risque utilisent les informations fournies en application de l'article 13 du présent règlement pour se conformer à leur obligation de procéder à une analyse d'impact relative à la protection des données en vertu de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680.

10. Sans préjudice de la directive (UE) 2016/680, dans le cadre d'une enquête en vue de la recherche ciblée d'une personne soupçonnée d'avoir commis une infraction pénale ou condamnée pour avoir commis une infraction pénale, le déployeur d'un système d'IA à haut risque pour l'identification biométrique à distance a posteriori demande l'autorisation, ex ante ou sans retard injustifié et au plus tard dans les 48 heures, d'une autorité judiciaire ou administrative dont la décision est contraignante et soumise à un contrôle juridictionnel, pour l'utilisation de ce système, sauf lorsqu'il est utilisé pour l'identification initiale d'un suspect potentiel sur la base de faits objectifs et vérifiables directement liés à l'infraction. Chaque utilisation est limitée à ce qui est strictement nécessaire pour enquêter sur une infraction pénale spécifique.

Si l'autorisation demandée en application du premier alinéa est rejetée, l'utilisation du système d'identification biométrique à distance a posteriori lié à l'autorisation demandée est interrompue avec effet immédiat et les données à caractère personnel liées à l'utilisation du système d'IA à haut risque pour lequel l'autorisation a été demandée sont supprimées.

En aucun cas, ce système d'IA à haut risque pour l'identification biométrique à distance a posteriori ne peut être utilisé à des fins répressives de manière non ciblée, sans aucun lien avec une infraction pénale, une procédure pénale, une menace réelle et actuelle ou réelle et prévisible d'une infraction pénale, ou la recherche d'une personne disparue spécifique. Il convient d'assurer qu'aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne puisse être prise par les autorités répressives sur la seule base des sorties de tels systèmes d'identification biométrique à distance a posteriori.

Le présent paragraphe est sans préjudice de l'article 9 du règlement (UE) 2016/679 et de l'article 10 de la directive (UE) 2016/680 pour le traitement des données biométriques.

Indépendamment de la finalité ou du déployeur, chaque utilisation de ces systèmes d'IA à haut risque est documentée dans le dossier de police pertinent et est mise à la disposition de l'autorité de surveillance du marché concernée et de l'autorité nationale chargée de la protection des données sur demande, à l'exclusion de la divulgation de données opérationnelles sensibles liées aux services répressifs. Le présent alinéa est sans préjudice des pouvoirs conférés par la directive (UE) 2016/680 aux autorités de contrôle.

Les déployeurs soumettent aux autorités de surveillance du marché concernées et aux autorités nationales chargées de la protection des données des rapports annuels sur leur utilisation de systèmes d'identification biométrique à distance a posteriori, à l'exclusion de la divulgation de données opérationnelles sensibles liées aux services répressifs. Les rapports peuvent être agrégés pour couvrir plus d'un déploiement.

▼B

Les États membres peuvent adopter, conformément au droit de l'Union, des lois plus restrictives sur l'utilisation de systèmes d'identification biométrique à distance a posteriori.

11. Sans préjudice de l'article 50 du présent règlement, les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, qui prennent des décisions ou facilitent les prises de décision concernant des personnes physiques, informent lesdites personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque. Pour les systèmes d'IA à haut risque utilisés à des fins répressives, l'article 13 de la directive (UE) 2016/680 s'applique.

12. Les déployeurs coopèrent avec les autorités compétentes concernées à toute mesure prise par ces autorités à l'égard du système d'IA à haut risque en vue de mettre en œuvre le présent règlement.

Article 27

Analyse d'impact des systèmes d'IA à haut risque sur les droits fondamentaux

1. Avant le déploiement d'un système d'IA à haut risque visé à l'article 6, paragraphe 2, à l'exception des systèmes d'IA à haut risque destinés à être utilisés dans le domaine visé à l'annexe III, point 2, les déployeurs qui sont des organismes de droit public ou des entités privées fournissant des services publics et les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, points 5), b) et c), effectuent une analyse de l'impact sur les droits fondamentaux que l'utilisation de ce système peut produire. À cette fin, les déployeurs effectuent une analyse comprenant:

a) une description des processus du déployeur dans lesquels le système d'IA à haut risque sera utilisé conformément à sa destination;

b) une description de la période pendant laquelle et de la fréquence à laquelle chaque système d'IA à haut risque est destiné à être utilisé;

c) les catégories de personnes physiques et les groupes susceptibles d'être concernés par son utilisation dans le contexte spécifique;

d) les risques spécifiques de préjudice susceptibles d'avoir une incidence sur les catégories de personnes physiques ou groupes de personnes identifiés en vertu du point c) du présent paragraphe, compte tenu des informations fournies par le fournisseur conformément à l'article 13;

e) une description de la mise en œuvre des mesures de contrôle humain, conformément à la notice d'utilisation;

f) les mesures à prendre en cas de matérialisation de ces risques, y compris les dispositifs relatifs à la gouvernance interne et aux mécanismes de plainte internes.

2. L'obligation établie au paragraphe 1 s'applique à la première utilisation du système d'IA à haut risque. Le déployeur peut, dans des cas similaires, s'appuyer sur des analyses d'impact sur les droits fondamentaux effectuées précédemment ou sur des analyses d'impact existantes réalisées par le fournisseur. Si, au cours de l'utilisation du système d'IA à haut risque, le déployeur estime qu'un des éléments énumérés au paragraphe 1 a changé ou n'est plus à jour, il prend les mesures nécessaires pour mettre à jour les informations.

▼B

3. Une fois l'analyse visée au paragraphe 1 du présent article effectuée, le déployeur en notifie les résultats à l'autorité de surveillance du marché, et soumet le modèle visé au paragraphe 5 du présent article, rempli, dans le cadre de la notification. Dans le cas visé à l'article 46, paragraphe 1, les déployeurs peuvent être exemptés de cette obligation de notification.

4. Si l'une des obligations prévues au présent article est déjà remplie au moyen de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, l'analyse d'impact sur les droits fondamentaux visée au paragraphe 1 du présent article complète ladite analyse d'impact relative à la protection des données.

5. Le Bureau de l'IA élabore un modèle de questionnaire, y compris au moyen d'un outil automatisé, afin d'aider les déployeurs à se conformer de manière simplifiée aux obligations qui leur incombent en vertu du présent article.

SECTION 4

Autorités notifiantes et organismes notifiés

Article 28

Autorités notifiantes

1. Chaque État membre désigne ou établit au moins une autorité notifiante chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle. Ces procédures sont élaborées en coopération entre les autorités notifiantes de tous les États membres.

2. Les États membres peuvent décider que l'évaluation et le contrôle visés au paragraphe 1 doivent être effectués par un organisme national d'accréditation au sens du règlement (CE) n° 765/2008 et conformément à ses dispositions.

3. Les autorités notifiantes sont établies, organisées et gérées de manière à éviter tout conflit d'intérêts avec les organismes d'évaluation de la conformité et à garantir l'objectivité et l'impartialité de leurs activités.

4. Les autorités notifiantes sont organisées de telle sorte que les décisions concernant la notification des organismes d'évaluation de la conformité soient prises par des personnes compétentes différentes de celles qui ont réalisé l'évaluation de ces organismes.

5. Les autorités notifiantes ne proposent ni ne fournissent aucune des activités réalisées par les organismes d'évaluation de la conformité, ni aucun service de conseil sur une base commerciale ou concurrentielle.

6. Les autorités notifiantes garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78.

▼B

7. Les autorités notifiantes disposent d'un personnel compétent en nombre suffisant pour la bonne exécution de leurs tâches. Le personnel compétent possède l'expertise nécessaire, le cas échéant, pour sa fonction, dans des domaines tels que les technologies de l'information, l'IA et le droit, y compris le contrôle du respect des droits fondamentaux.

Article 29

Demande de notification d'un organisme d'évaluation de la conformité

1. Les organismes d'évaluation de la conformité soumettent une demande de notification à l'autorité notifiante de l'État membre dans lequel ils sont établis.

2. La demande de notification est accompagnée d'une description des activités d'évaluation de la conformité, du ou des modules d'évaluation de la conformité et des types de systèmes d'IA pour lesquels l'organisme d'évaluation de la conformité se déclare compétent, ainsi que d'un certificat d'accréditation, lorsqu'il existe, délivré par un organisme national d'accréditation qui atteste que l'organisme d'évaluation de la conformité remplit les exigences énoncées à l'article 31.

Tout document en cours de validité relatif à des désignations existantes de l'organisme notifié demandeur en vertu de toute autre législation d'harmonisation de l'Union est ajouté.

3. Lorsque l'organisme d'évaluation de la conformité ne peut pas produire de certificat d'accréditation, il présente à l'autorité notifiante toutes les preuves documentaires nécessaires à la vérification, à la reconnaissance et au contrôle régulier de sa conformité avec les exigences définies à l'article 31.

4. Quant aux organismes notifiés désignés en vertu de toute autre législation d'harmonisation de l'Union, tous les documents et certificats liés à ces désignations peuvent être utilisés à l'appui de leur procédure de désignation au titre du présent règlement, le cas échéant. L'organisme notifié met à jour la documentation visée aux paragraphes 2 et 3 du présent article dès que des changements pertinents interviennent afin de permettre à l'autorité responsable des organismes notifiés de contrôler et de vérifier que toutes les exigences énoncées à l'article 31 demeurent observées.

Article 30

Procédure de notification

1. Les autorités notifiantes ne peuvent notifier que les organismes d'évaluation de la conformité qui ont satisfait aux exigences énoncées à l'article 31.

2. Les autorités notifiantes informent la Commission et les autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission quant à chaque organisme d'évaluation de la conformité visé au paragraphe 1.

▼B

3. La notification visée au paragraphe 2 du présent article comprend des informations complètes sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et les types de systèmes d'IA concernés, ainsi que l'attestation de compétence correspondante. Lorsqu'une notification n'est pas fondée sur le certificat d'accréditation visé à l'article 29, paragraphe 2, l'autorité notifiante fournit à la Commission et aux autres États membres les preuves documentaires attestant de la compétence de l'organisme d'évaluation de la conformité et des dispositions prises pour faire en sorte que cet organisme soit régulièrement contrôlé et continue à satisfaire aux exigences énoncées à l'article 31.

4. L'organisme d'évaluation de la conformité concerné ne peut effectuer les activités propres à un organisme notifié que si aucune objection n'est émise par la Commission ou les autres États membres dans les deux semaines suivant la notification par une autorité notifiante, si cette notification comprend le certificat d'accréditation visé à l'article 29, paragraphe 2, ou dans les deux mois suivant la notification par une autorité notifiante si cette notification comprend les preuves documentaires visées à l'article 29, paragraphe 3.

5. En cas d'objections, la Commission entame sans tarder des consultations avec les États membres et l'organisme d'évaluation de la conformité concernés. Au vu de ces consultations, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre et à l'organisme d'évaluation de la conformité concernés.

Article 31

Exigences concernant les organismes notifiés

1. Un organisme notifié est constitué en vertu du droit national d'un État membre et a la personnalité juridique.

2. Les organismes notifiés se conforment aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de procédures qui sont nécessaires à l'exécution de leurs tâches, ainsi qu'aux exigences appropriées en matière de cybersécurité.

3. La structure organisationnelle, la répartition des responsabilités, les liens hiérarchiques et le fonctionnement des organismes notifiés garantissent la confiance dans leurs activités et la fiabilité des résultats des activités d'évaluation de la conformité menées par les organismes notifiés.

4. Les organismes notifiés sont indépendants du fournisseur du système d'IA à haut risque pour lequel ils mènent les activités d'évaluation de la conformité. Les organismes notifiés sont également indépendants de tout autre opérateur ayant un intérêt économique dans les systèmes d'IA à haut risque qui font l'objet de l'évaluation, ainsi que de tout concurrent du fournisseur. Cela n'exclut pas l'utilisation de systèmes d'IA à haut risque évalués qui sont nécessaires au fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces systèmes d'IA à haut risque à des fins personnelles.

5. L'organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter ses tâches d'évaluation de la conformité ne participent pas directement à la conception, au développement,

▼B

à la commercialisation ou à l'utilisation de systèmes d'IA à haut risque, pas plus qu'ils ne représentent les parties engagées dans ces activités. Ils n'exercent aucune activité susceptible d'entrer en conflit avec leur indépendance de jugement ou leur intégrité en ce qui concerne les activités d'évaluation de la conformité pour lesquelles ils sont notifiés. Cela s'applique en particulier aux services de conseil.

6. Les organismes notifiés sont organisés et fonctionnent de façon à garantir l'indépendance, l'objectivité et l'impartialité de leurs activités. Les organismes notifiés documentent et appliquent une structure et des procédures visant à garantir l'impartialité et à encourager et appliquer les principes d'impartialité dans l'ensemble de leur organisation, du personnel et des activités d'évaluation.

7. Les organismes notifiés disposent de procédures documentées pour veiller à ce que leur personnel, leurs comités, leurs filiales, leurs sous-traitants et tout organisme associé ou le personnel d'organismes externes préservent, conformément à l'article 78, la confidentialité des informations auxquelles ils accèdent durant l'exercice de leurs activités d'évaluation de la conformité, sauf lorsque leur divulgation est requise par la loi. Le personnel des organismes notifiés est lié par le secret professionnel pour toutes les informations dont il a connaissance dans l'exercice de ses fonctions au titre du présent règlement, sauf à l'égard des autorités notifiantes de l'État membre où il exerce ses activités.

8. Les organismes notifiés disposent de procédures pour accomplir leurs activités qui tiennent dûment compte de la taille des fournisseurs, du secteur dans lequel ils exercent leurs activités, de leur structure et du degré de complexité du système d'IA concerné.

9. Les organismes notifiés souscrivent, pour leurs activités d'évaluation de la conformité, une assurance de responsabilité civile appropriée à moins que cette responsabilité ne soit couverte par l'État membre dans lequel ils sont établis sur la base du droit national ou que l'État membre soit lui-même responsable de l'évaluation de la conformité.

10. Les organismes notifiés sont en mesure d'accomplir toutes leurs tâches au titre du présent règlement avec la plus haute intégrité professionnelle et la compétence requise dans le domaine spécifique, qu'ils exécutent eux-mêmes ces tâches ou que celles-ci soient exécutées pour leur compte et sous leur responsabilité.

11. Les organismes notifiés disposent de compétences internes suffisantes pour pouvoir évaluer efficacement les tâches effectuées pour leur compte par des parties extérieures. L'organisme notifié dispose en permanence d'un personnel administratif, technique, juridique et scientifique en nombre suffisant et doté d'une expérience et de connaissances liées aux données, au traitement des données et aux types de systèmes d'IA en cause et aux exigences énoncées à la section 2.

12. Les organismes notifiés prennent part aux activités de coordination visées à l'article 38. Ils participent également, directement ou par l'intermédiaire d'un représentant, aux activités des organisations européennes de normalisation, ou font en sorte de se tenir informés des normes applicables et de leur état.

▼B

Article 32

Présomption de conformité avec les exigences concernant les organismes notifiés

Lorsqu'un organisme d'évaluation de la conformité démontre sa conformité avec les critères énoncés dans les normes harmonisées concernées, ou dans des parties de ces normes, dont les références ont été publiées au *Journal officiel de l'Union européenne*, il est présumé répondre aux exigences énoncées à l'article 31 dans la mesure où les normes harmonisées applicables couvrent ces exigences.

Article 33

Filiales des organismes notifiés et sous-traitance

1. Lorsqu'un organisme notifié sous-traite des tâches spécifiques dans le cadre de l'évaluation de la conformité ou a recours à une filiale, il s'assure que le sous-traitant ou la filiale répond aux exigences fixées à l'article 31 et en informe l'autorité notifiante.

2. Les organismes notifiés assument l'entière responsabilité des tâches effectuées par tout sous-traitants ou toute filiale.

3. Des activités ne peuvent être sous-traitées ou réalisées par une filiale qu'avec l'accord du fournisseur. Les organismes notifiés rendent publique une liste de leurs filiales.

4. Les documents pertinents concernant l'évaluation des qualifications du sous-traitant ou de la filiale et le travail exécuté par celui-ci ou celle-ci en vertu du présent règlement sont tenus à la disposition de l'autorité notifiante pendant une période de cinq ans à compter de la date de cessation de la sous-traitance.

Article 34

Obligations opérationnelles des organismes notifiés

1. Les organismes notifiés vérifient la conformité du système d'IA à haut risque conformément aux procédures d'évaluation de la conformité visées à l'article 43.

2. Les organismes notifiés évitent les charges inutiles pour les fournisseurs dans l'exercice de leurs activités et tiennent dûment compte de la taille du fournisseur, du secteur dans lequel il exerce ses activités, de sa structure et du degré de complexité du système d'IA à haut risque concerné, en particulier en vue de réduire au minimum les charges administratives et les coûts de mise en conformité pour les microentreprises et les petites entreprises au sens de la recommandation 2003/361/CE. L'organisme notifié respecte néanmoins le degré de rigueur et le niveau de protection requis afin de garantir la conformité du système d'IA à haut risque avec les exigences du présent règlement.

▼B

3. Les organismes notifiés mettent à la disposition de l'autorité notifiante visée à l'article 28 et lui soumettent sur demande toute la documentation pertinente, y compris celle des fournisseurs, afin de permettre à cette autorité de réaliser ses activités d'évaluation, de désignation, de notification et de surveillance et pour faciliter les évaluations décrites à la présente section.

Article 35

Numéros d'identification et listes des organismes notifiés

1. La Commission attribue un numéro d'identification unique à chaque organisme notifié, même lorsqu'un organisme est notifié au titre de plus d'un acte de l'Union.

2. La Commission rend publique la liste des organismes notifiés au titre du présent règlement et y mentionne leurs numéros d'identification et les activités pour lesquelles ils ont été notifiés. La Commission veille à ce que cette liste soit tenue à jour.

Article 36

Modifications apportées aux notifications

1. L'autorité notifiante notifie à la Commission et aux autres États membres toute modification pertinente apportée à la notification d'un organisme notifié au moyen de l'outil de notification électronique visé à l'article 30, paragraphe 2.

2. Les procédures établies aux articles 29 et 30 s'appliquent en cas d'extension de la portée de la notification.

En cas de modification de la notification autre qu'une extension de sa portée, les procédures prévues aux paragraphes 3 à 9 s'appliquent.

3. Lorsqu'un organisme notifié décide de cesser ses activités d'évaluation de la conformité, il informe l'autorité notifiante et les fournisseurs concernés dès que possible et, dans le cas d'un arrêt prévu de ses activités, au moins un an avant de mettre un terme à ses activités. Les certificats de l'organisme notifié peuvent rester valables pendant une période de neuf mois après l'arrêt des activités de l'organisme notifié, à condition qu'un autre organisme notifié confirme par écrit qu'il assumera la responsabilité des systèmes d'IA à haut risque concernés par ces certificats. Cet autre organisme notifié procède à une évaluation complète des systèmes d'IA à haut risque concernés avant la fin de cette période de neuf mois, avant de délivrer de nouveaux certificats pour les systèmes en question. Lorsque l'organisme notifié a mis un terme à ses activités, l'autorité notifiante retire la désignation.

4. Lorsqu'une autorité notifiante a des raisons suffisantes de considérer qu'un organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, l'autorité notifiante procède sans retard à une enquête avec la plus grande diligence. Dans ce contexte, elle informe l'organisme notifié concerné des

▼B

objections soulevées et lui donne la possibilité de faire connaître son point de vue. Si l'autorité notifiante conclut que l'organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, elle soumet la désignation à des restrictions, la suspend ou la retire, selon le cas, en fonction de la gravité du manquement. Elle en informe immédiatement la Commission et les autres États membres.

5. Lorsque sa désignation a été suspendue, restreinte ou révoquée en tout ou en partie, l'organisme notifié en informe les fournisseurs concernés dans un délai de dix jours.

6. En cas de restriction, de suspension ou de retrait d'une désignation, l'autorité notifiante prend les mesures nécessaires pour que les dossiers de l'organisme notifié en question soient conservés et pour qu'ils soient mis à la disposition des autorités notifiantes d'autres États membres et des autorités de surveillance du marché, à leur demande.

7. En cas de restriction, de suspension ou de retrait d'une désignation, l'autorité notifiante:

a) évalue l'incidence sur les certificats délivrés par l'organisme notifié;

b) transmet un rapport sur ses conclusions à la Commission et aux autres États membres dans un délai de trois mois après avoir signalé les modifications apportées à la désignation;

c) exige de l'organisme notifié qu'il suspende ou retire, dans un délai raisonnable qu'elle détermine, tous les certificats délivrés à tort afin d'assurer la conformité constante des systèmes d'IA à haut risque sur le marché;

d) informe la Commission et les États membres des certificats dont elle a demandé la suspension ou le retrait;

e) fournit aux autorités nationales compétentes de l'État membre dans lequel le fournisseur a son siège social toutes les informations pertinentes sur les certificats dont elle a demandé la suspension ou le retrait; cette autorité prend les mesures appropriées si cela est nécessaire pour éviter un risque potentiel pour la santé, la sécurité ou les droits fondamentaux.

8. À l'exception des certificats délivrés à tort, et lorsqu'une désignation a été suspendue ou restreinte, les certificats restent valables dans l'un des cas suivants:

a) l'autorité notifiante a confirmé, dans un délai d'un mois suivant la suspension ou la restriction, qu'il n'y a pas de risque pour la santé, la sécurité ou les droits fondamentaux en lien avec les certificats concernés par la suspension ou la restriction, et l'autorité notifiante a défini un calendrier de mesures pour remédier à la suspension ou à la restriction; ou

▼B

b) l'autorité notifiante a confirmé qu'aucun certificat ayant trait à la suspension ne sera délivré, modifié ou délivré à nouveau pendant la période de suspension ou de restriction et elle indique si l'organisme notifié est en mesure de continuer à contrôler les certificats existants délivrés et à en être responsable pour la durée de la suspension ou de la restriction. Si l'autorité notifiante considère que l'organisme notifié n'est pas en mesure de se charger des certificats existants délivrés, le fournisseur du système faisant l'objet du certificat confirme par écrit aux autorités nationales compétentes de l'État membre dans lequel il a son siège social, dans un délai de trois mois suivant la suspension ou la restriction, qu'un autre organisme notifié qualifié assume temporairement les fonctions de surveillance de l'organisme notifié et continue d'assumer la responsabilité des certificats pour la durée de la suspension ou de la restriction.

9. À l'exception des certificats délivrés à tort, et lorsqu'une désignation a été retirée, les certificats restent valables pendant une durée de neuf mois dans les cas suivants:

a) l'autorité nationale compétente de l'État membre dans lequel le fournisseur du système d'IA à haut risque faisant l'objet du certificat a son siège social a confirmé que les systèmes d'IA à haut risque en question ne présentent pas de risque pour la santé, la sécurité ou les droits fondamentaux; et

b) un autre organisme notifié a confirmé par écrit qu'il assumera la responsabilité immédiate de ces systèmes d'IA et achèvera son évaluation dans un délai de douze mois à compter du retrait de la désignation.

Dans le cas visé au premier alinéa, l'autorité nationale compétente de l'État membre dans lequel le fournisseur du système faisant l'objet du certificat a son siège peut prolonger à plusieurs reprises la durée de validité provisoire des certificats de trois mois supplémentaires, pour une durée totale maximale de douze mois.

L'autorité nationale compétente ou l'organisme notifié assumant les fonctions de l'organisme notifié concerné par la modification de la désignation en informe immédiatement la Commission, les autres États membres et les autres organismes notifiés.

Article 37

Contestation de la compétence des organismes notifiés

1. La Commission enquête, s'il y a lieu, sur tous les cas où il existe des raisons de douter de la compétence d'un organisme notifié ou du respect continu, par un organisme notifié, des exigences établies à l'article 31 et de ses responsabilités applicables.

2. L'autorité notifiante fournit à la Commission, sur demande, toutes les informations utiles relatives à la notification ou au maintien de la compétence de l'organisme notifié concerné.

3. La Commission veille à ce que toutes les informations sensibles obtenues au cours des enquêtes qu'elle mène au titre du présent article soient traitées de manière confidentielle conformément à l'article 78.

▼B

4. Lorsque la Commission établit qu'un organisme notifié ne répond pas ou ne répond plus aux exigences relatives à sa notification, elle informe l'État membre notifiant en conséquence et lui demande de prendre les mesures correctives qui s'imposent, y compris la suspension ou le retrait de la notification si nécessaire. Si l'État membre ne prend pas les mesures correctives qui s'imposent, la Commission peut, au moyen d'un acte d'exécution, suspendre, restreindre ou retirer la désignation. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Article 38

Coordination des organismes notifiés

1. La Commission veille à ce que, en ce qui concerne les systèmes d'IA à haut risque, une coordination et une coopération appropriées entre les organismes notifiés intervenant dans les procédures d'évaluation de la conformité conformément au présent règlement soient mises en place et gérées de manière adéquate dans le cadre d'un groupe sectoriel d'organismes notifiés.

2. Chaque autorité notifiante veille à ce que les organismes qu'elle a notifiés participent aux travaux d'un groupe visé au paragraphe 1, directement ou par l'intermédiaire de représentants désignés.

3. La Commission veille à l'échange des connaissances et des bonnes pratiques entre les autorités notifiantes.

Article 39

Organismes d'évaluation de la conformité de pays tiers

Les organismes d'évaluation de la conformité établis conformément à la législation d'un pays tiers avec lequel l'Union a conclu un accord peuvent être autorisés à exercer les activités d'organismes notifiés au titre du présent règlement, pour autant qu'ils répondent aux exigences prévues à l'article 31 ou qu'ils veillent à un niveau équivalent de respect.

SECTION 5

Normes, évaluation de la conformité, certificats, enregistrement

Article 40

Normes harmonisées et travaux de normalisation

1. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012 sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, du présent règlement, dans la mesure où ces exigences ou obligations sont couvertes par ces normes.

▼B

2. Conformément à l'article 10 du règlement (UE) n° 1025/2012, la Commission présente sans retard injustifié des demandes de normalisation couvrant toutes les exigences énoncées à la section 2 du présent chapitre et, le cas échéant, les demandes de normalisation couvrant les obligations énoncées au chapitre V, sections 2 et 3, du présent règlement. La demande de normalisation inclut également une demande de livrables sur les processus de déclaration et de documentation afin d'améliorer les performances des systèmes d'IA en matière de ressources, telles que la réduction de la consommation d'énergie et d'autres ressources par le système d'IA à haut risque au cours de son cycle de vie, et sur le développement économe en énergie de modèles d'IA à usage général. Lors de la préparation d'une demande de normalisation, la Commission consulte le Comité IA et les parties prenantes concernées, y compris le forum consultatif.

Lorsqu'elle présente une demande de normalisation aux organisations européennes de normalisation, la Commission précise que les normes doivent être claires, cohérentes, y compris avec les normes développées dans les différents secteurs pour les produits relevant de la législation d'harmonisation de l'Union existante dont la liste figure à l'annexe I, et visant à veiller à ce que les systèmes d'IA à haut risque ou les modèles d'IA à usage général mis sur le marché ou mis en service dans l'Union satisfont aux exigences ou obligations pertinentes énoncées dans le présent règlement.

La Commission demande aux organisations européennes de normalisation de fournir la preuve qu'elles mettent tout en œuvre pour atteindre les objectifs visés aux premier et deuxième alinéas du présent paragraphe, conformément à l'article 24 du règlement (UE) n° 1025/2012.

3. Les participants au processus de normalisation s'efforcent de favoriser les investissements et l'innovation dans le domaine de l'IA, y compris en renforçant la sécurité juridique, ainsi que la compétitivité et la croissance du marché de l'Union, de contribuer à renforcer la coopération mondiale en faveur d'une normalisation en tenant compte des normes internationales existantes dans le domaine de l'IA qui sont conformes aux valeurs et aux intérêts de l'Union et aux droits fondamentaux, et de renforcer la gouvernance multipartite en veillant à une représentation équilibrée des intérêts et à la participation effective de toutes les parties prenantes concernées conformément aux articles 5, 6 et 7 du règlement (UE) n° 1025/2012.

Article 41

Spécifications communes

1. La Commission peut adopter des actes d'exécution établissant des spécifications communes pour les exigences énoncées à la section 2 du présent chapitre ou, le cas échéant, pour les obligations énoncées au chapitre V, sections 2 et 3, lorsque les conditions suivantes sont remplies:

a) la Commission, en vertu de l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012, a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée pour les exigences énoncées à la section 2 du présent chapitre ou, le cas échéant, pour les obligations énoncées au chapitre V, sections 2 et 3, et:

▼B

i) la demande n'a été acceptée par aucune des organisations européennes de normalisation; ou

ii) les normes harmonisées faisant l'objet de cette demande n'ont pas été présentées dans le délai fixé conformément à l'article 10, paragraphe 1, du règlement (UE) n° 1025/2012; ou

iii) les normes harmonisées pertinentes ne répondent pas suffisamment aux préoccupations en matière de droits fondamentaux; ou

iv) les normes harmonisées ne sont pas conformes à la demande; et

b) aucune référence à des normes harmonisées couvrant les exigences visées à la section 2 du chapitre ou, le cas échéant, les obligations énoncées au chapitre V, sections 2 et 3, n'a été publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) n° 1025/2012, et aucune référence de ce type ne devrait être publiée dans un délai raisonnable.

Lors de la rédaction des spécifications communes, la Commission consulte le forum consultatif visé à l'article 67.

Les actes d'exécution visés au premier alinéa du présent paragraphe sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Avant d'élaborer un projet d'acte d'exécution, la Commission informe le comité visé à l'article 22 du règlement (UE) n° 1025/2012 qu'elle considère que les conditions énoncées au paragraphe 1 du présent article sont remplies.

3. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes aux spécifications communes visées au paragraphe 1, ou à des parties de ces spécifications, sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant pour se conformer aux obligations visées au chapitre V, sections 2 et 3, dans la mesure où ces exigences ou obligations sont couvertes par ces spécifications communes.

4. Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission en vue de la publication de sa référence au *Journal officiel de l'Union européenne*, la Commission procède à l'évaluation de cette norme harmonisée conformément au règlement (UE) n° 1025/2012. Lorsque la référence à une norme harmonisée est publiée au *Journal officiel de l'Union européenne*, la Commission abroge les actes d'exécution visés au paragraphe 1, ou les parties de ces actes qui couvrent les mêmes exigences que celles énoncées à la section 2 du présent chapitre ou, le cas échéant les mêmes obligations que celles énoncées au chapitre V, sections 2 et 3.

5. Lorsque les fournisseurs de systèmes d'IA à haut risque ou de modèles d'IA à usage général ne respectent pas les spécifications communes visées au paragraphe 1, ils justifient dûment avoir adopté des solutions techniques qui satisfont aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, à un niveau au moins équivalent auxdites spécifications.

▼B

6. Lorsqu'un État membre considère qu'une spécification commune ne satisfait pas entièrement aux exigences énoncées à la section 2 ou, le cas échéant aux obligations énoncées au chapitre V, sections 2 et 3, il en informe la Commission au moyen d'une explication détaillée. La Commission évalue ces informations et, le cas échéant, modifie l'acte d'exécution établissant la spécification commune concernée.

Article 42

Présomption de conformité avec certaines exigences

1. Les systèmes d'IA à haut risque qui ont été entraînés et testés avec des données tenant compte du cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel ils sont destinés à être utilisés sont présumés conformes aux exigences pertinentes établies à l'article 10, paragraphe 4.

2. Les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au règlement (UE) 2019/881 et dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences de cybersécurité énoncées à l'article 15 du présent règlement, dans la mesure où ces dernières sont couvertes par tout ou partie du certificat de cybersécurité ou de la déclaration de conformité.

Article 43

Évaluation de la conformité

1. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, lorsque, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, le fournisseur a appliqué les normes harmonisées visées à l'article 40 ou, le cas échéant, les spécifications communes visées à l'article 41, il choisit l'une des procédures d'évaluation de la conformité suivantes sur la base:

a) du contrôle interne visé à l'annexe VI; ou

b) de l'évaluation du système de gestion de la qualité et de l'évaluation de la documentation technique, avec l'intervention d'un organisme notifié, visée à l'annexe VII.

Pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées à la section 2, le fournisseur suit la procédure d'évaluation de la conformité prévue à l'annexe VII dans les cas suivants:

a) les normes harmonisées visées à l'article 40 n'existent pas et les spécifications communes visées à l'article 41 font défaut;

b) le fournisseur n'a pas appliqué la norme harmonisée ou ne l'a appliquée que partiellement;

c) les spécifications communes visées au point a) existent, mais le fournisseur ne les a pas appliquées;

d) une ou plusieurs des normes harmonisées visées au point a), ont été publiées assorties d'une restriction et seulement sur la partie de la norme qui a été soumise à une restriction.

▼B

Aux fins de la procédure d'évaluation de la conformité visée à l'annexe VII, le fournisseur peut choisir n'importe lequel des organismes notifiés. Toutefois, lorsque le système d'IA à haut risque est destiné à être mis en service par les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile ou par les institutions, organes ou organismes de l'UE, l'autorité de surveillance du marché visée à l'article 74, paragraphe 8 ou 9, selon le cas, agit en tant qu'organisme notifié.

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI, qui ne prévoit pas d'intervention d'un organisme notifié.

3. Pour les systèmes d'IA à haut risque couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, le fournisseur suit la procédure d'évaluation de la conformité pertinente selon les modalités requises par ces actes juridiques. Les exigences énoncées à la section 2 du présent chapitre s'appliquent à ces systèmes d'IA à haut risque et font partie de cette évaluation. Les points 4.3, 4.4 et 4.5 de l'annexe VII ainsi que le point 4.6, cinquième alinéa, de ladite annexe s'appliquent également.

Aux fins de ces évaluations, les organismes notifiés qui ont été notifiés en vertu de ces actes juridiques sont habilités à contrôler la conformité des systèmes d'IA à haut risque avec les exigences énoncées à la section 2, à condition que le respect, par ces organismes notifiés, des exigences énoncées à l'article 31, paragraphes 4, 5, 10 et 11, ait été évalué dans le cadre de la procédure de notification prévue par ces actes juridiques.

Lorsqu'un acte juridique énuméré à l'annexe I, section A, confère au fabricant du produit la faculté de ne pas faire procéder à une évaluation de la conformité par un tiers, à condition que ce fabricant ait appliqué toutes les normes harmonisées couvrant toutes les exigences pertinentes, ce fabricant ne peut faire usage de cette faculté que s'il a également appliqué les normes harmonisées ou, le cas échéant, les spécifications communes visées à l'article 41 couvrant toutes les exigences énoncées à la section 2 du présent chapitre.

4. Les systèmes d'IA à haut risque qui ont déjà été soumis à une procédure d'évaluation de la conformité sont soumis à une nouvelle procédure d'évaluation de la conformité lorsqu'ils font l'objet de modifications substantielles, que le système modifié soit destiné à être distribué plus largement ou reste utilisé par le déployeur actuel.

Pour les systèmes d'IA à haut risque qui continuent leur apprentissage après avoir été mis sur le marché ou mis en service, les modifications apportées au système d'IA à haut risque et à sa performance qui ont été déterminées au préalable par le fournisseur au moment de l'évaluation initiale de la conformité et font partie des informations contenues dans la documentation technique visée à l'annexe IV, point 2), f), ne constituent pas une modification substantielle.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier les annexes VI et VII afin de les mettre à jour compte tenu du progrès technique.

▼B

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier les paragraphes 1 et 2 du présent article afin de soumettre les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, à tout ou partie de la procédure d'évaluation de la conformité visée à l'annexe VII. La Commission adopte ces actes délégués en tenant compte de l'efficacité de la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI pour prévenir ou réduire au minimum les risques que ces systèmes font peser sur la santé et la sécurité et sur la protection des droits fondamentaux, ainsi que de la disponibilité de capacités et de ressources suffisantes au sein des organismes notifiés.

Article 44

Certificats

1. Les certificats délivrés par les organismes notifiés conformément à l'annexe VII sont établis dans une langue aisément compréhensible par les autorités compétentes de l'État membre dans lequel l'organisme notifié est établi.

2. Les certificats sont valables pendant la période indiquée sur ceux-ci, qui n'excède pas cinq ans pour les systèmes d'IA relevant de l'annexe I, et quatre ans pour les systèmes d'IA relevant de l'annexe III. À la demande du fournisseur, la durée de validité d'un certificat peut être prolongée d'une durée maximale de cinq ans à chaque fois pour les systèmes d'IA relevant de l'annexe I, et de quatre ans pour les systèmes d'IA relevant de l'annexe III, sur la base d'une nouvelle évaluation suivant les procédures d'évaluation de la conformité applicables. Tout document complémentaire à un certificat reste valable, à condition que le certificat qu'il complète le soit.

3. Lorsqu'un organisme notifié constate qu'un système d'IA ne répond plus aux exigences énoncées à la section 2, il suspend ou retire le certificat délivré ou l'assortit de restrictions, en tenant compte du principe de proportionnalité, sauf si le fournisseur applique, en vue du respect de ces exigences, des mesures correctives appropriées dans le délai imparti à cet effet par l'organisme notifié. L'organisme notifié motive sa décision.

Une procédure de recours contre les décisions des organismes notifiés, y compris concernant des certificats de conformité délivrés, est disponible.

Article 45

Obligations d'information des organismes notifiés

1. Les organismes notifiés communiquent à l'autorité notifiante:

a) tout certificat d'évaluation UE de la documentation technique, tout document complémentaire afférent à ce certificat, et toute approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;

▼B

b) tout refus, restriction, suspension ou retrait d'un certificat d'évaluation UE de la documentation technique ou d'une approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;

c) toute circonstance ayant une incidence sur la portée ou les conditions de la notification;

d) toute demande d'information reçue des autorités de surveillance du marché concernant les activités d'évaluation de la conformité;

e) sur demande, les activités d'évaluation de la conformité réalisées dans le cadre de leur notification et toute autre activité réalisée, y compris les activités transfrontières et sous-traitées.

2. Chaque organisme notifié porte à la connaissance des autres organismes notifiés:

a) les approbations de systèmes de gestion de la qualité qu'il a refusées, suspendues ou retirées et, sur demande, les approbations qu'il a délivrées;

b) les certificats d'évaluation UE de la documentation technique ou les documents complémentaires y afférents qu'il a refusés, retirés, suspendus ou soumis à d'autres restrictions et, sur demande, les certificats et/ou documents complémentaires y afférents qu'il a délivrés.

3. Chaque organisme notifié fournit aux autres organismes notifiés qui accomplissent des activités similaires d'évaluation de la conformité portant sur les mêmes types de systèmes d'IA des informations pertinentes sur les aspects liés à des résultats négatifs et, sur demande, à des résultats positifs d'évaluation de la conformité.

4. Les autorités notifiantes garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78.

Article 46

Dérogation à la procédure d'évaluation de la conformité

1. Par dérogation à l'article 43 et sur demande dûment justifiée, toute autorité de surveillance du marché peut, pour des raisons exceptionnelles de sécurité publique ou pour assurer la protection de la vie et de la santé humaines, la protection de l'environnement ou la protection d'actifs industriels et d'infrastructures d'importance majeure, autoriser la mise sur le marché ou la mise en service de systèmes d'IA à haut risque spécifiques sur le territoire de l'État membre concerné. Cette autorisation est accordée pour une période limitée pendant la durée des procédures d'évaluation de la conformité nécessaires, en tenant compte des raisons exceptionnelles justifiant la dérogation. Ces procédures sont menées à bien sans retard injustifié.

2. Dans une situation d'urgence dûment justifiée pour des raisons exceptionnelles de sécurité publique ou en cas de menace spécifique, substantielle et imminente pour la vie ou la sécurité physique des personnes physiques, les autorités répressives ou les autorités de protection civile peuvent mettre en service un service d'IA à haut risque spécifique sans avoir obtenu l'autorisation visée au paragraphe 1, à condition que cette autorisation soit demandée sans retard injustifié pendant ou après l'utilisation. Si l'autorisation visée au paragraphe 1 est refusée, l'utilisation du système d'IA à haut risque cesse immédiatement et tous les résultats et sorties de cette utilisation sont immédiatement mis au rebut.

▼B

3. L'autorisation visée au paragraphe 1 n'est délivrée que si l'autorité de surveillance du marché conclut que le système d'IA à haut risque satisfait aux exigences de la section 2. L'autorité de surveillance du marché informe la Commission et les autres États membres de toute autorisation délivrée conformément aux paragraphes 1 et 2. Cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives.

4. Si aucune objection n'est émise, dans un délai de quinze jours civils suivant la réception des informations visées au paragraphe 3, par un État membre ou par la Commission à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un État membre conformément au paragraphe 1, cette autorisation est réputée justifiée.

5. Si, dans un délai de quinze jours civils suivant la réception de la notification visée au paragraphe 3, un État membre soulève des objections à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un autre État membre, ou si la Commission estime que l'autorisation est contraire au droit de l'Union ou que la conclusion des États membres quant à la conformité du système visée au paragraphe 3 n'est pas fondée, la Commission entame sans retard des consultations avec l'État membre concerné. Les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Sur cette base, la Commission décide si l'autorisation est justifiée ou non. La Commission communique sa décision à l'État membre concerné ainsi qu'aux opérateurs concernés.

6. Si la Commission estime que l'autorisation est injustifiée, elle est retirée par l'autorité de surveillance du marché de l'État membre concerné.

7. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section A, seules les dérogations à l'évaluation de la conformité établies dans ladite législation d'harmonisation de l'Union s'appliquent.

Article 47

Déclaration UE de conformité

1. Le fournisseur établit une déclaration UE de conformité écrite, lisible par machine, signée à la main ou électroniquement concernant chaque système d'IA à haut risque et la tient à la disposition des autorités nationales compétentes pendant une durée de dix ans à partir du moment où le système d'IA à haut risque a été mis sur le marché ou mis en service. La déclaration UE de conformité identifie le système d'IA à haut risque pour lequel elle a été établie. Une copie de la déclaration UE de conformité est communiquée, sur demande, aux autorités nationales compétentes concernées.

2. La déclaration UE de conformité atteste que le système d'IA à haut risque concerné satisfait aux exigences énoncées à la section 2. La déclaration UE de conformité contient les informations qui figurent à l'annexe V et est traduite dans une langue aisément compréhensible par les autorités nationales compétentes des États membres dans lesquels le système d'IA à haut risque est mis sur le marché ou mis à disposition.

▼B

3. Si des systèmes d'IA à haut risque sont soumis à d'autres actes législatifs d'harmonisation de l'Union qui exigent également une déclaration UE de conformité, une seule déclaration UE de conformité est établie au titre de tous les actes législatifs de l'Union applicables au système d'IA à haut risque. La déclaration contient toutes les informations nécessaires à l'identification de la législation d'harmonisation de l'Union à laquelle la déclaration se rapporte.

4. Lors de l'établissement de la déclaration UE de conformité, le fournisseur assume la responsabilité du respect des exigences énoncées à la section 2. Le fournisseur tient à jour la déclaration UE de conformité, le cas échéant.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe V en mettant à jour le contenu de la déclaration UE de conformité prévu à ladite annexe afin d'y introduire les éléments devenus nécessaires compte tenu du progrès technique.

Article 48

Marquage CE

1. Le marquage CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) n° 765/2008.

2. Pour les systèmes d'IA à haut risque fournis numériquement, un marquage CE numérique n'est utilisé que s'il est facile d'y accéder par l'interface à partir de laquelle l'accès à ce système s'effectue ou au moyen d'un code facilement accessible lisible par machine ou d'autres moyens électroniques.

3. Le marquage CE est apposé de façon visible, lisible et indélébile sur les systèmes d'IA à haut risque. Si cela est impossible ou injustifié étant donné la nature du système d'IA à haut risque, il est apposé sur l'emballage ou sur les documents d'accompagnement, selon le cas.

4. Le cas échéant, le marquage CE est suivi du numéro d'identification de l'organisme notifié responsable des procédures d'évaluation de la conformité prévues à l'article 43. Le numéro d'identification de l'organisme notifié est apposé par l'organisme lui-même ou, sur instruction de celui-ci, par le fournisseur ou par le mandataire du fournisseur. Le numéro d'identification est également indiqué dans tous les documents publicitaires mentionnant que le système d'IA à haut risque est conforme aux exigences applicables au marquage CE.

5. Lorsque des systèmes d'IA à haut risque sont soumis à d'autres actes législatifs de l'Union qui prévoient aussi l'apposition du marquage CE, ce marquage indique que les systèmes d'IA à haut risque satisfont également aux exigences de ces autres actes législatifs.

Article 49

Enregistrement

1. Avant de mettre sur le marché ou de mettre en service un système d'IA à haut risque énuméré à l'annexe III, à l'exception des systèmes d'IA à haut risque visés à l'annexe III, point 2, le fournisseur ou, selon le cas, le mandataire s'enregistre dans la base de données de l'UE visée à l'article 71 et y enregistre aussi son système.

▼B

2. Avant de mettre sur le marché ou de mettre en service un système d'IA à propos duquel le fournisseur a conclu qu'il ne s'agissait pas d'un système à haut risque au titre de l'article 6, paragraphe 3, ce fournisseur ou, selon le cas, le mandataire s'enregistre dans la base de données de l'UE visée à l'article 71 et y enregistre aussi ce système.

3. Avant de mettre en service ou d'utiliser un système d'IA à haut risque énuméré à l'annexe III, à l'exception des systèmes d'IA à haut risque énumérés à l'annexe III, point 2, les déployeurs qui sont des autorités publiques, des institutions organes ou organismes de l'Union ou des personnes agissant en leur nom s'enregistrent, sélectionnent le système et enregistrent son utilisation dans la base de données de l'UE visée à l'article 71.

4. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, l'enregistrement visé aux paragraphes 1, 2 et 3 du présent article figure dans une section sécurisée non publique de la base de données de l'UE visée à l'article 71 et comprend uniquement les informations suivantes, selon le cas, visées:

a) à l'annexe VIII, section A, points 1 à 10, à l'exception des points 6, 8 et 9;

b) à l'annexe VIII, section B, points 1 à 5, et points 8 et 9;

c) à l'annexe VIII, section C, points 1 à 3;

d) à l'annexe IX, points 1, 2, 3 et 5.

Seules la Commission et les autorités nationales visées à l'article 74, paragraphe 8, ont accès aux différentes sections restreintes de la base de données de l'UE énumérées au premier alinéa du présent paragraphe.

5. Les systèmes d'IA à haut risque visés à l'annexe III, point 2, sont enregistrés au niveau national.

CHAPITRE IV

OBLIGATIONS DE TRANSPARENCE POUR LES FOURNISSEURS ET LES DÉPLOYEURS DE CERTAINS SYSTÈMES D'IA

Article 50

Obligations de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA

1. Les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir directement avec des personnes physiques soient conçus et développés de manière que les personnes physiques concernées soient informées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation. Cette obligation ne s'applique pas aux systèmes d'IA dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers, sauf si ces systèmes sont mis à la disposition du public pour permettre le signalement d'une infraction pénale.

▼B

2. Les fournisseurs de systèmes d'IA, y compris de systèmes d'IA à usage général, qui génèrent des contenus de synthèse de type audio, image, vidéo ou texte, veillent à ce que les sorties des systèmes d'IA soient marquées dans un format lisible par machine et identifiables comme ayant été générées ou manipulées par une IA. Les fournisseurs veillent à ce que leurs solutions techniques soient aussi efficaces, interopérables, solides et fiables que la technologie le permet, compte tenu des spécificités et des limites des différents types de contenus, des coûts de mise en œuvre et de l'état de la technique généralement reconnu, comme cela peut ressortir des normes techniques pertinentes. Cette obligation ne s'applique pas dans la mesure où les systèmes d'IA remplissent une fonction d'assistance pour la mise en forme standard ou ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique, ou lorsque leur utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière.

3. Les déployeurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique informent les personnes physiques qui y sont exposées du fonctionnement du système et traitent les données à caractère personnel conformément au règlement (UE) 2016/679, au règlement (UE) 2018/1725 et à la directive (UE) 2016/680, selon le cas. Cette obligation ne s'applique pas aux systèmes d'IA utilisés pour la catégorisation biométrique et la reconnaissance des émotions dont la loi autorise l'utilisation à des fins de prévention ou de détection des infractions pénales ou d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers et conformément au droit de l'Union.

4. Les déployeurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo constituant un hypertrucage indiquent que les contenus ont été générés ou manipulés par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière. Lorsque le contenu fait partie d'une œuvre ou d'un programme manifestement artistique, créatif, satirique, fictif ou analogue, les obligations de transparence énoncées au présent paragraphe se limitent à la divulgation de l'existence de tels contenus générés ou manipulés d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre.

Les déployeurs d'un système d'IA qui génère ou manipule des textes publiés dans le but d'informer le public sur des questions d'intérêt public indiquent que le texte a été généré ou manipulé par une IA. Cette obligation ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention ou de détection des infractions pénales, d'enquêtes ou de poursuites en la matière, ou lorsque le contenu généré par l'IA a fait l'objet d'un processus d'examen humain ou de contrôle éditorial et lorsqu'une personne physique ou morale assume la responsabilité éditoriale de la publication du contenu.

5. Les informations visées aux paragraphes 1 à 4 sont fournies aux personnes physiques concernées de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition. Les informations sont conformes aux exigences applicables en matière d'accessibilité.

6. Les paragraphes 1 à 4 n'ont pas d'incidence sur les exigences et obligations énoncées au chapitre III et sont sans préjudice des autres obligations de transparence prévues par le droit de l'Union ou le droit national pour les déployeurs de systèmes d'IA.

▼B

7. Le Bureau de l'IA encourage et facilite l'élaboration de codes de bonne pratique au niveau de l'Union afin de faciliter la mise en œuvre effective des obligations relatives à la détection et à l'étiquetage des contenus générés ou manipulés par une IA. La Commission peut adopter des actes d'exécution pour approuver ces codes de bonne pratique conformément à la procédure prévue à l'article 56, paragraphe 6. Si elle estime que le code n'est pas approprié, la Commission peut adopter un acte d'exécution précisant des règles communes pour la mise en œuvre de ces obligations conformément à la procédure d'examen prévue à l'article 98, paragraphe 2.

CHAPITRE V

MODÈLES D'IA À USAGE GÉNÉRAL

SECTION 1

Règles de classification

Article 51

Classification de modèles d'IA à usage général en tant que modèles d'IA à usage général présentant un risque systémique

1. Un modèle d'IA à usage général est classé comme modèle d'IA à usage général présentant un risque systémique s'il remplit l'une des conditions suivantes:

a) il dispose de capacités à fort impact évaluées sur la base de méthodologies et d'outils techniques appropriés, y compris des indicateurs et des critères de référence;

b) sur la base d'une décision de la Commission, d'office ou à la suite d'une alerte qualifiée du groupe scientifique, il possède des capacités ou un impact équivalents à ceux énoncés au point a), compte tenu des critères définis à l'annexe XIII.

2. Un modèle d'IA à usage général est présumé avoir des capacités à fort impact conformément au paragraphe 1, point a), lorsque la quantité cumulée de calcul utilisée pour son entraînement mesurée en opérations en virgule flottante est supérieure à 10^{25}.

3. La Commission adopte des actes délégués conformément à l'article 97 pour modifier les seuils énumérés aux paragraphes 1 et 2 du présent article, ainsi que pour compléter les critères de référence et les indicateurs à la lumière des évolutions technologiques, telles que les améliorations algorithmiques ou l'efficacité accrue du matériel informatique, si nécessaire, afin que ces seuils reflètent l'état de la technique.

Article 52

Procédure

1. Lorsqu'un modèle d'IA à usage général remplit la condition visée à l'article 51, paragraphe 1, point a), le fournisseur concerné en informe la Commission sans tarder et, en tout état de cause, dans un délai de deux semaines après la date à laquelle ce critère est rempli ou

▼B

après qu'il a été établi qu'il le sera. Cette notification comprend les informations nécessaires pour démontrer que le critère pertinent a été rempli. Si la Commission apprend l'existence d'un modèle d'IA à usage général présentant un risque systémique dont elle n'a pas été informée, elle peut décider de le désigner comme modèle présentant un risque systémique.

2. Le fournisseur d'un modèle d'IA à usage général qui remplit la condition visée à l'article 51, paragraphe 1, point a), peut présenter, avec sa notification, des arguments suffisamment étayés pour démontrer que, exceptionnellement, bien qu'il remplisse ce critère, le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique et ne devrait donc pas être classé comme modèle d'IA à usage général présentant un risque systémique.

3. Lorsque la Commission conclut que les arguments présentés conformément au paragraphe 2 ne sont pas suffisamment étayés et que le fournisseur concerné n'a pas été en mesure de démontrer que le modèle d'IA à usage général ne présente pas, en raison de ses caractéristiques spécifiques, de risque systémique, elle rejette ces arguments, et le modèle d'IA à usage général est considéré comme un modèle d'IA à usage général présentant un risque systémique.

4. La Commission peut désigner un modèle d'IA à usage général comme présentant un risque systémique, d'office ou à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a), sur la base des critères énoncés à l'annexe XIII.

La Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour modifier l'annexe XIII en précisant et mettant à jour les critères énoncés à ladite annexe.

5. Sur demande motivée d'un fournisseur dont le modèle a été désigné comme modèle d'IA à usage général présentant un risque systémique en vertu du paragraphe 4, la Commission tient compte de la demande et peut décider de réévaluer si le modèle d'IA à usage général peut encore être considéré comme présentant un risque systémique sur la base des critères énoncés à l'annexe XIII. Une telle demande contient les éléments objectifs, détaillés et nouveaux qui sont apparus depuis la décision de désignation. Les fournisseurs peuvent demander une réévaluation au plus tôt six mois après la décision de désignation. Lorsque la Commission, à la suite de sa réévaluation, décide de maintenir la désignation en tant que modèle d'IA à usage général présentant un risque systémique, les fournisseurs peuvent demander une réévaluation au plus tôt six mois après cette décision.

6. La Commission veille à ce qu'une liste des modèles d'IA à usage général présentant un risque systémique soit publiée et tient cette liste à jour, sans préjudice de la nécessité de respecter et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national.

▼B

SECTION 2

Obligations incombant aux fournisseurs de modèles d'IA à usage général

Article 53

Obligations incombant aux fournisseurs de modèles d'IA à usage général

1. Les fournisseurs de modèles d'IA à usage général:

a) élaborent et tiennent à jour la documentation technique du modèle, y compris son processus d'entraînement et d'essai et les résultats de son évaluation, qui contient, au minimum, les informations énoncées à l'annexe XI aux fins de la fournir, sur demande, au Bureau de l'IA et aux autorités nationales compétentes;

b) élaborent, tiennent à jour et mettent à disposition des informations et de la documentation à l'intention des fournisseurs de systèmes d'IA qui envisagent d'intégrer le modèle d'IA à usage général dans leurs systèmes d'IA. Sans préjudice de la nécessité d'observer et de protéger les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires conformément au droit de l'Union et au droit national, ces informations et cette documentation:

   i) permettent aux fournisseurs de systèmes d'IA d'avoir une bonne compréhension des capacités et des limites du modèle d'IA à usage général et de se conformer aux obligations qui leur incombent en vertu du présent règlement; et

   ii) contiennent, au minimum, les éléments énoncés à l'annexe XII;

c) mettent en place une politique visant à se conformer au droit de l'Union en matière de droit d'auteur et droits voisins, et notamment à identifier et à respecter, y compris au moyen de technologies de pointe, une réservation de droits exprimée conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790;

d) élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle d'IA à usage général, conformément à un modèle fourni par le Bureau de l'IA.

2. Les obligations énoncées au paragraphe 1, points a) et b), ne s'appliquent pas aux fournisseurs de modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. Cette exception ne s'applique pas aux modèles d'IA à usage général présentant un risque systémique.

3. Les fournisseurs de modèles d'IA à usage général coopèrent, en tant que de besoin, avec la Commission et les autorités nationales compétentes dans l'exercice de leurs compétences et pouvoirs en vertu du présent règlement.

▼B

4. Les fournisseurs de modèles d'IA à usage général peuvent s'appuyer sur des codes de bonne pratique au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Le respect des normes européennes harmonisées confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations. Les fournisseurs de modèles d'IA à usage général qui n'adhèrent pas à un code de bonnes pratiques approuvé ou ne respectent pas une norme européenne harmonisée démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'appréciation de la Commission.

5. Afin de faciliter le respect de l'annexe XI, et notamment du point 2, points d) et e), la Commission est habilitée à adopter des actes délégués conformément à l'article 97 pour préciser les méthodes de mesure et de calcul en vue de permettre l'élaboration d'une documentation comparable et vérifiable.

6. La Commission est habilitée à adopter des actes délégués conformément à l'article 97, paragraphe 2, pour modifier les annexes XI et XII à la lumière des évolutions technologiques.

7. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

Article 54

Mandataires des fournisseurs de modèles d'IA à usage général

1. Avant de mettre un modèle d'IA à usage général sur le marché de l'Union, les fournisseurs établis dans des pays tiers désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le fournisseur autorise son mandataire à exécuter les tâches indiquées dans le mandat que lui a confié le fournisseur.

3. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Il fournit une copie du mandat au Bureau de l'IA à la demande de ce dernier, dans l'une des langues officielles des institutions de l'Union. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter les tâches suivantes:

a) vérifier que la documentation technique prévue à l'annexe XI a été rédigée et que toutes les obligations visées à l'article 53 et, le cas échéant, à l'article 55 ont été remplies par le fournisseur;

b) tenir à la disposition du Bureau de l'IA et des autorités nationales compétentes une copie de la documentation technique prévue à l'annexe XI, pendant une période de dix ans après la mise sur le marché du modèle d'IA à usage général, et les coordonnées du fournisseur ayant désigné le mandataire;

c) communiquer au Bureau de l'IA, sur demande motivée de sa part, toutes les informations et tous les documents, y compris ceux visés au point b), nécessaires pour démontrer qu'il respecte les obligations du présent chapitre;

▼B

d) coopérer avec le Bureau de l'IA et les autorités compétentes, sur demande motivée de leur part, à toute mesure qu'ils prennent à l'égard d'un modèle d'IA à usage général, y compris lorsque le modèle est intégré dans des systèmes d'IA mis sur le marché ou mis en service dans l'Union.

4. Le mandat habilite le mandataire à servir d'interlocuteur, en plus ou à la place du fournisseur, au Bureau de l'IA ou aux autorités compétentes, pour toutes les questions liées au respect du présent règlement.

5. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent en vertu du présent règlement. Dans ce cas, il informe en outre immédiatement le Bureau de l'IA de la cessation du mandat et des motifs qui la sous-tendent.

6. L'obligation énoncée au présent article ne s'applique pas aux fournisseurs de modèles d'IA à usage général qui sont publiés dans le cadre d'une licence libre et ouverte permettant de consulter, d'utiliser, de modifier et de distribuer le modèle, et dont les paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics, à moins que les modèles d'IA à usage général présentent un risque systémique.

SECTION 3

Obligations incombant aux fournisseurs de modèles d'IA à usage général présentant un risque systémique

Article 55

Obligations incombant aux fournisseurs de modèles d'IA à usage général présentant un risque systémique

1. Outre les obligations énumérées aux articles 53 et 54, les fournisseurs de modèles d'IA à usage général présentant un risque systémique:

a) effectuent une évaluation des modèles sur la base de protocoles et d'outils normalisés reflétant l'état de la technique, y compris en réalisant et en documentant des essais contradictoires des modèles en vue d'identifier et d'atténuer les risques systémiques;

b) évaluent et atténuent les risques systémiques éventuels au niveau de l'Union, y compris leurs origines, qui peuvent découler du développement, de la mise sur le marché ou de l'utilisation de modèles d'IA à usage général présentant un risque systémique;

c) suivent, documentent et communiquent sans retard injustifié au Bureau de l'IA et, le cas échéant, aux autorités nationales compétentes les informations pertinentes concernant les incidents graves ainsi que les éventuelles mesures correctives pour y remédier;

d) garantissent un niveau approprié de protection en matière de cybersécurité pour le modèle d'IA à usage général présentant un risque systémique et l'infrastructure physique du modèle.

▼B

2. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique peuvent s'appuyer sur des codes de bonne pratique au sens de l'article 56 pour démontrer qu'ils respectent les obligations énoncées au paragraphe 1 du présent article, jusqu'à la publication d'une norme harmonisée. Le respect des normes européennes harmonisées confère au fournisseur une présomption de conformité dans la mesure où lesdites normes couvrent ces obligations. Les fournisseurs de modèles d'IA à usage général présentant un risque systémique qui n'adhèrent pas à un code de bonnes pratiques approuvé ou ne respectent pas une norme européenne harmonisée démontrent qu'ils disposent d'autres moyens appropriés de mise en conformité et les soumettent à l'appréciation de la Commission.

3. Toute information ou documentation obtenue en vertu du présent article, y compris les secrets d'affaires, est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

SECTION 4

Codes de bonnes pratiques

Article 56

Codes de bonne pratique

1. Le Bureau de l'IA encourage et facilite l'élaboration de codes de bonne pratique au niveau de l'Union afin de contribuer à la bonne application du présent règlement, en tenant compte des approches internationales.

2. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique couvrent au moins les obligations prévues aux articles 53 et 55, y compris les questions suivantes:

a) les moyens de s'assurer que les informations visées à l'article 53, paragraphe 1, points a) et b), sont mises à jour à la lumière des évolutions du marché et des technologies;

b) le niveau approprié de détail pour le résumé du contenu utilisé pour l'entraînement;

c) l'identification du type et de la nature des risques systémiques au niveau de l'Union, y compris leurs origines, le cas échéant;

d) les mesures, procédures et modalités d'évaluation et de gestion des risques systémiques au niveau de l'Union, y compris la documentation y afférente, qui sont proportionnées aux risques, prennent en considération leur gravité et leur probabilité et tiennent compte des défis spécifiques que pose la maîtrise de ces risques à la lumière des différentes façons dont ils peuvent apparaître ou se concrétiser tout au long de la chaîne de valeur de l'IA.

3. Le Bureau de l'IA peut inviter tous les fournisseurs de modèles d'IA à usage général, ainsi que les autorités nationales compétentes concernées, à participer à l'élaboration de codes de bonne pratique. Les organisations de la société civile, l'industrie, le monde universitaire et d'autres parties prenantes concernées, telles que les fournisseurs en aval et les experts indépendants, peuvent apporter leur soutien au processus.

▼B

4. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique définissent clairement leurs objectifs spécifiques et contiennent des engagements ou des mesures, y compris, le cas échéant, des indicateurs de performance clés, afin de garantir la réalisation de ces objectifs, et à ce qu'ils tiennent dûment compte des besoins et des intérêts de l'ensemble des parties intéressées, y compris les personnes concernées, au niveau de l'Union.

5. Le Bureau de l'IA veille à ce que les participants aux codes de bonne pratique fassent régulièrement rapport au Bureau de l'IA sur la mise en œuvre des engagements ainsi que sur les mesures qu'ils adoptent et leurs résultats, y compris mesurés par rapport aux indicateurs de performance clés, le cas échéant. Les indicateurs de performance clés et l'obligation de présenter des rapports reflètent les différences de taille et de capacité entre les différents participants.

6. Le Bureau de l'IA et le Comité IA contrôlent et évaluent régulièrement la réalisation des objectifs des codes de bonne pratique par les participants et leur contribution à la bonne application du présent règlement. Le Bureau de l'IA et le Comité IA évaluent si les codes de bonne pratique couvrent les obligations prévues aux articles 53 et 55, et contrôlent et évaluent régulièrement la réalisation de leurs objectifs. Ils publient leur évaluation de l'adéquation des codes de bonne pratique.

La Commission peut, au moyen d'un acte d'exécution, approuver un code de bonnes pratiques et lui conférer une validité générale au sein de l'Union. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

7. Le Bureau de l'IA peut inviter tous les fournisseurs de modèles d'IA à usage général à adhérer aux codes de bonne pratique. Pour les fournisseurs de modèles d'IA à usage général ne présentant pas de risque systémique, cette adhésion peut se limiter aux obligations prévues à l'article 53, à moins qu'ils ne déclarent explicitement leur intérêt à respecter le code complet.

8. Le Bureau de l'IA encourage et facilite également, le cas échéant, le réexamen et l'adaptation des codes de bonne pratique, en particulier à la lumière des normes émergentes. Le Bureau de l'IA participe à l'évaluation des normes disponibles.

9. Les codes de bonne pratique sont prêts au plus tard le 2 mai 2025. Le Bureau de l'IA prend les mesures nécessaires, y compris inviter les fournisseurs en vertu du paragraphe 7.

Si, à la date du 2 août 2025, un code de bonnes pratiques n'a pas pu être mis au point, ou si le Bureau de l'IA estime qu'il n'est pas approprié à la suite de son évaluation au titre du paragraphe 6 du présent article, la Commission peut prévoir, au moyen d'actes d'exécution, des règles communes pour la mise en œuvre des obligations prévues aux articles 53 et 55, y compris les questions énoncées au paragraphe 2 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

▼B

CHAPITRE VI

MESURES DE SOUTIEN À L'INNOVATION

Article 57

Bacs à sable réglementaires de l'IA

1. Les États membres veillent à ce que leurs autorités compétentes mettent en place au moins un bac à sable réglementaire de l'IA au niveau national, qui est opérationnel au plus tard le 2 août 2026. Ce bac à sable peut également être établi conjointement avec les autorités compétentes d'autres États membres. La Commission peut fournir un soutien technique, des conseils et des outils pour la mise en place et l'exploitation de bacs à sable réglementaires de l'IA.

L'obligation visée au premier alinéa peut également être remplie en participant à un bac à sable existant, pour autant que cette participation offre un niveau de couverture nationale équivalent pour les États membres participants.

2. Des bacs à sable réglementaires de l'IA supplémentaires au niveau régional ou au niveau local, ou établis conjointement avec les autorités compétentes d'autres États membres peuvent également être mis en place.

3. Le Contrôleur européen de la protection des données peut également créer un bac à sable réglementaire de l'IA pour les institutions, organes et organismes de l'Union, et peut exercer les rôles et les tâches des autorités nationales compétentes conformément au présent chapitre.

4. Les États membres veillent à ce que les autorités compétentes visées aux paragraphes 1 et 2 allouent des ressources suffisantes pour se conformer au présent article de manière efficace et en temps utile. Lorsqu'il y a lieu, les autorités nationales compétentes coopèrent avec d'autres autorités concernées et peuvent permettre la participation d'autres acteurs de l'écosystème de l'IA. Le présent article n'a pas d'incidence sur d'autres bacs à sable réglementaires établis en vertu du droit de l'Union ou du droit national. Les États membres assurent un niveau approprié de coopération entre les autorités chargées de la surveillance de ces autres bacs à sable et les autorités nationales compétentes.

5. Les bacs à sable réglementaires de l'IA établis en vertu du paragraphe 1 offrent un environnement contrôlé qui favorise l'innovation et facilite le développement, l'entraînement, la mise à l'essai et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique de bac à sable convenu entre les fournisseurs ou fournisseurs potentiels et l'autorité compétente. Ces bacs à sable peuvent comprendre des essais en conditions réelles qui y sont supervisés.

6. Les autorités compétentes fournissent, s'il y a lieu, des orientations, une surveillance et un soutien dans le cadre du bac à sable réglementaire de l'IA en ce qui concerne l'identification des risques, en particulier pour les droits fondamentaux, la santé et la sécurité, les essais, les mesures d'atténuation et leur efficacité par rapport aux obligations et exigences du présent règlement et, le cas échéant, d'autres dispositions du droit de l'Union et du droit national dont le respect est suivi dans le cadre du bac à sable.

▼B

7. Les autorités compétentes donnent aux fournisseurs et aux fournisseurs potentiels participant au bac à sable réglementaire de l'IA des orientations sur les attentes réglementaires et la manière de satisfaire aux exigences et obligations énoncées dans le présent règlement.

À la demande du fournisseur ou du fournisseur potentiel du système d'IA, l'autorité compétente fournit une preuve écrite des activités menées avec succès dans le bac à sable. L'autorité compétente fournit également un rapport de sortie détaillant les activités menées dans le bac à sable ainsi que les résultats et acquis d'apprentissage correspondants. Les fournisseurs peuvent utiliser ces documents pour démontrer leur conformité avec le présent règlement au moyen de la procédure d'évaluation de la conformité ou d'activités pertinentes de surveillance du marché. À cet égard, les rapports de sortie et la preuve écrite fournie par l'autorité nationale compétente sont évalués de manière positive par les autorités de surveillance du marché et les organismes notifiés, en vue d'accélérer les procédures d'évaluation de la conformité dans une mesure raisonnable.

8. Sous réserve des dispositions relatives à la confidentialité énoncées à l'article 78 et avec l'accord du fournisseur ou du fournisseur potentiel, la Commission et le Comité IA sont autorisés à accéder aux rapports de sortie et en tiennent compte, le cas échéant, dans l'exercice des tâches qui leur incombent en vertu du présent règlement. Si le fournisseur ou le fournisseur potentiel et l'autorité nationale compétente y consentent explicitement, le rapport de sortie peut être mis à la disposition du public par l'intermédiaire de la plateforme d'information unique visée au présent article.

9. La mise en place de bacs à sable réglementaires de l'IA vise à contribuer aux objectifs suivants:

a) améliorer la sécurité juridique afin d'assurer le respect réglementaire du présent règlement ou, le cas échéant, d'autres dispositions applicables du droit de l'Union et du droit national;

b) soutenir le partage des bonnes pratiques par la coopération avec les autorités participant au bac à sable réglementaire de l'IA;

c) favoriser l'innovation et la compétitivité et faciliter la mise en place d'un écosystème d'IA;

d) contribuer à l'apprentissage réglementaire fondé sur des données probantes;

e) faciliter et accélérer l'accès au marché de l'Union pour les systèmes d'IA, en particulier lorsqu'ils sont fournis par des PME, y compris des jeunes pousses.

10. Les autorités nationales compétentes veillent à ce que, dans la mesure où les systèmes d'IA innovants impliquent le traitement de données à caractère personnel ou relèvent à d'autres titres de la surveillance d'autres autorités nationales ou autorités compétentes assurant ou encadrant l'accès aux données, les autorités nationales chargées de la protection des données et ces autres autorités nationales ou autorités compétentes soient associées à l'exploitation du bac à sable réglementaire de l'IA et participent au contrôle des aspects qui relèvent de leurs tâches et pouvoirs respectifs.

11. Les bacs à sable réglementaires de l'IA n'ont pas d'incidence sur les pouvoirs en matière de contrôle ou de mesures correctives des autorités compétentes chargées de la surveillance des bacs à sable, y compris au niveau régional ou local. Tout risque substantiel pour la

▼B

santé, la sécurité et les droits fondamentaux constaté lors du développement et des tests de ces systèmes d'IA donne lieu à des mesures d'atténuation appropriées. Les autorités nationales compétentes sont habilitées à suspendre temporairement ou définitivement le processus d'essai ou la participation au bac à sable si aucune atténuation efficace n'est possible, et elles informent le Bureau de l'IA de cette décision. Les autorités nationales compétentes exercent leurs pouvoirs de surveillance, dans les limites de la législation applicable, en faisant usage de leurs pouvoirs discrétionnaires lorsqu'elles mettent en œuvre des dispositions juridiques relatives à un projet spécifique de bac à sable réglementaire de l'IA, dans le but de soutenir l'innovation dans le domaine de l'IA au sein de l'Union.

12. Les fournisseurs et les fournisseurs potentiels participant au bac à sable réglementaire de l'IA demeurent responsables, en vertu du droit de l'Union et du droit national applicable en matière de responsabilité, de tout préjudice infligé à des tiers en raison de l'expérimentation menée dans le bac à sable. Toutefois, sous réserve du respect par les fournisseurs potentiels du plan spécifique ainsi que des modalités de leur participation et de leur disposition à suivre de bonne foi les orientations fournies par l'autorité nationale compétente, aucune amende administrative n'est infligée par les autorités en cas de violation du présent règlement. Lorsque d'autres autorités compétentes chargées d'autres dispositions du droit de l'Union et du droit national ont participé activement à la surveillance du système d'IA dans le bac à sable et ont fourni des orientations en matière de conformité, aucune amende administrative n'est infligée en ce qui concerne ces dispositions.

13. Les bacs à sable réglementaires de l'IA sont conçus et mis en œuvre de manière à faciliter, le cas échéant, la coopération transfrontière entre les autorités nationales compétentes.

14. Les autorités nationales compétentes coordonnent leurs activités et coopèrent dans le cadre du Comité IA.

15. Les autorités nationales compétentes informent le Bureau de l'IA et le Comité IA de la mise en place d'un bac à sable et peuvent leur demander un soutien et des orientations. Le Bureau de l'IA publie une liste des bacs à sable prévus et existants et la tient à jour afin d'encourager une plus grande interaction dans les bacs à sable réglementaires de l'IA et la coopération transfrontière.

16. Les autorités nationales compétentes présentent des rapports annuels au Bureau de l'IA et au Comité IA, dont le premier est élaboré dans un délai d'un an à compter de la mise en place du bac à sable réglementaire de l'IA, puis tous les ans jusqu'à son terme, et un rapport final. Ces rapports fournissent des informations sur les progrès et les résultats de la mise en œuvre de ces bacs à sable, y compris les bonnes pratiques, les incidents, les enseignements et les recommandations concernant leur mise en place et, le cas échéant, sur l'application et la révision éventuelle du présent règlement, y compris ses actes délégués et actes d'exécution, et sur l'application d'autres dispositions législatives de l'Union contrôlés par les autorités compétentes dans le cadre du bac à sable. Les autorités nationales compétentes publient ces rapports annuels ou des résumés de ceux-ci en ligne. La Commission tient compte, s'il y a lieu, des rapports annuels dans l'exercice de ses tâches au titre du présent règlement.

▼B

17. La Commission développe une interface unique et spécifique contenant toutes les informations pertinentes relatives aux bacs à sable réglementaires de l'IA pour permettre aux parties prenantes d'interagir avec les bacs à sable réglementaires de l'IA et de s'informer auprès des autorités compétentes, ainsi que de demander des orientations non contraignantes sur la conformité de produits, services et modèles commerciaux innovants intégrant les technologies de l'IA, conformément à l'article 62, paragraphe 1, point c). La Commission assure une coordination proactive avec les autorités nationales compétentes, le cas échéant.

Article 58

Modalités détaillées pour les bacs à sable réglementaires de l'IA et fonctionnement de ceux-ci

1. Afin d'éviter une fragmentation à travers l'Union, la Commission adopte des actes d'exécution précisant les modalités détaillées de mise en place, de développement, de mise en œuvre, d'exploitation et de surveillance des bacs à sable réglementaires de l'IA. Les actes d'exécution contiennent des principes communs sur les questions suivantes:

a) les critères d'éligibilité et de sélection pour la participation au bac à sable réglementaire de l'IA;

b) les procédures de demande, de surveillance, de sortie et d'expiration du bac à sable réglementaire de l'IA, ainsi que de participation à celui-ci, y compris le plan du bac à sable et le rapport de sortie;

c) les conditions applicables aux participants.

Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Les actes d'exécution visés au paragraphe 1 garantissent que:

a) les bacs à sable réglementaires de l'IA sont ouverts à tout fournisseur ou fournisseur potentiel d'un système d'IA qui remplit les critères d'éligibilité et de sélection, lesquels sont transparents et équitables, et que les autorités nationales compétentes informent les demandeurs de leur décision dans un délai de trois mois à compter de la demande;

b) que les bacs à sable réglementaires de l'IA permettent un accès étendu et égal et suivent la demande de participation; les fournisseurs et fournisseurs potentiels peuvent également soumettre des demandes en partenariat avec des déployeurs et d'autre tiers concernés;

c) que les modalités détaillées pour les bacs à sable réglementaires de l'IA et les conditions relatives à ces derniers favorisent, dans toute la mesure du possible, la flexibilité permettant aux autorités nationales compétentes de mettre en place et d'exploiter leurs bacs à sable réglementaires de l'IA;

▼B

d) que l'accès aux bacs à sable réglementaires de l'IA est gratuit pour les PME, y compris les jeunes pousses, sans préjudice des coûts exceptionnels que les autorités nationales compétentes peuvent recouvrer de manière équitable et proportionnée;

e) qu'ils aident les fournisseurs et les fournisseurs potentiels, au moyen des acquis d'apprentissage des bacs à sable réglementaires de l'IA, à se conformer aux obligations d'évaluation de la conformité prévues par le présent règlement et à l'application volontaire des codes de conduite visés à l'article 95;

f) que les bacs à sable réglementaires de l'IA facilitent la participation d'autres acteurs pertinents au sein de l'écosystème de l'IA, tels que les organismes notifiés et les organisations de normalisation, les PME, y compris les jeunes pousses, les entreprises, les innovateurs, les installations d'expérimentation et d'essai, les laboratoires de recherche et d'expérimentation et les pôles européens d'innovation numérique, les centres d'excellence, les chercheurs individuels, afin de permettre et de faciliter la coopération avec les secteurs public et privé;

g) que les procédures, processus et exigences administratives applicables en matière de demande, de sélection, de participation et de sortie dans le cadre du bac à sable réglementaires de l'IA sont simples, facilement compréhensibles et clairement communiqués afin de faciliter la participation des PME, y compris des jeunes pousses, disposant de capacités juridiques et administratives limitées, et sont rationalisés dans toute l'Union, afin d'éviter la fragmentation et de permettre que la participation à un bac à sable réglementaire de l'IA mis en place par un État membre ou par le Contrôleur européen de la protection des données soit mutuellement et uniformément reconnue et produise les mêmes effets juridiques dans l'ensemble de l'Union;

h) que la participation au bac à sable réglementaire de l'IA est limitée à une période adaptée à la complexité et à l'envergure du projet, qui peut être prolongée par l'autorité nationale compétente;

i) que les bacs à sable réglementaire de l'IA facilitent le développement d'outils et d'infrastructures pour la mise à l'essai, l'étalonnage des performances, l'évaluation et l'explication des aspects des systèmes d'IA pertinents pour l'apprentissage réglementaire, tels que la précision, la solidité et la cybersécurité, ainsi que les mesures d'atténuation des risques d'atteinte aux droits fondamentaux et à la société au sens large.

3. Les fournisseurs potentiels dans les bacs à sable réglementaires de l'IA, en particulier les PME et les jeunes pousses, sont dirigés, le cas échéant, vers des services préalables au déploiement, tels que des orientations sur la mise en œuvre du présent règlement, et vers d'autres services à valeur ajoutée, tels que l'aide avec les documents de normalisation et la certification, les installations d'essai et d'expérimentation, les pôles européens d'innovation numérique et les centres d'excellence.

4. Lorsque les autorités nationales compétentes envisagent d'autoriser des essais en conditions réelles supervisés dans le cadre d'un bac à sable réglementaire de l'IA établi en vertu du présent article, elles conviennent spécifiquement des conditions de ces essais et, en particulier, des garanties appropriées avec les participants en vue de protéger les droits fondamentaux, la santé et la sécurité. Le cas échéant, elles coopèrent avec d'autres autorités nationales compétentes en vue d'assurer la cohérence des pratiques dans l'ensemble de l'Union.

▼B

Article 59

Traitement ultérieur de données à caractère personnel en vue du développement de certains systèmes d'IA dans l'intérêt public dans le cadre du bac à sable réglementaire de l'IA

1. Dans le bac à sable réglementaire de l'IA, les données à caractère personnel collectées légalement à d'autres fins peuvent être traitées uniquement aux fins du développement, de l'entraînement et de la mise à l'essai de certains systèmes d'IA dans le bac à sable, lorsque l'ensemble des conditions suivantes sont remplies:

a) les systèmes d'IA sont développés pour préserver des intérêts publics importants par une autorité publique ou une autre personne physique ou morale et dans un ou plusieurs des domaines suivants:

   i) la sécurité publique et la santé publique, y compris la détection, le diagnostic, la prévention, le contrôle et le traitement des maladies ainsi que l'amélioration des systèmes de soins de santé;

   ii) un niveau élevé de protection et d'amélioration de la qualité de l'environnement, la protection de la biodiversité, la protection contre la pollution, les mesures de transition écologique et les mesures d'atténuation du changement climatique et d'adaptation à celui-ci;

   iii) la durabilité énergétique;

   iv) la sécurité et la résilience des systèmes de transport et de la mobilité, des infrastructures critiques et des réseaux de transport;

   v) l'efficacité et la qualité de l'administration publique et des services publics;

b) les données traitées sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au chapitre III, section 2, lorsque ces exigences ne peuvent être satisfaites de manière efficace en traitant des données anonymisées, synthétiques ou autres à caractère non personnel;

c) il existe des mécanismes de suivi efficaces pour déterminer si des risques élevés pour les droits et les libertés des personnes concernées, visés à l'article 35 du règlement (UE) 2016/679 et à l'article 39 du règlement (UE) 2018/1725, sont susceptibles de survenir lors de l'expérimentation menée dans le cadre du bac à sable, ainsi que des mécanismes de réponse permettant d'atténuer rapidement ces risques et, au besoin, de faire cesser le traitement des données;

d) les données à caractère personnel à traiter dans le cadre du bac à sable se trouvent dans un environnement de traitement des données séparé, isolé et protégé sur le plan fonctionnel, placé sous le contrôle du fournisseur potentiel, et seules les personnes autorisées ont accès à ces données;

e) les fournisseurs ne peuvent en outre partager les données initialement collectées que conformément au droit de l'Union en matière de protection des données; aucune donnée à caractère personnel créée dans le bac à sable ne peut être partagée en dehors du bac à sable;

f) aucun traitement de données à caractère personnel effectué dans le cadre du bac à sable ne débouche sur des mesures ou des décisions affectant les personnes concernées ni n'a d'incidence sur l'application des droits que leur confère le droit de l'Union en matière de protection des données à caractère personnel;

▼B

g) les données à caractère personnel traitées dans le cadre du bac à sable sont protégées par des mesures techniques et organisationnelles appropriées et supprimées une fois que la participation au bac à sable a cessé ou que la période de conservation de ces données à caractère personnel a expiré;

h) les registres du traitement des données à caractère personnel dans le cadre du bac à sable sont conservés pendant la durée de la participation au bac à sable, sauf disposition contraire du droit de l'Union ou du droit national;

i) une description complète et détaillée du processus et de la justification de l'entraînement, de la mise à l'essai et de la validation du système d'IA est conservée avec les résultats des essais, et fait partie de la documentation technique visée à l'annexe IV;

j) un résumé succinct du projet d'IA développé dans le cadre du bac à sable, de ses objectifs et des résultats escomptés est publié sur le site web des autorités compétentes; cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

2. Aux fins de la prévention et de la détection d'infractions pénales, ainsi que des enquêtes et des poursuites en la matière ou de l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, sous le contrôle et la responsabilité des autorités répressives, le traitement des données à caractère personnel dans les bacs à sable réglementaires de l'IA est fondé sur une disposition spécifique du droit de l'Union ou du droit national et soumis aux mêmes conditions cumulatives que celles visées au paragraphe 1.

3. Le paragraphe 1 est sans préjudice du droit de l'Union ou du droit national excluant le traitement des données à caractère personnel à des fins autres que celles expressément mentionnées dans ce droit, ainsi que sans préjudice du droit de l'Union ou du droit national établissant le fondement du traitement des données à caractère personnel qui est nécessaire aux fins du développement, de la mise à l'essai et de l'entraînement de systèmes d'IA innovants, ou de toute autre base juridique, dans le respect du droit de l'Union relatif à la protection des données à caractère personnel.

Article 60

Essais de systèmes d'IA à haut risque en conditions réelles en dehors des bacs à sable réglementaires de l'IA

1. Les essais de systèmes d'IA à haut risque en conditions réelles en dehors des bacs à sable réglementaires de l'IA peuvent être effectués par les fournisseurs ou fournisseurs potentiels de systèmes d'IA à haut risque énumérés à l'annexe III, conformément au présent article et au plan d'essais en conditions réelles visé au présent article, sans préjudice des interdictions prévues à l'article 5.

La Commission précise, par voie d'actes d'exécution, les éléments détaillés du plan d'essais en conditions réelles. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

Le présent paragraphe est sans préjudice du droit de l'Union ou du droit national relatif aux essais en conditions réelles de systèmes d'IA à haut risque liés aux produits qui relèvent de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I.

▼B

2. Les fournisseurs ou fournisseurs potentiels peuvent effectuer, seuls ou en partenariat avec un ou plusieurs déployeurs ou déployeurs potentiels, des essais des systèmes d'IA à haut risque visés à l'annexe III, en conditions réelles, à tout moment avant la mise sur le marché ou la mise en service du système d'IA concerné.

3. Les essais de systèmes d'IA à haut risque en conditions réelles au titre du présent article sont sans préjudice de tout examen éthique exigé par le droit de l'Union ou le droit national.

4. Les fournisseurs ou fournisseurs potentiels ne peuvent effectuer les essais en conditions réelles que si toutes les conditions suivantes sont remplies:

a) le fournisseur ou le fournisseur potentiel a établi un plan d'essais en conditions réelles et l'a soumis à l'autorité de surveillance du marché dans l'État membre où les essais en conditions réelles doivent être réalisés;

b) l'autorité de surveillance du marché de l'État membre où les essais en conditions réelles doivent être réalisés a approuvé les essais en conditions réelles et le plan d'essais en conditions réelles; lorsque l'autorité de surveillance du marché n'a pas fourni de réponse dans un délai de 30 jours, les essais en conditions réelles et le plan d'essais en conditions réelles sont réputés approuvés; lorsque le droit national ne prévoit pas d'approbation tacite, les essais en conditions réelles restent soumis à autorisation;

c) le fournisseur ou fournisseur potentiel, à l'exception des fournisseurs ou fournisseurs potentiels de systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, ainsi que des systèmes d'IA à haut risque visés à l'annexe III, point 2, a enregistré les essais en conditions réelles dans la partie non publique de la base de données de l'UE visée à l'article 71, paragraphe 4, avec un numéro d'identification unique à l'échelle de l'Union et les informations indiquées à l'annexe IX; le fournisseur ou fournisseur potentiel de systèmes d'IA à haut risque visé à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, a enregistré les essais en conditions réelles dans la partie non publique de la base de données de l'UE visée à l'article 49, paragraphe 4, point d), avec un numéro d'identification unique à l'échelle de l'Union et les informations y indiquées; le fournisseur ou fournisseur potentiel de systèmes d'IA à haut risque visé à l'annexe III, point 2, a enregistré les essais en conditions réelles conformément à l'article 49, paragraphe 5.

d) le fournisseur ou fournisseur potentiel effectuant les essais en conditions réelles est établi dans l'Union ou a désigné un représentant légal établi dans l'Union;

e) les données collectées et traitées aux fins des essais en conditions réelles ne sont transférées vers des pays tiers qu'à condition que des garanties appropriées et applicables en vertu du droit de l'Union soient en place;

f) les essais en conditions réelles ne durent pas plus longtemps que nécessaire pour atteindre leurs objectifs et, en tout état de cause, pas plus de six mois, qui peuvent être prolongés pour une période supplémentaire de six mois, sous réserve d'une notification préalable par le fournisseur ou fournisseur potentiel à l'autorité de surveillance du marché, accompagnée d'une explication des raisons qui motivent une telle prolongation;

▼B

g) les participants aux essais en conditions réelles qui sont des personnes appartenant à des groupes vulnérables en raison de leur âge ou de leur handicap sont dûment protégées;

h) lorsqu'un fournisseur ou un fournisseur potentiel organise les essais en conditions réelles en coopération avec un ou plusieurs déployeurs ou déployeurs potentiels, ces derniers ont été préalablement informés de tous les aspects des essais qui sont pertinents pour leur décision de participer et ont reçu les instructions d'utilisation adéquates pour le système d'IA visé à l'article 13; le fournisseur ou fournisseur potentiel et le déployeur ou déployeur potentiel concluent un accord précisant leurs rôles et responsabilités en vue d'assurer le respect des dispositions relatives aux essais en conditions réelles prévues par le présent règlement et en vertu d'autres dispositions applicables du droit de l'Union et du droit national;

i) les participants aux essais en conditions réelles ont donné leur consentement éclairé conformément à l'article 61 ou, dans le cas des services répressifs, lorsque la recherche d'un consentement éclairé empêcherait de réaliser les essais du système d'IA, les essais proprement dits et les résultats des essais en conditions réelles n'ont pas d'effet négatif sur les participants, et leurs données à caractère personnel sont supprimées une fois les essais réalisés;

j) le fournisseur ou le fournisseur potentiel ainsi que les déployeurs ou les déployeurs potentiels effectuent un contrôle effectif des essais en conditions réelles, par des personnes dûment qualifiées dans le domaine concerné et disposant des capacités, de la formation et de l'autorité nécessaires pour accomplir leurs tâches;

k) les prévisions, recommandations ou décisions du système d'IA peuvent effectivement être infirmées et ignorées.

5. Tout participant aux essais en conditions réelles, ou son représentant légal, selon le cas, peut, sans encourir de préjudice et sans devoir se justifier, se retirer des essais à tout moment, en révoquant son consentement éclairé et peut demander la suppression immédiate et définitive de ses données à caractère personnel. Le retrait du consentement éclairé n'affecte pas les activités déjà menées.

6. Conformément à l'article 75, les États membres confèrent à leurs autorités de surveillance du marché le pouvoir d'exiger des fournisseurs et des fournisseurs potentiels qu'ils fournissent des informations, de procéder à des inspections inopinées à distance ou sur place et d'effectuer des vérifications concernant la réalisation des essais en conditions réelles et des systèmes d'IA à haut risque connexes. Les autorités de surveillance du marché utilisent ces pouvoirs pour veiller au développement sûr des essais en conditions réelles.

7. Tout incident grave constaté au cours des essais en conditions réelles est signalé à l'autorité nationale de surveillance du marché, conformément à l'article 73. Le fournisseur ou fournisseur potentiel adopte des mesures d'atténuation immédiates ou, à défaut, suspend les essais en conditions réelles jusqu'à ce que cette atténuation soit effective ou y met fin en l'absence d'atténuation. Le fournisseur ou fournisseur potentiel établit une procédure pour le rappel rapide du système d'IA lors de la cessation des essais en conditions réelles.

▼B

8. Les fournisseurs ou fournisseurs potentiels informent l'autorité nationale de surveillance du marché de l'État membre où les essais en conditions réelles doivent être réalisés de la suspension ou de la cessation des essais en conditions réelles et des résultats finaux.

9. Le fournisseur ou le fournisseur potentiel sont responsables, en vertu du droit de l'Union et du droit national applicable en matière de responsabilité, de tout préjudice causé durant les essais en conditions réelles.

Article 61

Consentement éclairé à participer aux essais en conditions réelles en dehors des bacs à sable réglementaires de l'IA

1. Aux fins des essais en conditions réelles visés à l'article 60, le consentement éclairé donné librement est obtenu des participants aux essais avant que ceux-ci ne prennent part à ces essais et après qu'ils ont été dûment informés au moyen d'informations concises, claires, pertinentes et compréhensibles concernant:

a) la nature et les objectifs des essais en conditions réelles ainsi que les désagréments éventuels pouvant être liés à sa participation;

b) les conditions dans lesquelles les essais en conditions réelles doivent être réalisés, y compris la durée prévue de la participation;

c) les droits et garanties concernant leur participation, en particulier leur droit de refuser de participer aux essais en conditions réelles et leur droit de s'en retirer à tout moment sans encourir de préjudice et sans devoir se justifier;

d) les modalités selon lesquelles il peut être demandé que des prévisions, recommandations ou décisions du système d'IA soient infirmées ou ignorées;

e) le numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles conformément à l'article 60, paragraphe 4, point c), et les coordonnées du fournisseur ou de son représentant légal auprès duquel des informations complémentaires peuvent être obtenues.

2. Le consentement éclairé est daté et documenté et une copie en est remise aux participants aux essais ou à leur représentant légal.

Article 62

Mesures en faveur des fournisseurs et déployeurs, en particulier les PME, y compris les jeunes pousses

1. Les États membres:

a) accordent aux PME, y compris les jeunes pousses, qui ont leur siège social ou une succursale dans l'Union, un accès prioritaire aux bacs à sable réglementaires de l'IA, dans la mesure où elles remplissent les conditions d'éligibilité et les critères de sélection; l'accès prioritaire n'empêche pas d'autres PME, y compris les jeunes pousses, autres que celles visées au présent alinéa, d'accéder au bac à sable réglementaire de l'IA, pour autant qu'elles remplissent également les conditions d'éligibilité et les critères de sélection;

▼B

b) organisent des activités spécifiques de sensibilisation et de formation à l'application du présent règlement, adaptées aux besoins des PME, y compris les jeunes pousses, les déployeurs et, si nécessaire, les pouvoirs publics locaux;

c) utilisent des canaux privilégiés existants et, s'il y a lieu, en établissent de nouveaux avec les PME, y compris les jeunes pousses, les déployeurs, d'autres innovateurs et, si nécessaire, les pouvoirs publics locaux, afin de fournir des conseils et de répondre aux questions relatives à la mise en œuvre du présent règlement, y compris en ce qui concerne la participation à des bacs à sable réglementaires de l'IA;

d) facilitent la participation des PME et d'autres parties concernées au processus d'élaboration de la normalisation.

2. Les intérêts et les besoins spécifiques des PME fournisseuses, y compris les jeunes pousses, sont pris en considération lors de la fixation des frais liés à l'évaluation de la conformité visée à l'article 43, ces frais étant réduits proportionnellement à leur taille, à la taille de leur marché et à d'autres indicateurs pertinents.

3. Le Bureau de l'IA:

a) fournit des modèles normalisés pour les domaines qui relèvent du présent règlement, comme précisé par le Comité IA dans sa demande;

b) met au point et tient à jour une plateforme d'information unique fournissant des informations faciles à utiliser en rapport avec le présent règlement pour tous les opérateurs dans l'ensemble de l'Union;

c) organise des campagnes de communication appropriées pour sensibiliser aux obligations découlant du présent règlement;

d) évalue et promeut la convergence des bonnes pratiques en matière de procédures de passation de marchés publics en ce qui concerne les systèmes d'IA.

Article 63

Dérogations pour des opérateurs spécifiques

1. Les microentreprises au sens de la recommandation 2003/361/CE peuvent se conformer de manière simplifiée à certains éléments du système de gestion de la qualité requis par l'article 17 du présent règlement, pour autant qu'elles n'aient pas d'entreprises partenaires ou d'entreprises liées au sens de ladite recommandation. À cette fin, la Commission élabore des lignes directrices sur les éléments du système de gestion de la qualité qui peuvent être respectés de manière simplifiée en tenant compte des besoins des microentreprises, sans affecter le niveau de protection ni la nécessité de se conformer aux exigences relatives aux systèmes d'IA à haut risque.

2. Le paragraphe 1 du présent article ne peut être interprété comme dispensant ces opérateurs de satisfaire à d'autres exigences ou obligations prévues par le présent règlement, y compris celles établies aux articles 9, 10, 11, 12, 13, 14, 15, 72 et 73.

▼B

CHAPITRE VII

GOUVERNANCE

SECTION 1

Gouvernance au niveau de l'Union

Article 64

Bureau de l'IA

1. La Commission développe l'expertise et les capacités de l'Union dans le domaine de l'IA par l'intermédiaire du Bureau de l'IA.

2. Les États membres facilitent l'accomplissement des tâches confiées au Bureau de l'IA, telles qu'elles sont définies dans le présent règlement.

Article 65

Création et structure du Comité européen de l'intelligence artificielle

1. Un Comité européen de l'intelligence artificielle (ci-après dénommé «Comité IA») est créé.

2. Le Comité IA est composé d'un représentant par État membre. Le Contrôleur européen de la protection des données participe en qualité d'observateur. Le Bureau de l'IA assiste également aux réunions du Comité IA sans toutefois prendre part aux votes. D'autres autorités, organes ou experts nationaux et de l'Union peuvent être invités aux réunions par le Comité IA au cas par cas, lorsque les questions examinées relèvent de leurs compétences.

3. Chaque représentant est désigné par son État membre pour une période de trois ans, renouvelable une fois.

4. Les États membres veillent à ce que leurs représentants au sein du Comité IA:

a) disposent des compétences et pouvoirs pertinents dans leur État membre afin de contribuer activement à l'accomplissement des tâches du Comité IA visées à l'article 66;

b) soient désignés comme point de contact unique vis-à-vis du Comité IA et, lorsqu'il y a lieu, compte tenu des besoins des États membres, comme point de contact unique pour les parties prenantes;

c) soient habilités à faciliter la cohérence et la coordination entre les autorités nationales compétentes de leur État membre en ce qui concerne la mise en œuvre du présent règlement, y compris par la collecte de données et d'informations pertinentes aux fins de l'accomplissement de leurs tâches au sein du Comité IA.

5. Les représentants désignés des États membres adoptent le règlement intérieur du Comité IA à la majorité des deux tiers. Le règlement intérieur établit, en particulier, les procédures de sélection, la durée du mandat et les spécifications des missions du président, les modalités de vote détaillées et l'organisation des activités du Comité IA et de celles de ses sous-groupes.

▼B

6. Le Comité IA établit deux sous-groupes permanents chargés de fournir une plateforme de coopération et d'échange entre les autorités de surveillance du marché et les autorités notifiantes au sujet des questions liées à la surveillance du marché et aux organismes notifiés respectivement.

Le sous-groupe permanent pour la surveillance du marché devrait agir au titre de groupe de coopération administrative (ADCO) pour le présent règlement au sens de l'article 30 du règlement (UE) 2019/1020.

Le Comité IA peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le cas échéant, des représentants du forum consultatif visé à l'article 67 peuvent être invités à ces sous-groupes ou à des réunions spécifiques de ces sous-groupes en qualité d'observateurs.

7. Le Comité IA est organisé et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités.

8. Le Comité IA est présidé par l'un des représentants des États membres. Le Bureau de l'IA assure le secrétariat du Comité IA, convoque les réunions à la demande du président et prépare l'ordre du jour conformément aux tâches du Comité IA au titre du présent règlement et à son règlement intérieur.

Article 66

Tâches du Comité IA

Le Comité IA conseille et assiste la Commission et les États membres afin de faciliter l'application cohérente et efficace du présent règlement. À cette fin, le Comité IA peut notamment:

a) contribuer à la coordination entre les autorités nationales compétentes chargées de l'application du présent règlement et, en coopération avec les autorités de surveillance du marché concernées et sous réserve de leur accord, soutenir les activités conjointes des autorités de surveillance du marché visées à l'article 74, paragraphe 11;

b) recueillir l'expertise technique et réglementaire ainsi que les bonnes pratiques et les partager entre les États membres;

c) fournir des conseils sur la mise en œuvre du présent règlement, en particulier en ce qui concerne le contrôle de l'application des règles relatives aux modèles d'IA à usage général;

d) contribuer à l'harmonisation des pratiques administratives dans les États membres, y compris en ce qui concerne la dérogation à la procédure d'évaluation de la conformité visée à l'article 46, le fonctionnement des bacs à sable réglementaires de l'IA et les essais en conditions réelles visés aux articles 57, 59 et 60;

e) à la demande de la Commission ou de sa propre initiative, émettre des recommandations et des avis écrits sur toute question pertinente liée à la mise en œuvre du présent règlement et à son application cohérente et efficace, y compris:

   i) sur l'élaboration et l'application de codes de conduite et de codes de bonne pratique conformément au présent règlement, ainsi que des lignes directrices de la Commission;

▼B

ii) sur l'évaluation et le réexamen du présent règlement conformément à l'article 112, y compris en ce qui concerne les signalements d'incidents graves visés à l'article 73, le fonctionnement de la base de données de l'UE visée à l'article 71, l'élaboration des actes délégués ou des actes d'exécution, ainsi que les alignements éventuels du présent règlement sur les dispositions d'harmonisation de la législation de l'Union figurant à l'annexe I;

iii) sur les spécifications techniques ou les normes existantes se rapportant aux exigences énoncées au chapitre III, section 2;

iv) sur l'utilisation des normes harmonisées ou des spécifications communes visées aux articles 40 et 41;

v) sur les tendances, telles que la compétitivité mondiale de l'Europe dans le domaine de l'IA, l'adoption de l'IA dans l'Union et le développement des compétences numériques;

vi) sur les tendances concernant l'évolution de la typologie des chaînes de valeur de l'IA, en particulier en ce qui concerne les conséquences qui en découlent en termes de responsabilité;

vii) sur la nécessité éventuelle de modifier l'annexe III conformément à l'article 7, et sur la nécessité éventuelle d'une révision de l'article 5 conformément à l'article 112, en tenant compte des éléments probants pertinents disponibles et des dernières évolutions technologiques;

f) soutenir la Commission afin de promouvoir la maîtrise de l'IA, la sensibilisation du public et la compréhension des avantages, des risques, des garanties, des droits et des obligations liés à l'utilisation des systèmes d'IA;

g) faciliter l'élaboration de critères communs et d'une interprétation commune, entre les opérateurs du marché et les autorités compétentes, des concepts pertinents prévus par le présent règlement, y compris en contribuant au développement de critères de référence;

h) coopérer, lorsqu'il y a lieu, avec d'autres institutions, organes et organismes de l'Union, ainsi que des groupes d'experts et réseaux compétents de l'Union, en particulier dans les domaines de la sécurité des produits, de la cybersécurité, de la concurrence, des services numériques et des services de médias, des services financiers, de la protection des consommateurs, de la protection des données et des droits fondamentaux;

i) contribuer à une coopération efficace avec les autorités compétentes de pays tiers et des organisations internationales;

j) aider les autorités nationales compétentes et la Commission à développer l'expertise organisationnelle et technique nécessaire à la mise en œuvre du présent règlement, y compris en contribuant à l'évaluation des besoins de formation du personnel des États membres participant à la mise en œuvre du présent règlement;

k) aider le Bureau de l'IA à soutenir les autorités nationales compétentes dans la mise en place et le développement de bacs à sable réglementaires de l'IA, et faciliter la coopération et le partage d'informations entre les bacs à sable réglementaires de l'IA;

l) contribuer à l'élaboration de documents d'orientation et fournir des conseils pertinents en la matière;

▼B

m) conseiller la Commission sur les questions internationales en matière d'IA;

n) fournir des avis à la Commission sur les alertes qualifiées concernant les modèles d'IA à usage général;

o) recevoir des avis des États membres sur les alertes qualifiées concernant les modèles d'IA à usage général, ainsi que sur les expériences et pratiques nationales en matière de suivi et de contrôle de l'application des systèmes d'IA, en particulier des systèmes intégrant les modèles d'IA à usage général.

Article 67

Forum consultatif

1. Un forum consultatif est créé pour fournir une expertise technique et conseiller le Comité IA et la Commission, ainsi que pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.

2. La composition du forum consultatif est équilibrée en ce qui concerne la représentation des parties prenantes, y compris l'industrie, les jeunes pousses, les PME, la société civile et le monde universitaire. La composition du forum consultatif est équilibrée sur le plan des intérêts commerciaux et non commerciaux et, dans la catégorie des intérêts commerciaux, en ce qui concerne les PME et les autres entreprises.

3. La Commission nomme les membres du forum consultatif, conformément aux critères énoncés au paragraphe 2, parmi les parties prenantes possédant une expertise reconnue dans le domaine de l'IA.

4. La durée du mandat des membres du forum consultatif est de deux ans et peut être prolongée au maximum de quatre ans.

5. L'Agence des droits fondamentaux, l'ENISA, le Comité européen de normalisation (CEN), le Comité européen de normalisation électrotechnique (CENELEC) et l'Institut européen de normalisation des télécommunications (ETSI) sont membres permanents du forum consultatif.

6. Le forum consultatif établit son règlement intérieur. Il élit parmi ses membres deux coprésidents, conformément aux critères énoncés au paragraphe 2. Leur mandat est d'une durée de deux ans, renouvelable une fois.

7. Le forum consultatif tient des réunions régulières au moins deux fois par an. Il peut inviter des experts et d'autres parties prenantes à ses réunions.

8. Le forum consultatif peut préparer des avis, des recommandations et des contributions écrites à la demande du Comité IA ou de la Commission.

9. Le forum consultatif peut créer des sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques liées aux objectifs du présent règlement.

10. Le forum consultatif prépare un rapport annuel sur ses activités. Ce rapport est rendu public.

▼B

Article 68

Groupe scientifique d'experts indépendants

1. La Commission adopte, au moyen d'un acte d'exécution, des dispositions relatives à la constitution d'un groupe scientifique d'experts indépendants (ci-après dénommé «groupe scientifique») destiné à soutenir les activités de contrôle de l'application du présent règlement. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

2. Le groupe scientifique est composé d'experts sélectionnés par la Commission en fonction de leur expertise à la pointe des connaissances scientifiques ou techniques dans le domaine de l'IA, nécessaire pour s'acquitter des tâches énoncées au paragraphe 3, et est en mesure de démontrer qu'ils remplissent toutes les conditions suivantes:

a) disposer d'une expertise et d'une compétence particulières ainsi que d'une expertise scientifique ou technique dans le domaine de l'IA;

b) être indépendant vis-à-vis de tout fournisseur de systèmes d'IA ou de modèles d'IA à usage général;

c) être capable de mener des activités avec diligence, précision et objectivité.

La Commission, en consultation avec le Comité IA, détermine le nombre d'experts au sein du groupe scientifique en fonction des besoins et veille à une représentation équitable entre les hommes et les femmes ainsi que sur le plan géographique.

3. Le groupe scientifique conseille et soutient le Bureau de l'IA, notamment en ce qui concerne les tâches suivantes:

a) soutenir la mise en œuvre et le contrôle de l'application du présent règlement en ce qui concerne les modèles et systèmes d'IA à usage général, en particulier:

   i) en alertant le Bureau de l'IA au sujet d'éventuels risques systémiques posés au niveau de l'Union par des modèles d'IA à usage général, conformément à l'article 90;

   ii) en contribuant à la mise au point d'outils et de méthodologies destinés à évaluer les capacités des modèles et systèmes d'IA à usage général, y compris au moyen de critères de référence;

   iii) en fournissant des conseils quant à la classification des modèles d'IA à usage général présentant un risque systémique;

   iv) en fournissant des conseils quant à la classification de différents modèles et systèmes d'IA à usage général;

   v) en contribuant à la mise au point d'outils et de modèles;

b) soutenir, à leur demande, les autorités de surveillance du marché dans leur travail;

c) soutenir les activités transfrontières de surveillance du marché visées à l'article 74, paragraphe 11, sans préjudice des pouvoirs des autorités de surveillance du marché;

d) soutenir le Bureau de l'IA dans l'exercice de ses fonctions dans le cadre de la procédure de sauvegarde de l'Union prévue à l'article 81.

▼B

4. Les experts du groupe scientifique s'acquittent de leurs tâches avec impartialité et objectivité, et garantissent la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités. Ils ne sollicitent ni n'acceptent d'instructions de quiconque dans l'exercice des tâches qui leur incombent en vertu du paragraphe 3. Chaque expert établit une déclaration d'intérêts qui est rendue publique. Le Bureau de l'IA met en place des systèmes et des procédures visant à prévenir et gérer efficacement les conflits d'intérêts potentiels.

5. L'acte d'exécution visé au paragraphe 1 comprend des dispositions sur les conditions, les procédures et les modalités détaillées permettant au groupe scientifique et à ses membres d'émettre des alertes et de demander l'assistance du Bureau de l'IA pour l'exécution des tâches du groupe scientifique.

Article 69

Accès des États membres au groupe scientifique

1. Les États membres peuvent faire appel à des experts du groupe scientifique pour soutenir leurs activités de contrôle de l'application du présent règlement.

2. Les États membres peuvent être tenus de payer des honoraires pour les conseils et le soutien fournis par les experts. La structure et le niveau des honoraires ainsi que le barème et la structure des dépens récupérables sont définis dans l'acte d'exécution visé à l'article 68, paragraphe 1, en tenant compte des objectifs consistant à mettre en œuvre le présent règlement de façon appropriée, à assurer un bon rapport coût-efficacité et à garantir que tous les États membres aient un accès effectif à des experts.

3. La Commission facilite l'accès en temps utile des États membres aux experts, en fonction des besoins, et veille à ce que la combinaison des activités de soutien menées par les structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 84 et par les experts au titre du présent article soit organisée de manière efficace et apporte la meilleure valeur ajoutée possible.

SECTION 2

Autorités nationales compétentes

Article 70

Désignation des autorités nationales compétentes et des points de contact uniques

1. Chaque État membre établit ou désigne en tant qu'autorités nationales compétentes au moins une autorité notifiante et au moins une autorité de surveillance du marché aux fins du présent règlement. Ces autorités nationales compétentes exercent leurs pouvoirs de manière indépendante, impartiale et sans parti pris, afin de préserver l'objectivité de leurs activités et de leurs tâches et d'assurer l'application et la mise en œuvre du présent règlement. Les membres de ces autorités s'abstiennent de tout acte incompatible avec leurs fonctions. Pour autant que ces principes soient respectés, les activités et tâches précitées peuvent être exécutées par une ou plusieurs autorités désignées, en fonction des besoins organisationnels de l'État membre.

▼B

2. Les États membres communiquent à la Commission les autorités notifiantes et les autorités de surveillance du marché désignées et les tâches incombant à ces autorités, ainsi que toute modification ultérieure y afférente. Les États membres rendent publiques des informations sur la manière dont les autorités compétentes et les points de contact uniques peuvent être contactés, par voie électronique, au plus tard le 2 août 2025. Les États membres désignent une autorité de surveillance du marché pour faire office de point de contact unique pour le présent règlement et communiquent à la Commission l'identité du point de contact unique. La Commission publie une liste des points de contact uniques.

3. Les États membres veillent à ce que leurs autorités nationales compétentes disposent de ressources techniques, financières et humaines suffisantes, ainsi que d'infrastructures pour mener à bien efficacement les tâches qui leur sont confiées en vertu du présent règlement. En particulier, les autorités nationales compétentes disposent en permanence d'un personnel en nombre suffisant, qui possède, parmi ses compétences et son expertise, une compréhension approfondie des technologies de l'IA, des données et du traitement de données, de la protection des données à caractère personnel, de la cybersécurité, des droits fondamentaux, des risques pour la santé et la sécurité, et une connaissance des normes et exigences légales en vigueur. Chaque année, les États membres évaluent et, si nécessaire, mettent à jour les exigences portant sur les compétences et les ressources visées au présent paragraphe.

4. Les autorités nationales compétentes prennent des mesures appropriées pour garantir un niveau adapté de cybersécurité.

5. Dans le cadre de l'accomplissement de leurs tâches, les autorités nationales compétentes agissent conformément aux obligations de confidentialité énoncées à l'article 78.

6. Au plus tard le 2 août 2025, et tous les deux ans par la suite, les États membres font rapport à la Commission sur l'état des ressources financières et humaines des autorités nationales compétentes, et lui présentent une évaluation de l'adéquation de ces ressources. La Commission transmet ces informations au Comité IA pour discussion et recommandations éventuelles.

7. La Commission facilite les échanges d'expériences entre les autorités nationales compétentes.

8. Les autorités nationales compétentes peuvent fournir des orientations et des conseils sur la mise en œuvre du présent règlement, en particulier aux PME, y compris les jeunes pousses, en tenant compte des orientations et conseils du Comité IA et de la Commission, selon le cas. Chaque fois que les autorités nationales compétentes envisagent de fournir des orientations et des conseils concernant un système d'IA dans des domaines relevant d'autres actes législatifs de l'Union, les autorités compétentes nationales en vertu de ces actes législatifs de l'Union sont consultées, le cas échéant.

9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données agit en tant qu'autorité compétente responsable de leur surveillance.

▼B

CHAPITRE VIII

BASE DE DONNÉES DE L'UE POUR LES SYSTÈMES D'IA À HAUT RISQUE

Article 71

Base de données de l'UE pour les systèmes d'IA à haut risque énumérés à l'annexe III

1. La Commission, en collaboration avec les États membres, crée et tient à jour une base de données de l'UE contenant les informations visées aux paragraphes 2 et 3 du présent article en ce qui concerne les systèmes d'IA à haut risque visés à l'article 6, paragraphe 2, qui sont enregistrés conformément aux articles 49 et 60 et les systèmes d'IA qui ne sont pas considérés à haut risque en vertu de l'article 6, paragraphe 3, et qui sont enregistrés conformément à l'article 6, paragraphe 4, et à l'article 49. Lorsqu'elle définit les spécifications fonctionnelles de cette base de données, la Commission consulte les experts compétents et, lorsqu'elle les met à jour, elle consulte le Comité IA.

2. Les données énumérées à l'annexe VIII, sections A et B, sont introduites dans la base de données de l'UE par le fournisseur ou, le cas échéant, par le mandataire.

3. Les données énumérées à la section C de l'annexe VIII sont introduites dans la base de données de l'UE par le déployeur qui est ou agit pour le compte d'une autorité, d'une agence ou d'un organisme public, conformément à l'article 49, paragraphes 3 et 4.

4. À l'exception de la section visée à l'article 49, paragraphe 4, et à l'article 60, paragraphe 4, point c), les informations contenues dans la base de données de l'UE enregistrées conformément à l'article 49 sont accessibles et mises à la disposition du public d'une manière conviviale. Ces informations devraient être consultables grâce à une navigation aisée et lisibles par machine. Les informations enregistrées conformément à l'article 60 ne sont accessibles qu'aux autorités de surveillance du marché et à la Commission, sauf si le fournisseur ou fournisseur potentiel a donné son consentement pour que ces informations soient également accessibles au public.

5. La base de données de l'UE ne contient des données à caractère personnel que dans la mesure où celles-ci sont nécessaires à la collecte et au traitement d'informations conformément au présent règlement. Ces informations incluent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et légalement autorisées à représenter le fournisseur ou le déployeur, selon le cas.

6. La Commission est la responsable du traitement pour la base de données de l'UE. Elle met à la disposition des fournisseurs, des fournisseurs potentiels et des déployeurs un soutien technique et administratif approprié. La base de données de l'UE est conforme aux exigences applicables en matière d'accessibilité.

▼B

CHAPITRE IX

SURVEILLANCE APRÈS COMMERCIALISATION, PARTAGE D'INFORMATIONS ET SURVEILLANCE DU MARCHÉ

SECTION 1

Surveillance après commercialisation

Article 72

Surveillance après commercialisation par les fournisseurs et plan de surveillance après commercialisation pour les systèmes d'IA à haut risque

1. Les fournisseurs établissent et documentent un système de surveillance après commercialisation d'une manière qui soit proportionnée à la nature des technologies d'IA et des risques du système d'IA à haut risque.

2. Le système de surveillance après commercialisation collecte, documente et analyse, de manière active et systématique, les données pertinentes qui peuvent être fournies par les déployeurs ou qui peuvent être collectées via d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur cycle de vie, et qui permettent au fournisseur d'évaluer si les systèmes d'IA respectent en permanence les exigences énoncées au chapitre III, section 2. Le cas échéant, la surveillance après commercialisation comprend une analyse de l'interaction avec d'autres systèmes d'IA. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs qui sont des autorités répressives.

3. Le système de surveillance après commercialisation repose sur un plan de surveillance après commercialisation. Le plan de surveillance après commercialisation fait partie de la documentation technique visée à l'annexe IV. La Commission adopte un acte d'exécution fixant des dispositions détaillées établissant un modèle pour le plan de surveillance après commercialisation et la liste des éléments à inclure dans le plan au plus tard le 2 février 2026. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

4. Pour les systèmes d'IA à haut risque relevant de la législation d'harmonisation de l'Union énumérés à la section A de l'annexe I, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de ces actes, afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les éléments nécessaires décrits aux paragraphes 1, 2 et 3 en utilisant le modèle visé au paragraphe 3 dans les systèmes et plans existants au titre desdits actes, pour autant que cela donne lieu à un niveau de protection équivalent.

Le premier alinéa du présent paragraphe s'applique également aux systèmes d'IA à haut risque visés à l'annexe III, point 5, mis sur le marché ou mis en service par des établissements financiers qui sont soumis à des exigences en vertu de la législation de l'Union sur les services financiers concernant leur gouvernance, leurs dispositifs ou leurs processus internes.

▼B

SECTION 2

Partage d'informations sur les incidents graves

Article 73

Signalement d'incidents graves

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union signalent tout incident grave aux autorités de surveillance du marché des États membres dans lesquels cet incident s'est produit.

2. Le signalement visé au paragraphe 1 est effectué immédiatement après que le fournisseur a établi un lien de causalité, ou la probabilité raisonnable qu'un tel lien existe, entre le système d'IA et l'incident grave et, en tout état de cause, au plus tard 15 jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

Le délai pour le signalement visé au premier alinéa tient compte de l'ampleur de l'incident grave.

3. Nonobstant le paragraphe 2 du présent article, en cas d'infraction de grande ampleur ou d'incident grave au sens de l'article 3, point 49), b), le signalement visé au paragraphe 1 du présent article est effectué immédiatement, et au plus tard deux jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de cet incident.

4. Nonobstant le paragraphe 2, en cas de décès d'une personne, le signalement est effectué immédiatement après que le fournisseur ou le déployeur a établi un lien de causalité entre le système d'IA à haut risque et l'incident grave ou dès qu'il soupçonne un tel lien, mais au plus tard 10 jours après la date à laquelle le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

5. Si cela est nécessaire pour assurer un signalement en temps utile, le fournisseur ou, le cas échéant, le déployeur peut soumettre un signalement initial incomplet, suivi d'un signalement complet.

6. À la suite du signalement d'un incident grave en application du paragraphe 1, le fournisseur mène sans tarder les investigations nécessaires liées à l'incident grave et au système d'IA concerné. Ces investigations comprennent notamment une évaluation des risques résultant de l'incident, ainsi que des mesures correctives.

Le fournisseur coopère avec les autorités compétentes et, le cas échéant, avec l'organisme notifié concerné, au cours des investigations visées au premier alinéa, et ne mène aucune investigation nécessitant de modifier le système d'IA concerné d'une manière susceptible d'avoir une incidence sur toute évaluation ultérieure des causes de l'incident, avant d'informer les autorités compétentes de telles mesures.

7. Dès réception d'une notification relative à un incident grave visé à l'article 3, point 49) c), l'autorité de surveillance du marché compétente informe les autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1. La Commission élabore des orientations spécifiques pour faciliter le respect des obligations énoncées au paragraphe 1 du présent article. Ces orientations sont publiées au plus tard le 2 août 2025, et font l'objet d'une évaluation régulière.

▼B

8. L'autorité de surveillance du marché prend les mesures qui s'imposent, conformément à l'article 19 du règlement (UE) 2019/1020, dans un délai de sept jours à compter de la date à laquelle elle a reçu la notification visée au paragraphe 1 du présent article, et suit les procédures de notification prévues par ledit règlement.

9. Pour les systèmes d'IA à haut risque visés à l'annexe III qui sont mis sur le marché ou mis en service par des fournisseurs qui sont soumis à des instruments législatifs de l'Union établissant des obligations de signalement équivalentes à celles énoncées dans le présent règlement, la notification des incidents graves est limitée à ceux visés à l'article 3, point 49) c).

10. Pour les systèmes d'IA à haut risque qui sont des composants de sécurité de dispositifs, ou qui sont eux-mêmes des dispositifs, relevant des règlements (UE) 2017/745 et (UE) 2017/746, la notification des incidents graves est limitée à ceux qui sont visés à l'article 3, point 49) c), du présent règlement, et est adressée à l'autorité nationale compétente choisie à cette fin par les États membres dans lesquels l'incident s'est produit.

11. Les autorités nationales compétentes notifient immédiatement à la Commission tout incident grave, qu'elles aient ou non pris des mesures à cet égard, conformément à l'article 20 du règlement (UE) 2019/1020.

SECTION 3

Contrôle de l'application

Article 74

Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union

1. Le règlement (UE) 2019/1020 s'applique aux systèmes d'IA relevant du présent règlement. Aux fins du contrôle effectif de l'application du présent règlement:

a) toute référence à un opérateur économique en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les opérateurs identifiés à l'article 2, paragraphe 1, du présent règlement;

b) toute référence à un produit en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les systèmes d'IA relevant du champ d'application du présent règlement.

2. Dans le cadre des obligations d'information qui leur incombent en vertu de l'article 34, paragraphe 4, du règlement (UE) 2019/1020, les autorités de surveillance du marché communiquent chaque année à la Commission et aux autorités nationales de la concurrence concernées toute information recueillie dans le cadre des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de l'Union relatif aux règles de concurrence. Elles font également rapport chaque année à la Commission sur les recours aux pratiques interdites intervenus au cours de l'année concernée et sur les mesures prises.

3. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité responsable des activités de surveillance du marché désignée en vertu de ces actes juridiques.

▼B

Par dérogation au premier alinéa, et dans des circonstances appropriées, les États membres peuvent désigner une autre autorité compétente pour faire office d'autorité de surveillance du marché, à condition d'assurer la coordination avec les autorités sectorielles de surveillance du marché compétentes chargées du contrôle de l'application des actes juridiques énumérés à l'annexe I.

4. Les procédures visées aux articles 79 à 83 du présent règlement ne s'appliquent pas aux systèmes d'IA liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure la section A de l'annexe I, lorsque ces actes juridiques prévoient déjà des procédures assurant un niveau de protection équivalent et ayant le même objectif. En pareils cas, ce sont les procédures sectorielles pertinentes qui s'appliquent.

5. Sans préjudice des pouvoirs conférés aux autorités de surveillance du marché par l'article 14 du règlement (UE) 2019/1020, afin d'assurer le contrôle effectif de l'application du présent règlement, les autorités de surveillance du marché peuvent exercer les pouvoirs visés à l'article 14, paragraphe 4, points d) et j), dudit règlement à distance, le cas échéant.

6. Pour les systèmes d'IA à haut risque mis sur le marché, mis en service ou utilisés par des établissements financiers régis par la législation de l'Union sur les services financiers, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité nationale responsable de la surveillance financière de ces établissements en vertu de cette législation dans la mesure où la mise sur le marché, la mise en service ou l'utilisation du système d'IA est directement liée à la fourniture de ces services financiers.

7. Par dérogation au paragraphe 6, dans des circonstances appropriées, et pour autant que la coordination soit assurée, l'État membre peut désigner une autre autorité compétente comme autorité de surveillance du marché aux fins du présent règlement.

Les autorités nationales de surveillance du marché surveillant les établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) n° 1024/2013, devraient communiquer sans tarder à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour les missions de surveillance prudentielle de la Banque centrale européenne définies dans ledit règlement.

8. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, du présent règlement, dans la mesure où ils sont utilisés à des fins répressives, de gestion des frontières et de justice et démocratie, et pour les systèmes d'IA à haut risque énumérés à l'annexe III, points 6, 7 et 8, du présent règlement, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités compétentes en matière de contrôle de la protection des données en vertu du règlement (UE) 2016/679 ou de la directive (UE) 2016/680, soit toute autre autorité désignée en application des mêmes conditions énoncées aux articles 41 à 44 de la directive (UE) 2016/680. Les activités de surveillance du marché ne portent en aucune manière atteinte à l'indépendance des autorités judiciaires ni n'interfèrent d'une autre manière avec leurs activités lorsque ces autorités agissent dans l'exercice de leurs fonctions judiciaires.

▼B

9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données est leur autorité de surveillance du marché, sauf en ce qui concerne la Cour de justice de l'Union européenne agissant dans l'exercice de ses fonctions judiciaires.

10. Les États membres facilitent la coordination entre les autorités de surveillance du marché désignées en vertu du présent règlement et les autres autorités ou organismes nationaux compétents pour surveiller l'application de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou dans d'autres législations de l'Union, qui sont susceptibles d'être pertinents pour les systèmes d'IA à haut risque visés à l'annexe III.

11. Les autorités de surveillance du marché et la Commission sont en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener soit par les autorités de surveillance du marché, soit par les autorités de surveillance du marché conjointement avec la Commission, qui ont pour objectif de promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser ou de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont identifiés comme présentant un risque grave dans deux États membres ou plus conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA fournit une aide à la coordination des enquêtes conjointes.

12. Sans préjudice des pouvoirs prévus par le règlement (UE) 2019/1020, et lorsque cela est pertinent et limité à ce qui est nécessaire à l'accomplissement de leurs tâches, les fournisseurs accordent aux autorités de surveillance du marché un accès complet à la documentation ainsi qu'aux jeux de données d'entraînement, de validation et de test utilisés pour le développement des systèmes d'IA à haut risque, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'interfaces de programmation d'application (API) ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

13. Les autorités de surveillance du marché se voient accorder l'accès au code source du système d'IA à haut risque sur demande motivée et uniquement lorsque les deux conditions suivantes sont réunies:

a) l'accès au code source est nécessaire pour évaluer la conformité d'un système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2; et

b) les procédures d'essai ou d'audit et les vérifications fondées sur les données et la documentation communiquées par le fournisseur ont été entièrement accomplies ou se sont révélées insuffisantes.

14. Toute information ou documentation obtenue par les autorités de surveillance du marché est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

Article 75

Assistance mutuelle, surveillance du marché et contrôle des systèmes d'IA à usage général

1. Lorsqu'un système d'IA repose sur un modèle d'IA à usage général, et que le modèle et le système sont mis au point par le même fournisseur, le Bureau de l'IA est habilité à contrôler et surveiller la conformité de ce système d'IA avec les obligations prévues par le

▼B

présent règlement. Pour s'acquitter de ses tâches de contrôle et de surveillance, le Bureau de l'IA dispose de tous les pouvoirs d'une autorité de surveillance du marché prévus dans la présente section et dans le règlement (UE) 2019/1020.

2. Lorsqu'elles ont des raisons suffisantes de considérer que des systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque en vertu du présent règlement ne sont pas conformes aux exigences énoncées dans le présent règlement, les autorités de surveillance du marché concernées coopèrent avec le Bureau de l'IA pour procéder à des évaluations de la conformité, et en informent le Comité IA et les autres autorités de surveillance du marché.

3. Lorsqu'une autorité de surveillance du marché n'est pas en mesure de conclure son enquête sur le système d'IA à haut risque en raison de son incapacité à accéder à certaines informations relatives au modèle d'IA à usage général bien qu'elle ait déployé tous les efforts appropriés pour obtenir ces informations, elle peut présenter une demande motivée au Bureau de l'IA, par laquelle l'accès à ces informations est mis en œuvre. Dans ce cas, le Bureau de l'IA fournit sans tarder à l'autorité requérante, et en tout état de cause dans un délai de 30 jours, toute information qu'il juge pertinente pour déterminer si un système d'IA à haut risque est non conforme. Les autorités de surveillance du marché garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78 du présent règlement. La procédure prévue au chapitre VI du règlement (UE) 2019/1020 s'applique mutatis mutandis.

Article 76

Supervision des essais en conditions réelles par les autorités de surveillance du marché

1. Les autorités de surveillance du marché ont les compétences et les pouvoirs nécessaires pour veiller à ce que les essais en conditions réelles soient conformes au présent règlement.

2. Lorsque des essais en conditions réelles sont effectués pour des systèmes d'IA supervisés dans un bac à sable réglementaire de l'IA en vertu de l'article 58, les autorités de surveillance du marché vérifient le respect de l'article 60 dans le cadre de leur rôle de surveillance du bac à sable réglementaire de l'IA. Ces autorités peuvent, lorsqu'il y a lieu, autoriser le fournisseur ou le fournisseur potentiel à effectuer les essais en conditions réelles, par dérogation aux conditions énoncées à l'article 60, paragraphe 4, points f) et g).

3. Lorsqu'une autorité de surveillance du marché a été informée d'un incident grave par le fournisseur potentiel, le fournisseur ou tout tiers, ou qu'elle a d'autres raisons de penser que les conditions énoncées aux articles 60 et 61 ne sont pas remplies, elle peut prendre l'une ou l'autre des décisions suivantes sur son territoire, selon le cas:

a) suspendre ou faire cesser les essais en conditions réelles;

b) exiger du fournisseur ou du fournisseur potentiel et du déployeur ou futur déployeur qu'ils modifient tout aspect des essais en conditions réelles.

▼B

4. Lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3 du présent article, ou a formulé une objection au sens de l'article 60, paragraphe 4, point b), la décision ou l'objection est motivée et indique les modalités selon lesquelles le fournisseur ou le fournisseur potentiel peut contester la décision ou l'objection.

5. Le cas échéant, lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3, elle en communique les motifs aux autorités de surveillance du marché des autres États membres dans lesquels le système d'IA a été testé conformément au plan d'essais.

Article 77

Pouvoirs des autorités de protection des droits fondamentaux

1. Les autorités ou organismes publics nationaux qui supervisent ou font respecter les obligations au titre du droit de l'Union visant à protéger les droits fondamentaux, y compris le droit à la non-discrimination, en ce qui concerne l'utilisation des systèmes d'IA à haut risque visés à l'annexe III sont habilités à demander toute documentation créée ou conservée en vertu du présent règlement et à y avoir accès dans une langue et un format accessibles lorsque l'accès à cette documentation est nécessaire à l'accomplissement effectif de leur mandat dans les limites de leurs compétences. L'autorité ou l'organisme public concerné informe l'autorité de surveillance du marché de l'État membre concerné de toute demande de ce type.

2. Au plus tard le 2 novembre 2024, chaque État membre identifie les autorités ou organismes publics visés au paragraphe 1 et met la liste de ces autorités ou organismes à la disposition du public. Les États membres notifient la liste à la Commission et aux autres États membres, et tiennent cette liste à jour.

3. Lorsque la documentation visée au paragraphe 1 ne suffit pas pour déterminer s'il y a eu violation des obligations au titre du droit de l'Union protégeant les droits fondamentaux, l'autorité ou l'organisme public visé au paragraphe 1 peut présenter à l'autorité de surveillance du marché une demande motivée visant à organiser des tests du système d'IA à haut risque par des moyens techniques. L'autorité de surveillance du marché organise les tests avec la participation étroite de l'autorité ou organisme public ayant présenté la demande dans un délai raisonnable après celle-ci.

4. Toute information ou documentation obtenue par les autorités ou organismes publics nationaux visés au paragraphe 1 du présent article en application des dispositions du présent article est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

Article 78

Confidentialité

1. La Commission, les autorités de surveillance du marché et les organismes notifiés, ainsi que toute autre personne physique ou morale associée à l'application du présent règlement respectent, conformément au droit de l'Union ou au droit national, la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier:

▼B

a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil ([1]);

b) la mise en œuvre effective du présent règlement, notamment en ce qui concerne les inspections, les investigations ou les audits;

c) les intérêts en matière de sécurité nationale et publique;

d) la conduite des procédures pénales ou administratives;

e) les informations classifiées en vertu du droit de l'Union ou du droit national.

2. Les autorités associées à l'application du présent règlement conformément au paragraphe 1 demandent uniquement les données qui sont strictement nécessaires à l'évaluation du risque posé par les systèmes d'IA et à l'exercice de leurs pouvoirs conformément au présent règlement et au règlement (UE) 2019/1020. Elles mettent en place des mesures de cybersécurité adéquates et efficaces pour protéger la sécurité et la confidentialité des informations et des données obtenues, et suppriment les données collectées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été obtenues, conformément au droit de l'Union ou au droit national applicable.

3. Sans préjudice des paragraphes 1 et 2, les informations échangées à titre confidentiel entre les autorités nationales compétentes ou entre celles-ci et la Commission ne sont pas divulguées sans consultation préalable de l'autorité nationale compétente dont elles émanent et du déployeur lorsque les systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, sont utilisés par les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile et lorsque cette divulgation risquerait de porter atteinte aux intérêts en matière de sécurité nationale et publique. Cet échange d'informations ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

Lorsque les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile sont fournisseurs de systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, la documentation technique visée à l'annexe IV reste dans les locaux de ces autorités. Ces autorités veillent à ce que les autorités de surveillance du marché visées à l'article 74, paragraphes 8 et 9, selon le cas, puissent, sur demande, avoir immédiatement accès à la documentation ou en obtenir une copie. Seuls les membres du personnel de l'autorité de surveillance du marché disposant d'une habilitation de sécurité au niveau approprié sont autorisés à avoir accès à cette documentation ou à une copie de celle-ci.

4. Les paragraphes 1, 2 et 3 sont sans effet sur les droits ou obligations de la Commission, des États membres et de leurs autorités compétentes, ainsi que sur les droits ou obligations des organismes notifiés, en matière d'échange d'informations et de diffusion de mises en garde, y compris dans le contexte de la coopération transfrontière, et sur les obligations d'information incombant aux parties concernées en vertu du droit pénal des États membres.

([1]) Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

▼B

5. La Commission et les États membres peuvent, lorsque cela est nécessaire et conformément aux dispositions pertinentes des accords internationaux et commerciaux, échanger des informations confidentielles avec les autorités de réglementation de pays tiers avec lesquels ils ont conclu des accords bilatéraux ou multilatéraux en matière de confidentialité garantissant un niveau de confidentialité approprié.

Article 79

Procédure applicable au niveau national aux systèmes d'IA présentant un risque

1. On entend par systèmes d'IA présentant un risque, un «produit présentant un risque» au sens de l'article 3, point 19), du règlement (UE) 2019/1020, dans la mesure où ils présentent des risques pour la santé ou la sécurité, ou pour les droits fondamentaux, des personnes.

2. Lorsque l'autorité de surveillance du marché d'un État membre a des raisons suffisantes de considérer qu'un système d'IA présente un risque au sens du paragraphe 1 du présent article, elle procède à une évaluation de la conformité du système d'IA concerné avec l'ensemble des exigences et obligations énoncées dans le présent règlement. Une attention particulière est accordée aux systèmes d'IA présentant un risque pour les groupes vulnérables. Lorsque sont identifiés des risques pour les droits fondamentaux, l'autorité de surveillance du marché informe également les autorités ou organismes publics nationaux concernés visés à l'article 77, paragraphe 1, et coopère pleinement avec eux. Les opérateurs concernés coopèrent, en tant que de besoin, avec l'autorité de surveillance du marché et avec les autres autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1.

Si, au cours de cette évaluation, l'autorité de surveillance du marché ou, le cas échéant, l'autorité de surveillance du marché en coopération avec l'autorité publique nationale visée à l'article 77, paragraphe 1, constate que le système d'IA ne respecte pas les exigences et obligations énoncées dans le présent règlement, elle invite sans retard injustifié l'opérateur concerné à prendre toutes les mesures correctives appropriées pour mettre le système d'IA en conformité, le retirer du marché ou le rappeler dans un délai qu'elle peut prescrire, et en tout état de cause au plus tard dans les 15 jours ouvrables, ou dans un délai prévu par la législation d'harmonisation de l'Union concernée, le délai le plus court étant retenu.

L'autorité de surveillance du marché informe l'organisme notifié concerné en conséquence. L'article 18 du règlement (UE) 2019/1020 s'applique aux mesures visées au deuxième alinéa du présent paragraphe.

3. Lorsque l'autorité de surveillance du marché considère que la non-conformité n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées de l'opérateur.

4. L'opérateur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.

▼B

5. Lorsque l'opérateur d'un système d'IA ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2, l'autorité de surveillance du marché prend toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du système d'IA sur son marché national ou sa mise en service, pour retirer le produit ou le système d'IA autonome de ce marché ou pour le rappeler. L'autorité notifie ces mesures sans retard injustifié à la Commission et aux autres États membres.

6. La notification visée au paragraphe 5 contient toutes les précisions disponibles, notamment les informations nécessaires pour identifier le système d'IA non conforme, son origine et la chaîne d'approvisionnement, la nature de la non-conformité alléguée et du risque encouru, ainsi que la nature et la durée des mesures nationales prises et les arguments avancés par l'opérateur concerné. En particulier, l'autorité de surveillance du marché indique si la non-conformité découle d'une ou plusieurs des causes suivantes:

a) le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5;

b) le non-respect, par le système d'IA à haut risque, des exigences énoncées au chapitre III, section 2;

c) des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 qui confèrent une présomption de conformité;

d) le non-respect de l'article 50.

7. Les autorités de surveillance du marché autres que l'autorité de surveillance du marché de l'État membre qui a entamé la procédure informent sans retard injustifié la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent à propos de la non-conformité du système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans les trois mois suivant la réception de la notification visée au paragraphe 5, aucune objection n'a été émise par une autorité de surveillance du marché d'un État membre ou par la Commission à l'encontre d'une mesure provisoire prise par une autorité de surveillance du marché d'un autre État membre, cette mesure est réputée justifiée. Cette disposition est sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020. Le délai de trois mois visé au présent paragraphe est ramené à 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 du présent règlement.

9. Les autorités de surveillance du marché veillent à ce que les mesures restrictives appropriées soient prises sans retard injustifié à l'égard du produit ou du système d'IA concerné, par exemple son retrait de leur marché.

▼B

Article 80

Procédure applicable aux systèmes d'IA classés par le fournisseur comme n'étant pas à haut risque en application de l'annexe III

1. Lorsqu'une autorité de surveillance du marché a des raisons suffisantes de considérer qu'un système d'IA classé par le fournisseur comme n'étant pas à haut risque en application de l'article 6, paragraphe 3, est en réalité à haut risque, elle procède à une évaluation du système d'IA concerné quant à la question de sa classification en tant que système d'IA à haut risque sur la base des conditions énoncées à l'article 6, paragraphe 3, et dans les lignes directrices de la Commission.

2. Lorsque, au cours de cette évaluation, l'autorité de surveillance du marché constate que le système d'IA concerné est à haut risque, elle demande sans retard injustifié au fournisseur concerné de prendre toutes les mesures nécessaires pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement, ainsi que de prendre les mesures correctives appropriées dans un délai que l'autorité de surveillance du marché peut prescrire.

3. Lorsque l'autorité de surveillance du marché considère que l'utilisation du système d'IA concerné n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées du fournisseur.

4. Le fournisseur veille à ce que toutes les mesures nécessaires soient prises pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement. Lorsque le fournisseur d'un système d'IA concerné ne met pas le système d'IA en conformité avec ces exigences et obligations dans le délai visé au paragraphe 2 du présent article, il fait l'objet d'amendes conformément à l'article 99.

5. Le fournisseur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.

6. Lorsque le fournisseur du système d'IA concerné ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2 du présent article, l'article 79, paragraphe 5 à 9, s'applique.

7. Lorsque, au cours de l'évaluation prévue au paragraphe 1 du présent article, l'autorité de surveillance du marché établit que le système d'IA a été classé à tort par le fournisseur comme n'étant pas à haut risque afin de contourner l'application des exigences figurant au chapitre III, section 2, le fournisseur fait l'objet d'amendes conformément à l'article 99.

8. Dans l'exercice de leur pouvoir de contrôle de l'application du présent article, et conformément à l'article 11 du règlement (UE) 2019/1020, les autorités de surveillance du marché peuvent effectuer des contrôles appropriés, en tenant compte notamment des informations stockées dans la base de données de l'UE visée à l'article 71 du présent règlement.

▼B

Article 81

Procédure de sauvegarde de l'Union

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 79, paragraphe 5, ou dans un délai de 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, l'autorité de surveillance du marché d'un État membre soulève des objections à l'encontre d'une mesure prise par une autre autorité de surveillance du marché, ou que la Commission estime que cette mesure est contraire au droit de l'Union, la Commission entame sans retard injustifié des consultations avec l'autorité de surveillance du marché de l'État membre concerné et le ou les opérateurs, et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission, dans un délai de six mois, ou de 60 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, à compter de la notification visée à l'article 79, paragraphe 5, décide si la mesure nationale est justifiée ou non et communique sa décision à l'autorité de surveillance du marché de l'État membre concerné. La Commission informe également toutes les autres autorités de surveillance du marché de sa décision.

2. Lorsque la Commission estime que la mesure prise par l'État membre concerné est justifiée, tous les États membres veillent à prendre des mesures restrictives appropriées à l'égard du système d'IA concerné, par exemple en exigeant le retrait du système d'IA de leur marché sans retard injustifié, et en informent la Commission. Lorsque la Commission estime que la mesure nationale n'est pas justifiée, l'État membre concerné retire la mesure et en informe la Commission.

3. Lorsque la mesure nationale est jugée justifiée et que la non-conformité du système d'IA est attribuée à des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 du présent règlement, la Commission applique la procédure prévue à l'article 11 du règlement (UE) n° 1025/2012.

Article 82

Systèmes d'IA conformes qui présentent un risque

1. Lorsque, ayant réalisé une évaluation au titre de l'article 79, après avoir consulté l'autorité publique nationale concernée visée à l'article 77, paragraphe 1, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un système d'IA à haut risque soit conforme au présent règlement, il comporte néanmoins un risque pour la santé ou la sécurité des personnes, pour les droits fondamentaux, ou pour d'autres aspects relatifs à la protection de l'intérêt public, elle demande à l'opérateur concerné de prendre toutes les mesures appropriées pour faire en sorte que le système d'IA concerné, une fois mis sur le marché ou mis en service, ne présente plus ce risque, et ce sans retard injustifié, dans un délai qu'elle peut prescrire.

2. Le fournisseur ou autre opérateur concerné s'assure que des mesures correctives sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union dans le délai prescrit par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

▼B

3. Les États membres informent immédiatement la Commission et les autres États membres d'une constatation au titre du paragraphe 1. Les informations fournies incluent toutes les précisions disponibles, notamment les données nécessaires à l'identification du système d'IA concerné, l'origine et la chaîne d'approvisionnement de ce système d'IA, la nature du risque encouru, ainsi que la nature et la durée des mesures nationales prises.

4. La Commission entame sans retard injustifié des consultations avec les États membres concernés et les opérateurs concernés, et évalue les mesures nationales prises. En fonction des résultats de cette évaluation, la Commission décide si la mesure est justifiée ou non et, si nécessaire, propose d'autres mesures appropriées.

5. La Commission communique immédiatement sa décision aux États membres concernés ainsi qu'aux opérateurs concernés. Elle en informe également les autres États membres.

Article 83

Non-conformité formelle

1. Lorsque l'autorité de surveillance du marché d'un État membre fait l'une des constatations ci-après, elle invite le fournisseur concerné à mettre un terme à la non-conformité en question, dans un délai qu'elle peut prescrire:

a) le marquage CE a été apposé en violation de l'article 48;

b) le marquage CE n'a pas été apposé;

c) la déclaration UE de conformité visée à l'article 47 n'a pas été établie;

d) la déclaration UE de conformité visée à l'article 47 n'a pas été établie correctement;

e) l'enregistrement dans la base de données de l'UE visée à l'article 71 n'a pas été effectué;

f) le cas échéant, il n'a pas été désigné de mandataire;

g) la documentation technique n'est pas disponible.

2. Si le cas de non-conformité visé au paragraphe 1 persiste, l'autorité de surveillance du marché de l'État membre concerné prend toutes les mesures appropriées et proportionnées pour restreindre ou interdire la mise à disposition du système d'IA à haut risque sur le marché ou pour assurer son rappel ou son retrait sans tarder du marché.

Article 84

Structures de soutien de l'Union pour les essais en matière d'IA

1. La Commission désigne une ou plusieurs structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 21, paragraphe 6, du règlement (UE) 2019/1020 dans le domaine de l'intelligence artificielle.

▼B

2. Sans préjudice des tâches visées au paragraphe 1, les structures de soutien de l'Union pour les essais en matière d'IA fournissent également des avis techniques ou scientifiques indépendants à la demande du Comité IA, de la Commission ou des autorités de surveillance du marché.

SECTION 4

Voies de recours

Article 85

Droit d'introduire une réclamation auprès d'une autorité de surveillance du marché

Sans préjudice d'autres recours administratifs ou judiciaires, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement peut déposer des réclamations auprès de l'autorité de surveillance du marché concernée.

Conformément au règlement (UE) 2019/1020, ces réclamations sont prises en compte aux fins de l'exercice des activités de surveillance du marché, et sont traitées conformément aux procédures spécifiques établies en conséquence par les autorités de surveillance du marché.

Article 86

Droit à l'explication des décisions individuelles

1. Toute personne concernée faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un système d'IA à haut risque mentionné à l'annexe III, à l'exception des systèmes énumérés au point 2 de ladite annexe, et qui produit des effets juridiques ou affecte significativement cette personne de façon similaire d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux a le droit d'obtenir du déployeur des explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise.

2. Le paragraphe 1 ne s'applique pas à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions à l'obligation prévue audit paragraphe découlent du droit de l'Union ou du droit national dans le respect du droit de l'Union.

3. Le présent article ne s'applique que dans la mesure où le droit visé au paragraphe 1 n'est pas prévu par ailleurs dans le droit de l'Union.

Article 87

Signalement de violations et protection des auteurs de signalement

La directive (UE) 2019/1937 s'applique aux signalements de violations du présent règlement et à la protection des personnes signalant ces violations.

▼B

SECTION 5

Surveillance, enquêtes, contrôle de l'application et contrôle en ce qui concerne les fournisseurs de modèles d'IA à usage général

Article 88

Contrôle de l'exécution des obligations incombant aux fournisseurs de modèles d'IA à usage général

1. La Commission dispose de pouvoirs exclusifs pour surveiller et contrôler le respect du chapitre V, en tenant compte des garanties procédurales prévues à l'article 94. La Commission confie l'exécution de ces tâches au Bureau de l'IA, sans préjudice des pouvoirs d'organisation dont elle dispose ainsi que de la répartition des compétences entre les États membres et l'Union fondée sur les traités.

2. Sans préjudice de l'article 75, paragraphe 3, les autorités de surveillance du marché peuvent demander à la Commission d'exercer les pouvoirs prévus dans la présente section, lorsque cela est nécessaire et proportionné pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.

Article 89

Mesures de contrôle

1. Aux fins de l'exécution des tâches qui lui sont conférées dans le cadre de la présente section, le Bureau de l'IA peut prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs du présent règlement par les fournisseurs de modèles d'IA à usage général, y compris leur adhésion à des codes de bonne pratique approuvés.

2. Les fournisseurs en aval ont le droit d'introduire une réclamation pour violation du présent règlement. La réclamation est dûment motivée et indique au moins:

a) le point de contact du fournisseur du modèle d'IA à usage général concerné;

b) une description des faits pertinents, les dispositions concernées du présent règlement et la raison pour laquelle le fournisseur en aval considère que le fournisseur du modèle d'IA à usage général concerné a enfreint le présent règlement;

c) toute autre information que le fournisseur en aval qui a envoyé la demande juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

Article 90

Alertes de risques systémiques données par le groupe scientifique

1. Le groupe scientifique peut adresser une alerte qualifiée au Bureau de l'IA lorsqu'il a des raisons de soupçonner:

a) qu'un modèle d'IA à usage général présente un risque concret identifiable au niveau de l'Union; ou

▼B

b) qu'un modèle d'IA à usage général satisfait aux conditions visées à l'article 51.

2. À la suite d'une telle alerte qualifiée, la Commission, par l'intermédiaire du Bureau de l'IA et après en avoir informé le Comité IA, peut exercer les pouvoirs prévus à la présente section aux fins de l'évaluation de la question. Le Bureau de l'IA informe le Comité IA de toute mesure prise conformément aux articles 91 à 94.

3. L'alerte qualifiée est dûment motivée et indique au moins:

a) le point de contact du fournisseur du modèle d'IA à usage général concerné présentant un risque systémique;

b) une description des faits pertinents et les motifs de l'alerte donnée par le groupe scientifique;

c) toute autre information que le groupe scientifique juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

Article 91

Pouvoir de demander de la documentation et des informations

1. La Commission peut demander au fournisseur du modèle d'IA à usage général concerné de fournir la documentation établie par le fournisseur conformément aux articles 53 et 55, ou toute information supplémentaire nécessaire pour évaluer la conformité du fournisseur avec le présent règlement.

2. Avant d'envoyer la demande d'informations, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.

3. Sur demande dûment motivée du groupe scientifique, la Commission peut adresser une demande d'informations au fournisseur d'un modèle d'IA à usage général, lorsque l'accès à ces informations est nécessaire et proportionné pour l'accomplissement des tâches du groupe scientifique au titre de l'article 68, paragraphe 2.

4. La demande d'informations mentionne la base juridique et l'objet de la demande, précise quelles informations sont requises, fixe un délai dans lequel les informations doivent être fournies, et indique les amendes prévues à l'article 101 en cas de fourniture d'informations inexactes, incomplètes ou trompeuses.

5. Le fournisseur du modèle d'IA à usage général concerné, ou son représentant, fournit les informations demandées. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas de personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts fournissent les informations demandées pour le compte du fournisseur du modèle d'IA à usage général concerné. Les avocats dûment habilités à agir peuvent fournir des informations pour le compte de leurs clients. Les clients demeurent néanmoins pleinement responsables si les informations fournies sont incomplètes, inexactes ou trompeuses.

▼B

Article 92

Pouvoir de procéder à des évaluations

1. Le Bureau de l'IA, après consultation du Comité IA, peut procéder à des évaluations du modèle d'IA à usage général concerné:

a) pour évaluer le respect, par le fournisseur, des obligations prévues par le présent règlement, lorsque les informations recueillies en vertu de l'article 91 sont insuffisantes; ou

b) pour enquêter sur les risques systémiques, au niveau de l'Union, des modèles d'IA à usage général présentant un risque systémique, en particulier à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a).

2. La Commission peut décider de désigner des experts indépendants chargés de procéder à des évaluations pour son compte, y compris des experts du groupe scientifique établi en vertu de l'article 68. Les experts indépendants désignés pour cette tâche satisfont aux critères énoncés à l'article 68, paragraphe 2.

3. Aux fins du paragraphe 1, la Commission peut demander l'accès au modèle d'IA à usage général concerné par l'intermédiaire d'API ou d'autres moyens et outils techniques appropriés, y compris le code source.

4. La demande d'accès indique la base juridique, l'objet et les motifs de la demande et fixe le délai dans lequel l'accès doit être accordé, ainsi que les amendes prévues à l'article 101 en cas de non-fourniture de l'accès.

5. Les fournisseurs du modèle d'IA à usage général concerné ou son représentant fournissent les informations requises. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas la personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts, accordent l'accès demandé pour le compte du fournisseur du modèle d'IA à usage général concerné.

6. La Commission adopte des actes d'exécution établissant les modalités détaillées et les conditions des évaluations, y compris les modalités détaillées d'intervention d'experts indépendants, et la procédure relative à leur sélection. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

7. Avant de demander l'accès au modèle d'IA à usage général concerné, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général afin de recueillir davantage d'informations sur les essais internes du modèle, les garanties internes visant à prévenir les risques systémiques, ainsi que d'autres procédures internes et les mesures que le fournisseur a prises pour atténuer ces risques.

Article 93

Pouvoir de demander des mesures

1. Lorsque cela est nécessaire et approprié, la Commission peut demander aux fournisseurs:

▼B

a) de prendre les mesures appropriées pour se conformer aux obligations énoncées à aux articles 53 et 54;

b) de mettre en œuvre des mesures d'atténuation, lorsque l'évaluation effectuée conformément à l'article 92 a suscité des préoccupations sérieuses et fondées quant à un risque systémique au niveau de l'Union;

c) de restreindre la mise à disposition du modèle sur le marché, de le retirer ou de le rappeler.

2. Avant qu'une mesure ne soit demandée, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.

3. Si, au cours du dialogue structuré visé au paragraphe 2, le fournisseur du modèle d'IA à usage général présentant un risque systémique s'engage à mettre en œuvre des mesures d'atténuation pour faire face à un risque systémique au niveau de l'Union, la Commission peut, par une décision, rendre ces engagements contraignants et déclarer qu'il n'y a plus lieu d'agir.

Article 94

Droits procéduraux des opérateurs économiques du modèle d'IA à usage général

L'article 18 du règlement (UE) 2019/1020 s'applique mutatis mutandis aux fournisseurs du modèle d'IA à usage général, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

CHAPITRE X

CODES DE CONDUITE ET LIGNES DIRECTRICES

Article 95

Codes de conduite pour l'application volontaire de certaines exigences

1. Le Bureau de l'IA et les États membres encouragent et facilitent l'élaboration de codes de conduite, comportant des mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire, aux systèmes d'IA autres que les systèmes d'IA à haut risque, de tout ou partie des exigences énoncées au chapitre III, section 2, en tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur permettant l'application de ces exigences.

2. Le Bureau de l'IA et les États membres facilitent l'élaboration de codes de conduite concernant l'application volontaire, y compris par les déployeurs, d'exigences spécifiques à tous les systèmes d'IA, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que, entre autres:

a) les éléments applicables prévus dans les lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance;

▼B

b) l'évaluation et la réduction au minimum de l'incidence des systèmes d'IA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficaces de l'IA;

c) la promotion de la maîtrise de l'IA, en particulier chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA;

d) la facilitation d'une conception inclusive et diversifiée des systèmes d'IA, notamment par la mise en place d'équipes de développement inclusives et diversifiées et la promotion de la participation des parties prenantes à ce processus;

e) l'évaluation et la prévention de l'impact négatif des systèmes d'IA sur les personnes ou groupes de personnes vulnérables, y compris en ce qui concerne l'accessibilité pour les personnes handicapées, ainsi que sur l'égalité de genre.

3. Les codes de conduite peuvent être élaborés par des fournisseurs ou déployeurs individuels de systèmes d'IA ou par des organisations les représentant ou par les deux, y compris avec la participation de toute partie intéressée et de leurs organisations représentatives, y compris des organisations de la société civile et le monde universitaire. Les codes de conduite peuvent porter sur un ou plusieurs systèmes d'IA, compte tenu de la similarité de la destination des systèmes concernés.

4. Le Bureau de l'IA et les États membres prennent en considération les intérêts et les besoins spécifiques des PME, y compris les jeunes pousses, lorsqu'ils encouragent et facilitent l'élaboration de codes de conduite.

Article 96

Lignes directrices de la Commission sur la mise en œuvre du présent règlement

1. La Commission élabore des lignes directrices sur la mise en œuvre pratique du présent règlement, et en particulier sur:

a) l'application des exigences et obligations visées aux articles 8 à 15 et à l'article 25;

b) les pratiques interdites visées à l'article 5;

c) la mise en œuvre pratique des dispositions relatives aux modifications substantielles;

d) la mise en œuvre pratique des obligations de transparence prévues à l'article 50;

e) des informations détaillées sur la relation entre le présent règlement et la législation d'harmonisation de l'Union dont la liste figure à l'annexe I ainsi que d'autres actes législatifs pertinents de l'Union, y compris en ce qui concerne la cohérence de leur application;

f) l'application de la définition d'un système d'IA telle qu'elle figure à l'article 3, point 1).

▼B

Lorsqu'elle publie ces lignes directrices, la Commission accorde une attention particulière aux besoins des PME, y compris les jeunes pousses, des pouvoirs publics locaux et des secteurs les plus susceptibles d'être affectés par le présent règlement.

Les lignes directrices visées au premier alinéa du présent paragraphe tiennent dûment compte de l'état de la technique généralement reconnu en matière d'IA, ainsi que des normes harmonisées et spécifications communes pertinentes visées aux articles 40 et 41, ou des normes harmonisées ou spécifications techniques qui sont énoncées en vertu de la législation d'harmonisation de l'Union.

2. À la demande des États membres ou du Bureau de l'IA, ou de sa propre initiative, la Commission met à jour les lignes directrices précédemment adoptées lorsque cela est jugé nécessaire.

CHAPITRE XI

DÉLÉGATION DE POUVOIR ET PROCÉDURE DE COMITÉ

Article 97

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, est conféré à la Commission pour une durée de cinq ans à partir du 1er août 2024. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 «Mieux légiférer».

5. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie au Parlement européen et au Conseil simultanément.

▼B

6. Un acte délégué adopté en vertu de l'article 6, paragraphe 6 ou 7, de l'article 7, paragraphe 1 ou 3, de l'article 11, paragraphe 3, de l'article 43, paragraphe 5 ou 6, de l'article 47, paragraphe 5, de l'article 51, paragraphe 3, de l'article 52, paragraphe 4, ou de l'article 53, paragraphe 5 ou 6, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 98

Comité

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) nº 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) nº 182/2011 s'applique.

CHAPITRE XII

SANCTIONS

Article 99

Sanctions

1. Conformément aux conditions établies dans le présent règlement, les États membres déterminent le régime des sanctions et autres mesures d'exécution, qui peuvent également comprendre des avertissements et des mesures non monétaires, applicables aux violations du présent règlement commises par des opérateurs, et prennent toute mesure nécessaire pour veiller à la mise en œuvre correcte et effective de ces sanctions, tenant ainsi compte des lignes directrices publiées par la Commission en vertu de l'article 96. Ces sanctions doivent être effectives, proportionnées et dissuasives. Elles tiennent compte des intérêts des PME, y compris les jeunes pousses, et de leur viabilité économique.

2. Les États membres informent la Commission, sans retard et au plus tard à la date d'entrée en application, du régime des sanctions et des autres mesures d'exécution visées au paragraphe 1, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'amendes administratives pouvant aller jusqu'à 35 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 7 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

4. La non-conformité avec l'une quelconque des dispositions suivantes relatives aux opérateurs ou aux organismes notifiés, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 3 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu:

▼B

a) les obligations incombant aux fournisseurs en vertu de l'article 16;

b) les obligations incombant aux mandataires en vertu de l'article 22;

c) les obligations incombant aux importateurs en vertu de l'article 23;

d) les obligations incombant aux distributeurs en vertu de l'article 24;

e) les obligations incombant aux déployeurs en vertu de l'article 26;

f) les exigences et obligations applicables aux organismes notifiés en application de l'article 31, de l'article 33, paragraphes 1, 3 et 4, ou de l'article 34;

g) les obligations de transparence pour les fournisseurs et les déployeurs conformément à l'article 50.

5. La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales compétentes en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 7 500 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 1 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

6. Dans le cas des PME, y compris les jeunes pousses, chaque amende visée au présent article s'élève au maximum aux pourcentages ou montants visés aux paragraphes 3, 4 et 5, le chiffre le plus faible étant retenu.

7. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et, le cas échéant, il est tenu compte des éléments suivants:

a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné, ainsi que, le cas échéant, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;

b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour la même violation;

c) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités au même opérateur pour des violations d'autres dispositions du droit de l'Union ou du droit national, lorsque ces violations résultent de la même activité ou omission constituant une violation pertinente au sens du présent règlement;

d) la taille, le chiffre d'affaires annuel et la part de marché de l'opérateur qui commet la violation;

e) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation;

f) le degré de coopération établi avec les autorités nationales compétentes en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

g) le degré de responsabilité de l'opérateur, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;

▼B

h) la manière dont les autorités nationales compétentes ont eu connaissance de la violation, notamment si, et dans quelle mesure, l'opérateur a notifié la violation;

i) le fait que la violation a été commise délibérément ou par négligence;

j) toute mesure prise par l'opérateur pour atténuer le préjudice subi par les personnes concernées.

8. Chaque État membre établit les règles déterminant dans quelle mesure des amendes administratives peuvent être imposées à des autorités et organismes publics établis sur son territoire.

9. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que les amendes sont imposées par les juridictions nationales compétentes ou par d'autres organismes, selon le cas prévu dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

10. L'exercice des pouvoirs conférés par le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit national, y compris des recours juridictionnels effectifs et une procédure régulière.

11. Les États membres font rapport chaque année à la Commission sur les amendes administratives qu'ils ont infligées au cours de l'année concernée, conformément au présent article, ainsi que sur toute action en justice ou procédure judiciaire connexe.

Article 100

Amendes administratives imposées aux institutions, organes et organismes de l'Union

1. Le Contrôleur européen de la protection des données peut imposer des amendes administratives aux institutions, organes et organismes de l'Union relevant du champ d'application du présent règlement. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et il est dûment tenu compte des éléments suivants:

a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné ainsi que, s'il y a lieu, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;

b) le degré de responsabilité de l'institution, organe ou organisme de l'Union, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;

c) toute mesure prise par l'institution, organe ou organisme de l'Union pour atténuer les dommages subis par les personnes touchées;

d) le niveau de coopération établi avec le Contrôleur européen de la protection des données en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs, y compris le respect de toute mesure précédemment ordonnée par le Contrôleur européen de la protection des données à l'encontre de l'institution, organe ou organisme de l'Union concerné pour le même objet;

▼B

e) toute violation similaire commise précédemment par l'institution, organe ou organisme de l'Union;

f) la manière dont le Contrôleur européen de la protection des données a eu connaissance de la violation, notamment si, et le cas échéant dans quelle mesure, l'institution, organe ou organisme de l'Union a notifié la violation;

g) le budget annuel de l'institution, organe ou organisme de l'Union.

2. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'une amende administrative pouvant aller jusqu'à 1 500 000 EUR.

3. La non-conformité du système d'IA avec les exigences ou obligations au titre du présent règlement, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 750 000 EUR.

4. Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution, organe ou organisme de l'Union faisant l'objet des procédures conduites par le Contrôleur européen de la protection des données la possibilité de faire connaître son point de vue sur l'éventuelle infraction. Le Contrôleur européen de la protection des données ne fonde ses décisions que sur les éléments et les circonstances au sujet desquels les parties concernées ont pu formuler des observations. Les éventuels plaignants sont étroitement associés à la procédure.

5. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.

6. Les fonds collectés en imposant des amendes en vertu du présent article contribuent au budget général de l'Union. Les amendes ne compromettent pas le bon fonctionnement de l'institution, organe ou organisme de l'Union faisant l'objet d'une amende.

7. Le Contrôleur européen de la protection des données informe chaque année la Commission des amendes administratives qu'il a infligées en vertu du présent article ainsi que de toute action en justice ou procédure judiciaire qu'il a engagée.

Article 101

Amendes applicables aux fournisseurs de modèles d'IA à usage général

1. La Commission peut infliger aux fournisseurs de modèles d'IA à usage général des amendes n'excédant pas 3 % de leur chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, ou 15 000 000 EUR, le montant le plus élevé étant retenu, lorsque la Commission constate que le fournisseur, de manière délibérée ou par négligence:

▼B

a) a enfreint les dispositions pertinentes du présent règlement;

b) n'a pas donné suite à une demande de document ou d'informations au titre de l'article 91, ou a fourni des informations inexactes, incomplètes ou trompeuses;

c) ne s'est pas conformé à une mesure demandée au titre de l'article 93;

d) n'a pas donné à la Commission accès au modèle d'IA à usage général ou au modèle d'IA à usage général présentant un risque systémique en vue de procéder à une évaluation conformément à l'article 92.

Pour fixer le montant de l'amende ou de l'astreinte, il y a lieu de prendre en considération la nature, la gravité et la durée de la violation, tout en tenant dûment compte des principes de proportionnalité et d'adéquation. La Commission tient également compte des engagements pris conformément à l'article 93, paragraphe 3, ou pris dans les codes de bonne pratique pertinents conformément à l'article 56.

2. Avant d'adopter la décision en vertu du paragraphe 1, la Commission communique ses constatations préliminaires au fournisseur du modèle d'IA à usage général, et lui donne la possibilité d'être entendu.

3. Les amendes infligées conformément au présent article sont effectives, proportionnées et dissuasives.

4. Les informations relatives aux amendes infligées en vertu du présent article sont en outre communiquées au Comité IA, le cas échéant.

5. La Cour de justice de l'Union européenne statue avec compétence de pleine juridiction sur les recours formés contre les décisions par lesquelles la Commission a fixé une amende au titre du présent article. Elle peut supprimer, réduire ou majorer l'amende infligée.

6. La Commission adopte des actes d'exécution contenant les modalités détaillées des procédures et des garanties procédurales en vue de l'adoption éventuelle de décisions en vertu du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

CHAPITRE XIII

DISPOSITIONS FINALES

Article 102

Modification du règlement (CE) n° 300/2008

À l'article 4, paragraphe 3, du règlement (CE) n° 300/2008, l'alinéa suivant est ajouté:

▼B

«Lors de l'adoption de mesures détaillées relatives aux spécifications techniques et aux procédures d'approbation et d'utilisation des équipements de sûreté en ce qui concerne les systèmes d'intelligence artificielle au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 103

Modification du règlement (UE) n° 167/2013

À l'article 17, paragraphe 5, du règlement (UE) n° 167/2013, l'alinéa suivant est ajouté:

«Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 104

Modification du règlement (UE) n° 168/2013

À l'article 22, paragraphe 5, du règlement (UE) n° 168/2013, l'alinéa suivant est ajouté:

«Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

▼B

Article 105

Modification de la directive 2014/90/UE

À l'article 8 de la directive 2014/90/UE, le paragraphe suivant est ajouté:

«5. Pour les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), lorsqu'elle exerce ses activités conformément au paragraphe 1 et qu'elle adopte des spécifications techniques et des normes d'essai conformément aux paragraphes 2 et 3, la Commission tient compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 106

Modification de la directive (UE) 2016/797

À l'article 5 de la directive (UE) 2016/797, le paragraphe suivant est ajouté:

«12. Lors de l'adoption d'actes délégués conformément au paragraphe 1 et d'actes d'exécution conformément au paragraphe 11 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 107

Modification du règlement (UE) 2018/858

À l'article 5 du règlement (UE) 2018/858, le paragraphe suivant est ajouté:

▼B

«4. Lors de l'adoption d'actes délégués conformément au paragraphe 3 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 108

Modifications du règlement (UE) 2018/1139

Le règlement (UE) 2018/1139 est modifié comme suit:

1) À l'article 17, le paragraphe suivant est ajouté:

«3. Sans préjudice du paragraphe 2, lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

2) À l'article 19, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

3) À l'article 43, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

▼B

4) À l'article 47, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

5) À l'article 57, le paragraphe suivant est ajouté:

«Lors de l'adoption de ces actes d'exécution en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

6) À l'article 58, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

Article 109

Modification du règlement (UE) 2019/2144

À l'article 11 du règlement (UE) 2019/2144, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes d'exécution conformément au paragraphe 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil (*), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

(*) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 110

Modification de la directive (UE) 2020/1828

À l'annexe I de la directive (UE) 2020/1828 du Parlement européen et du Conseil ([2]), le point suivant est ajouté:

([2]) Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

▼B

«68) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Article 111

Systèmes d'IA déjà mis sur le marché ou mis en service et modèles d'IA à usage général déjà mis sur le marché

1. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), les systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe X et mis sur le marché ou mis en service avant le 2 août 2027 sont mis en conformité avec le présent règlement au plus tard le 31 décembre 2030.

Il est tenu compte des exigences énoncées dans le présent règlement lors de l'évaluation de chaque système d'information à grande échelle établi par les actes juridiques énumérés à l'annexe X devant être effectuée conformément à ces actes juridiques et lorsque ces actes juridiques sont remplacés ou modifiés.

2. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), le présent règlement s'applique aux opérateurs de systèmes d'IA à haut risque, autres que les systèmes visés au paragraphe 1 du présent article, qui ont été mis sur le marché ou mis en service avant le 2 août 2026, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leurs conceptions. En tout état de cause, les fournisseurs et les déployeurs de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques prennent les mesures nécessaires pour se conformer aux exigences et obligations du présent règlement au plus tard le 2 août 2030.

3. Les fournisseurs de modèles d'IA à usage général qui ont été mis sur le marché avant le 2 août 2025 prennent les mesures nécessaires pour se conformer aux obligations prévues par le présent règlement au plus tard le 2 août 2027.

Article 112

Évaluation et réexamen

1. La Commission évalue la nécessité de modifier la liste figurant à l'annexe III et la liste des pratiques d'IA interdites figurant à l'article 5, une fois par an après l'entrée en vigueur du présent règlement et jusqu'à la fin de la période de délégation de pouvoir énoncée à l'article 97. La Commission transmet les conclusions de cette évaluation au Parlement européen et au Conseil.

▼B

2. Au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen et au Conseil sur les éléments suivants:

a) la nécessité de modifications pour étendre des rubriques de domaine existantes ou ajouter de nouvelles rubriques de domaine dans l'annexe III;

b) les modifications de la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires au titre de l'article 50;

c) les modifications visant à renforcer l'efficacité du système de surveillance et de gouvernance.

3. Au plus tard le 2 août 2029 et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Le rapport comprend une évaluation en ce qui concerne la structure de contrôle de l'application ainsi que l'éventuelle nécessité d'une agence de l'Union pour remédier aux lacunes identifiées. Sur la base des constatations, ce rapport est, le cas échéant, accompagné d'une proposition de modification du présent règlement. Les rapports sont publiés.

4. Les rapports visés au paragraphe 2 prêtent une attention particulière aux éléments suivants:

a) l'état des ressources financières, techniques et humaines dont les autorités nationales compétentes ont besoin pour mener efficacement à bien les missions qui leur sont dévolues par le présent règlement;

b) l'état des sanctions, notamment les amendes administratives visées à l'article 99, paragraphe 1, appliquées par les États membres en cas de violation du présent règlement;

c) les normes harmonisées adoptées et les spécifications communes élaborées à l'appui du présent règlement;

d) le nombre d'entreprises qui arrivent sur le marché après l'entrée en application du présent règlement, et combien d'entre elles sont des PME.

5. Au plus tard le 2 août 2028, la Commission évalue le fonctionnement du Bureau de l'IA, afin de déterminer si des pouvoirs et compétences suffisants lui ont été conférés pour s'acquitter de ses tâches, et s'il serait pertinent et nécessaire pour la bonne mise en œuvre et l'application correcte du présent règlement de renforcer le Bureau de l'IA et ses compétences d'exécution et d'accroître ses ressources. La Commission présente un rapport sur son évaluation au Parlement européen et au Conseil.

6. Au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission présente un rapport sur l'examen de l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, et évalue la nécessité de mesures ou d'actions supplémentaires, y compris de mesures ou d'actions contraignantes. Ce rapport est présenté au Parlement européen et au Conseil et il est rendu public.

▼B

7. Au plus tard le 2 août 2028 et tous les trois ans par la suite, la Commission évalue l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées au chapitre III, section 2, pour les systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à haut risque, y compris en ce qui concerne la durabilité environnementale.

8. Aux fins des paragraphes 1 à 7, le Comité IA, les États membres et les autorités nationales compétentes fournissent des informations à la Commission à la demande de cette dernière et sans retard injustifié.

9. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 à 7, la Commission tient compte des positions et des conclusions du Comité IA, du Parlement européen, du Conseil et d'autres organismes ou sources pertinents.

10. La Commission soumet, si nécessaire, des propositions appropriées visant à modifier le présent règlement, notamment en tenant compte de l'évolution des technologies, de l'effet des systèmes d'IA sur la santé et la sécurité, ainsi que sur les droits fondamentaux, et à la lumière de l'état d'avancement de la société de l'information.

11. Pour orienter les évaluations et les réexamens visés aux paragraphes 1 à 7 du présent article, le Bureau de l'IA entreprend de mettre au point une méthode objective et participative pour l'évaluation des niveaux de risque fondée sur les critères décrits dans les articles pertinents et l'inclusion de nouveaux systèmes dans:

a) la liste figurant à l'annexe III, y compris l'extension des rubriques de domaine existantes ou l'ajout de nouvelles rubriques de domaine dans ladite annexe;

b) la liste des pratiques interdites figurant à l'article 5; et

c) la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires en application de l'article 50.

12. Toute modification du présent règlement en vertu du paragraphe 10, ou tout acte délégué ou acte d'exécution pertinent, qui concerne la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, tient compte des spécificités réglementaires de chaque secteur, ainsi et des mécanismes de gouvernance, d'évaluation de la conformité et d'applications existants et des autorités qui y sont établies.

13. Au plus tard le 2 août 2031, la Commission procède à une évaluation de sa mise en application dont elle fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte des premières années d'application du présent règlement. Sur la base des conclusions, ce rapport est accompagné, le cas échéant, d'une proposition de modification du présent règlement en ce qui concerne la structure de contrôle de l'application ainsi que la nécessité d'une agence de l'Union pour remédier aux lacunes identifiées.

▼B

Article 113

Entrée en vigueur et application

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du 2 août 2026.

Toutefois:

a) les chapitres I et II sont applicables à partir du 2 février 2025;

b) le chapitre III, section 4, le chapitre V, le chapitre VII, le chapitre XII et l'article 78 s'appliquent à partir du 2 août 2025, à l'exception de l'article 101;

c) l'article 6, paragraphe 1, et les obligations correspondantes du présent règlement s'appliquent à partir du 2 août 2027.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

▼B

ANNEXE I

Liste de la législation d'harmonisation de l'Union

Section A. Liste de la législation d'harmonisation de l'Union fondée sur le nouveau cadre législatif

1. Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24);

2. Directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets (JO L 170 du 30.6.2009, p. 1);

3. Directive 2013/53/UE du Parlement européen et du Conseil du 20 novembre 2013 relative aux bateaux de plaisance et aux véhicules nautiques à moteur et abrogeant la directive 94/25/CE (JO L 354 du 28.12.2013, p. 90);

4. Directive 2014/33/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les ascenseurs et les composants de sécurité pour ascenseurs (JO L 96 du 29.3.2014, p. 251);

5. Directive 2014/34/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles (JO L 96 du 29.3.2014, p. 309);

6. Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62);

7. Directive 2014/68/UE du Parlement européen et du Conseil du 15 mai 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des équipements sous pression (JO L 189 du 27.6.2014, p. 164);

8. Règlement (UE) 2016/424 du Parlement européen et du Conseil du 9 mars 2016 relatif aux installations à câbles et abrogeant la directive 2000/9/CE (JO L 81 du 31.3.2016, p. 1);

9. Règlement (UE) 2016/425 du Parlement européen et du Conseil du 9 mars 2016 relatif aux équipements de protection individuelle et abrogeant la directive 89/686/CEE du Conseil (JO L 81 du 31.3.2016, p. 51);

10. Règlement (UE) 2016/426 du Parlement européen et du Conseil du 9 mars 2016 concernant les appareils brûlant des combustibles gazeux et abrogeant la directive 2009/142/CE (JO L 81 du 31.3.2016, p. 99);

11. Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1);

12. Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

Section B. Liste des autres législations d'harmonisation de l'Union

13. Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72);

▼B

14. Règlement (UE) n° 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52);

15. Règlement (UE) n° 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1);

16. Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146);

17. Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44);

18. Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1);

19. Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1);

20. Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil et le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1), dans la mesure où il concerne la conception, la production et la mise sur le marché des aéronefs visés à son article 2, paragraphe 1, points a) et b), lorsque cela concerne des aéronefs sans équipage à bord et leurs moteurs, hélices, pièces et équipements de contrôle à distance.

▼B

ANNEXE II

Liste des infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii)

Infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii):

— terrorisme,

— traite des êtres humains,

— exploitation sexuelle des enfants et pédopornographie,

— trafic de stupéfiants ou de substances psychotropes,

— trafic d'armes, de munitions ou d'explosifs,

— homicide volontaire, coups et blessures graves,

— trafic d'organes ou de tissus humains,

— trafic de matières nucléaires ou radioactives,

— enlèvement, séquestration ou prise d'otage,

— crimes relevant de la compétence de la Cour pénale internationale,

— détournement d'avion ou de navire,

— viol,

— criminalité environnementale,

— vol organisé ou à main armée,

— sabotage,

— participation à une organisation criminelle impliquée dans une ou plusieurs des infractions énumérées ci-dessus.

▼B

ANNEXE III

Systèmes d'IA à haut risque visés à l'article 6, paragraphe 2

Les systèmes d'IA à haut risque au sens de l'article 6, paragraphe 2, sont les systèmes d'IA répertoriés dans l'un des domaines suivants:

1. Biométrie, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

   a) systèmes d'identification biométrique à distance.

      Cela n'inclut pas les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique dont la seule finalité est de confirmer qu'une personne physique spécifique est la personne qu'elle prétend être;

   b) systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique, en fonction d'attributs ou de caractéristiques sensibles ou protégés, sur la base de la déduction de ces attributs ou de ces caractéristiques;

   c) systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions.

2. Infrastructures critiques: systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité.

3. Éducation et formation professionnelle:

   a) systèmes d'IA destinés à être utilisés pour déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement et de formation professionnelle, à tous les niveaux;

   b) systèmes d'IA destinés à être utilisés pour évaluer les acquis d'apprentissage, y compris lorsque ceux-ci sont utilisés pour orienter le processus d'apprentissage de personnes physiques dans les établissements d'enseignement et de formation professionnelle, à tous les niveaux;

   c) systèmes d'IA destinés à être utilisés pour évaluer le niveau d'enseignement approprié qu'une personne recevra ou sera en mesure d'atteindre, dans le contexte ou au sein d'établissements d'enseignement et de formation professionnelle à tous les niveaux;

   d) systèmes d'IA destinés à être utilisés pour surveiller et détecter des comportements interdits chez les étudiants lors d'examens dans le contexte d'établissements d'enseignement et de formation ou en leur sein à tous les niveaux;

4. Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant:

   a) systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, en particulier pour publier des offres d'emploi ciblées, analyser et filtrer les candidatures et évaluer les candidats;

   b) systèmes d'IA destinés à être utilisés pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations.

5. Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels:

▼B

a) systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soins de santé, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services;

b) systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières;

c) systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie;

d) systèmes d'IA destinés à évaluer et hiérarchiser les appels d'urgence émanant de personnes physiques ou à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par la police, les pompiers et l'assistance médicale, ainsi que pour les systèmes de tri des patients admis dans les services de santé d'urgence.

6. Répression, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

a) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives ou en leur nom pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales;

b) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives, en tant que polygraphes ou outils similaires;

c) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales;

d) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer le risque qu'une personne physique commette une infraction ou récidive, sans se fonder uniquement sur le profilage des personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes;

e) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre de la détection d'infractions pénales, d'enquêtes ou de poursuites en la matière ou de l'exécution de sanctions pénales.

7. Migration, asile et gestion des contrôles aux frontières, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

a) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, en tant que polygraphes et outils similaires;

▼B

b) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour évaluer un risque, y compris un risque pour la sécurité, un risque de migration irrégulière ou un risque pour la santé, posé par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre;

c) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour aider les autorités publiques compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, y compris les évaluations connexes de la fiabilité des éléments de preuve;

d) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques, à l'exception de la vérification des documents de voyage.

8. Administration de la justice et processus démocratiques:

a) systèmes d'IA destinés à être utilisés par les autorités judiciaires ou en leur nom, pour les aider à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits, ou à être utilisés de manière similaire lors du règlement extrajudiciaire d'un litige;

b) systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums. Sont exclus les systèmes d'IA aux sorties desquels les personnes physiques ne sont pas directement exposées, tels que les outils utilisés pour organiser, optimiser ou structurer les campagnes politiques sous l'angle administratif ou logistique.

▼B

ANNEXE IV

Documentation technique visée à l'article 11, paragraphe 1

La documentation technique visée à l'article 11, paragraphe 1, contient au moins les informations ci-après, selon le système d'IA concerné:

1. une description générale du système d'IA, y compris:

   a) la destination, le nom du fournisseur et la version du système, faisant apparaître sa relation aux versions précédentes;

   b) la manière dont le système d'IA interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels, y compris avec d'autres systèmes d'IA, qui ne font pas partie du système d'IA lui-même, le cas échéant;

   c) les versions des logiciels ou des micrologiciels pertinents et toute exigence relative aux mises à jour de la version;

   d) la description de toutes les formes sous lesquelles le système d'IA est mis sur le marché ou mis en service, telles que les packs logiciels intégrés dans du matériel informatique, les téléchargements ou les API;

   e) la description du matériel informatique sur lequel le système d'IA est destiné à être exécuté;

   f) lorsque le système d'IA est un composant de produits, des photographies ou des illustrations montrant les caractéristiques externes, le marquage et la disposition interne de ces produits;

   g) une description de base de l'interface utilisateur fournie au déployeur;

   h) une notice d'utilisation à l'intention du déployeur et une description de base de l'interface utilisateur fournie au déployeur, le cas échéant;

2. une description détaillée des éléments du système d'IA et de son processus de développement, y compris:

   a) les méthodes et étapes suivies pour le développement du système d'IA, y compris, le cas échéant, le recours à des systèmes ou outils pré-entraînés fournis par des tiers et la manière dont ceux-ci ont été utilisés, intégrés ou modifiés par le fournisseur;

   b) les spécifications de conception du système, à savoir la logique générale du système d'IA et des algorithmes; les principaux choix de conception, y compris le raisonnement et les hypothèses retenues, y compris en ce qui concerne les personnes ou les groupes de personnes à l'égard desquels le système est destiné à être utilisé; les principaux choix de classification; ce que le système est conçu pour optimiser, ainsi que la pertinence des différents paramètres; la description des sorties attendues du système et de leur qualité; les décisions relatives aux compromis éventuels en ce qui concerne les solutions techniques adoptées pour se conformer aux exigences énoncées au chapitre III, section 2;

   c) la description de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global; les ressources informatiques utilisées pour développer, entraîner, mettre à l'essai et valider le système d'IA;

▼B

d) le cas échéant, les exigences relatives aux données en ce qui concerne les fiches décrivant les méthodes et techniques d'entraînement et les jeux de données d'entraînement utilisés, y compris une description générale de ces jeux de données et des informations sur leur provenance, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées; les procédures d'étiquetage (par exemple pour l'apprentissage supervisé), les méthodes de nettoyage des données (par exemple la détection des valeurs aberrantes);

e) l'évaluation des mesures de contrôle humain nécessaires conformément à l'article 14, y compris une évaluation des mesures techniques nécessaires pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA, conformément à l'article 13, paragraphe 3, point d);

f) le cas échéant, une description détaillée des modifications prédéterminées du système d'IA et de ses performances, ainsi que toutes les informations pertinentes relatives aux solutions techniques adoptées pour garantir que continue d'être assurée la conformité du système d'IA aux les exigences pertinentes énoncées au chapitre III, section 2;

g) les procédures de validation et d'essai utilisées, y compris les informations sur les données de validation et d'essai utilisées et leurs principales caractéristiques; les indicateurs utilisés pour mesurer l'exactitude, la robustesse et le respect des autres exigences pertinentes énoncées au chapitre III, section 2, ainsi que les éventuelles incidences discriminatoires; les journaux de test et tous les rapports de test datés et signés par les personnes responsables, y compris en ce qui concerne les modifications prédéterminées visées au point f);

h) les mesures de cybersécurité qui ont été prises;

3. des informations détaillées sur la surveillance, le fonctionnement et le contrôle du système d'IA, en particulier en ce qui concerne: les capacités et les limites du système sur le plan de sa performance, y compris le degré d'exactitude pour des personnes ou des groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé et le niveau global d'exactitude prévu par rapport à sa destination; les résultats non intentionnels et sources de risques prévisibles pour la santé et la sécurité, les droits fondamentaux et en termes de discrimination compte tenu de la destination du système d'IA; les mesures de contrôle humain nécessaires conformément à l'article 14, y compris les mesures techniques mises en place pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA; les spécifications concernant les données d'entrée, le cas échéant;

4. une description de l'adéquation des indicateurs de performance à ce système d'IA spécifique;

5. une description détaillée du système de gestion des risques conformément à l'article 9;

6. une description des modifications pertinentes apportées par le fournisseur au système tout au long de son cycle de vie;

7. une liste des normes harmonisées appliquées, en totalité ou en partie, dont les références ont été publiées au *Journal officiel de l'Union européenne*; lorsqu'aucune norme harmonisée de ce type n'a été appliquée, une description détaillée des solutions adoptées pour satisfaire aux exigences énoncées au chapitre III, section 2, y compris une liste des autres normes pertinentes et spécifications techniques appliquées;

8. une copie de la déclaration UE de conformité visée à l'article 47;

9. une description détaillée du système en place pour évaluer les performances du système d'IA après la commercialisation conformément à l'article 72, y compris le plan de surveillance après commercialisation visé à l'article 72, paragraphe 3.

▼B

ANNEXE V

Déclaration UE de conformité

La déclaration UE de conformité visée à l'article 47 contient l'ensemble des informations suivantes:

1. le nom et le type du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;

2. le nom et l'adresse du fournisseur ou, le cas échéant, de son mandataire;

3. une attestation certifiant que la déclaration UE de conformité visée à l'article 47 est établie sous la seule responsabilité du fournisseur;

4. une déclaration attestant que le système d'IA respecte le présent règlement et, le cas échéant, toute autre législation de l'Union applicable prévoyant l'établissement de la déclaration UE de conformité visée à l'article 47;

5. lorsqu'un système d'IA nécessite le traitement de données à caractère personnel, une déclaration qui atteste que ledit système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 ainsi qu'à la directive (UE) 2016/680;

6. des références aux éventuelles normes harmonisées pertinentes utilisées ou aux éventuelles autres spécifications communes par rapport auxquelles la conformité est déclarée;

7. le cas échéant, le nom et le numéro d'identification de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré;

8. le lieu et la date de délivrance de la déclaration, le nom et la fonction du signataire ainsi que la mention de la personne pour le compte de laquelle ce dernier a signé, et une signature.

▼B

ANNEXE VI

Procédure d'évaluation de la conformité fondée sur le contrôle interne

1. La procédure d'évaluation de la conformité fondée sur le contrôle interne est la procédure d'évaluation de la conformité décrite aux points 2, 3 et 4.

2. Le fournisseur vérifie que le système de gestion de la qualité établi est conforme aux exigences de l'article 17.

3. Le fournisseur examine les informations contenues dans la documentation technique afin d'évaluer la conformité du système d'IA aux exigences essentielles pertinentes énoncées au chapitre III, section 2.

4. Le fournisseur vérifie également que le processus de conception et de développement du système d'IA et son système de surveillance après commercialisation prévu à l'article 72 sont cohérents avec la documentation technique.

▼B

ANNEXE VII

Conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique

1. Introduction

La conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique est la procédure d'évaluation de la conformité décrite aux points 2 à 5.

2. Vue d'ensemble

Le système de gestion de la qualité approuvé pour la conception, le développement et les essais des systèmes d'IA conformément à l'article 17 est examiné conformément au point 3 et soumis à la surveillance spécifiée au point 5. La documentation technique du système d'IA est examinée conformément au point 4.

3. Système de gestion de la qualité

3.1. La demande du fournisseur comprend:

a) le nom et l'adresse du fournisseur, ainsi que le nom et l'adresse d'un mandataire si la demande est introduite par celui-ci;

b) la liste des systèmes d'IA couverts par le même système de gestion de la qualité;

c) la documentation technique de chaque système d'IA couvert par le même système de gestion de la qualité;

d) la documentation relative au système de gestion de la qualité qui couvre tous les aspects énumérés à l'article 17;

e) une description des procédures en place pour garantir que le système de gestion de la qualité reste adéquat et efficace;

f) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié.

3.2. Le système de gestion de la qualité est évalué par l'organisme notifié, qui détermine s'il satisfait aux exigences visées à l'article 17.

La décision est notifiée au fournisseur ou à son mandataire.

La notification contient les conclusions de l'évaluation du système de gestion de la qualité et la décision d'évaluation motivée.

3.3. Le système de gestion de la qualité tel qu'approuvé continue d'être mis en œuvre et adapté par le fournisseur afin de rester adéquat et efficace.

3.4. Toute modification envisagée du système de gestion de la qualité approuvé ou de la liste des systèmes d'IA couverts par ce dernier est portée à l'attention de l'organisme notifié par le fournisseur.

Les modifications proposées sont examinées par l'organisme notifié, qui décide si le système de gestion de la qualité modifié continue de satisfaire aux exigences visées au point 3.2, ou si une réévaluation est nécessaire.

L'organisme notifié notifie sa décision au fournisseur. La notification contient les conclusions de l'examen des modifications et la décision d'évaluation motivée.

▼B

4. Contrôle de la documentation technique

4.1. Outre la demande visée au point 3, une demande est déposée par le fournisseur auprès d'un organisme notifié de son choix pour l'évaluation de la documentation technique relative au système d'IA que le fournisseur prévoit de mettre sur le marché ou de mettre en service et qui est couvert par le système de gestion de la qualité visé au point 3.

4.2. La demande comprend:

a) le nom et l'adresse du fournisseur;

b) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié;

c) la documentation technique visée à l'annexe IV.

4.3. La documentation technique est examinée par l'organisme notifié. Lorsque cela est pertinent et dans les limites de ce qui est nécessaire à l'accomplissement de ses tâches, l'organisme notifié se voit accorder un accès complet aux jeux de données d'entraînement, de validation et d'essai utilisés, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'API ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

4.4. Lors de l'examen de la documentation technique, l'organisme notifié peut exiger que le fournisseur apporte des preuves supplémentaires ou effectue des essais supplémentaires afin de permettre une évaluation correcte de la conformité du système d'IA avec les exigences énoncées au chapitre III, section 2. Lorsque l'organisme notifié n'est pas satisfait des essais effectués par le fournisseur, l'organisme notifié effectue directement des essais adéquats, le cas échéant.

4.5. Lorsque cela est nécessaire pour évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2, après que tous les autres moyens raisonnables de vérifier la conformité ont été épuisés et se sont révélés insuffisants, et sur demande motivée, l'accès aux modèles d'entraînement et aux modèles entraînés du système d'IA, y compris à ses paramètres pertinents, est aussi accordé à l'organisme notifié. Cet accès est soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires.

4.6. La décision de l'organisme notifié est notifiée au fournisseur ou à son mandataire. La notification contient les conclusions de l'évaluation de la documentation technique et la décision d'évaluation motivée.

Lorsque le système d'IA est conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié délivre un certificat d'évaluation UE de la documentation technique. Le certificat indique le nom et l'adresse du fournisseur, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du système d'IA.

Le certificat et ses annexes contiennent toutes les informations pertinentes pour permettre l'évaluation de la conformité du système d'IA et le contrôle du système d'IA pendant son utilisation, le cas échéant.

Lorsque le système d'IA n'est pas conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié refuse de délivrer un certificat d'évaluation UE de la documentation technique et en informe le demandeur, en lui précisant les raisons de son refus.

▼B

Lorsque le système d'IA ne satisfait pas à l'exigence relative aux données utilisées pour l'entraîner, il devra être entraîné à nouveau avant l'introduction d'une nouvelle demande d'évaluation de la conformité. Dans ce cas, la décision d'évaluation motivée de l'organisme notifié refusant de délivrer le certificat d'évaluation UE de la documentation technique contient des considérations spécifiques sur la qualité des données utilisées pour entraîner le système d'IA, en particulier sur les raisons de la non-conformité.

4.7. Les éventuelles modifications du système d'IA susceptibles d'avoir une incidence sur la conformité du système d'IA avec les exigences ou sur sa destination sont évaluées par l'organisme notifié qui a délivré le certificat d'évaluation UE de la documentation technique. Le fournisseur informe cet organisme notifié de son intention d'introduire une telle modification ou s'il prend autrement connaissance de l'existence de telles modifications. Les modifications envisagées sont évaluées par l'organisme notifié, qui décide si elles nécessitent une nouvelle évaluation de la conformité conformément à l'article 43, paragraphe 4, ou si elles peuvent faire l'objet d'un document complémentaire au certificat d'évaluation UE de la documentation technique. Dans ce dernier cas, l'organisme notifié évalue les modifications, informe le fournisseur de sa décision et, lorsque les modifications sont approuvées, lui fournit un document complémentaire au certificat d'évaluation UE de la documentation technique.

5. Surveillance du système de gestion de la qualité approuvé

5.1. Le but de la surveillance effectuée par l'organisme notifié visé au point 3 est de s'assurer que le fournisseur se conforme dûment aux conditions du système de gestion de la qualité approuvé.

5.2. À des fins d'évaluation, le fournisseur autorise l'organisme notifié à accéder aux locaux où les systèmes d'IA sont conçus, développés ou mis à l'essai. Le fournisseur partage en outre avec l'organisme notifié toutes les informations nécessaires.

5.3. L'organisme notifié effectue périodiquement des audits pour s'assurer que le fournisseur maintient et applique le système de gestion de la qualité; il transmet un rapport d'audit au fournisseur. Dans le cadre de ces audits, l'organisme notifié peut effectuer des essais supplémentaires des systèmes d'IA pour lesquels un certificat d'évaluation UE de la documentation technique a été délivré.

▼B

ANNEXE VIII

Informations à fournir lors de l'enregistrement d'un système d'IA à haut risque conformément à l'article 49

Section A - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 1

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 1:

1. le nom, l'adresse et les coordonnées du fournisseur;

2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;

3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;

4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;

5. une description de la destination du système d'IA ainsi que des composants et fonctions gérées au moyen de ce système d'IA;

6. une description de base et concise des informations utilisées par le système (données, entrées) et de sa logique de fonctionnement;

7. le statut du système d'IA (sur le marché ou en service; plus mis sur le marché/en service, rappelé);

8. le type, le numéro et la date d'expiration du certificat délivré par l'organisme notifié et le nom ou le numéro d'identification de cet organisme notifié, le cas échéant;

9. une copie numérisée du certificat visé au point 8, le cas échéant;

10. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union;

11. une copie de la déclaration UE de conformité visée à l'article 47;

12. une notice d'utilisation en format électronique; ces informations ne sont pas à fournir pour les systèmes d'IA à haut risque dans les domaines des activités répressives ou de la migration, de l'asile et de la gestion des contrôles aux frontières visés à l'annexe III, points 1, 6 et 7;

13. une adresse URL vers des informations supplémentaires (facultatif).

Section B - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 2

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à enregistrer conformément à l'article 49, paragraphe 2:

1. le nom, l'adresse et les coordonnées du fournisseur;

2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;

3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;

4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;

▼B

5. une description de la destination du système d'IA;

6. la ou les conditions visées à l'article 6, paragraphe 3, sur la base desquelles le système d'IA est considéré comme n'étant pas à haut risque;

7. un résumé succinct des motifs pour lesquels le système d'IA est considéré comme n'étant pas à haut risque en application de la procédure prévue à l'article 6, paragraphe 3;

8. le statut du système d'IA (sur le marché ou en service; plus sur le marché/en service, rappelé);

9. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union.

Section C - Informations à fournir par les déployeurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 3

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 3:

1. le nom, l'adresse et les coordonnées du déployeur;

2. le nom, l'adresse et les coordonnées de toute personne qui soumet des informations au nom du déployeur;

3. l'adresse URL de l'entrée du système d'IA dans la base de données de l'UE par son fournisseur;

4. une synthèse des conclusions de l'analyse d'impact sur les droits fondamentaux réalisée conformément à l'article 27;

5. un résumé de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, comme précisé à l'article 26, paragraphe 8, du présent règlement, le cas échéant.

▼B

ANNEXE IX

Informations à fournir lors de l'enregistrement de systèmes d'IA à haut risque énumérés à l'annexe III en ce qui concerne les essais en conditions réelles conformément à l'article 60

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les essais en conditions réelles à enregistrer conformément à l'article 60:

1. un numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles;

2. le nom et les coordonnées du fournisseur ou du fournisseur potentiel et des déployeurs participant aux essais en conditions réelles;

3. une brève description du système d'IA et de sa destination, ainsi que d'autres informations nécessaires à l'identification du système;

4. une synthèse des caractéristiques principales du plan d'essais en conditions réelles;

5. des informations sur la suspension ou la cessation des essais en conditions réelles.

▼B

ANNEXE X

Actes législatifs de l'Union relatifs aux systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

1. Système d'information Schengen

   a) Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).

   b) Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018, p. 14).

   c) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

2. Système d'information sur les visas

   a) Règlement (UE) 2021/1133 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (UE) n° 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 et (UE) 2019/818 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système d'information sur les visas (JO L 248 du 13.7.2021, p. 1).

   b) Règlement (UE) 2021/1134 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) n° 767/2008, (CE) n° 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 et (UE) 2019/1896 du Parlement européen et du Conseil et abrogeant les décisions 2004/512/CE et 2008/633/JAI du Conseil, aux fins de réformer le système d'information sur les visas (JO L 248 du 13.7.2021, p. 11).

3. Eurodac

   Règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'«Eurodac» pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/1315, (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) n° 603/2013 du Parlement européen et du Conseil (JO L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Système d'entrée/de sortie

   Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 (JO L 327 du 9.12.2017, p. 20).

▼B

5. Système européen d'information et d'autorisation concernant les voyages

   a) Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n° 1077/2011, (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1).

   b) Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) (JO L 236 du 19.9.2018, p. 72).

6. Système européen d'information sur les casiers judiciaires concernant des ressortissants de pays tiers et des apatrides

   Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

7. Interopérabilité

   a) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) n° 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI (JO L 135 du 22.5.2019, p. 27).

   b) Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85).

▼B

ANNEXE XI

Documentation technique visée à l'article 53, paragraphe 1, point a) – documentation technique pour les fournisseurs de modèles d'IA à usage général

Section 1

Informations devant être fournies par tous les fournisseurs de modèles d'IA à usage général

La documentation technique visée à l'article 53, paragraphe 1, point a), contient au moins les informations ci-après, en fonction de la taille et du profil de risque du modèle:

1. Une description générale du modèle d'IA à usage général, y compris:

   a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;

   b) les politiques applicables en matière d'utilisation acceptable;

   c) la date de publication et les méthodes de distribution;

   d) l'architecture et le nombre de paramètres;

   e) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;

   f) la licence.

2. Une description détaillée des éléments du modèle visés au point 1, et des informations pertinentes sur le processus de développement, y compris les éléments suivants:

   a) les moyens techniques (p. ex.: notice d'utilisation, infrastructure, outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;

   b) les spécifications de conception du modèle et du processus d'entraînement, y compris les méthodes et techniques d'entraînement, les principaux choix de conception, y compris le raisonnement et les hypothèses retenues; ce que le modèle est conçu pour optimiser, ainsi que la pertinence des différents paramètres, le cas échéant;

   c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation (p. ex.: nettoyage, filtrage, etc.), le nombre de points de données, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées, ainsi que toutes les autres mesures visant à détecter l'inadéquation des sources de données et les méthodes permettant de détecter les biais identifiables, le cas échéant;

   d) les ressources informatiques utilisées pour entraîner le modèle (p. ex.: nombre d'opérations en virgule flottante), le temps d'entraînement et d'autres détails pertinents liés à l'entraînement;

   e) la consommation d'énergie connue ou estimée du modèle.

   En ce qui concerne le point e), lorsque la consommation d'énergie du modèle est inconnue, la consommation d'énergie peut être estimée en s'appuyant sur des informations concernant les ressources informatiques utilisées.

Section 2

Informations devant être fournies par les fournisseurs de modèles d'IA à usage général présentant un risque systémique

1. Une description détaillée des stratégies d'évaluation, y compris les résultats de l'évaluation, sur la base des protocoles et outils d'évaluation publics disponibles ou d'autres méthodes d'évaluation. Les stratégies d'évaluation comprennent des critères, des indicateurs et les méthodes d'évaluation pour l'identification des limites.

▼B

2. Le cas échéant, une description détaillée des mesures mises en place pour effectuer des essais contradictoires internes et/ou externes (p. ex.: méthode de l'équipe rouge), des adaptations de modèles, y compris l'alignement et le réglage fin.

3. Le cas échéant, une description détaillée de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global.

▼B

ANNEXE XII

Informations relatives à la transparence visées à l'article 53, paragraphe 1, point b) – documentation technique pour les fournisseurs de modèles d'IA à usage général aux fournisseurs en aval qui intègrent le modèle dans leur système d'IA

Les informations visées à l'article 53, paragraphe 1, point b) comprennent au moins:

1. Une description générale du modèle d'IA à usage général, y compris:

   a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;

   b) les politiques applicables en matière d'utilisation acceptable;

   c) la date de publication et les méthodes de distribution;

   d) la manière dont le modèle interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels qui ne font pas partie du modèle lui-même, le cas échéant;

   e) les versions des logiciels pertinents liés à l'utilisation du modèle d'IA à usage général, le cas échéant;

   f) l'architecture et le nombre de paramètres;

   g) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;

   h) la licence pour le modèle.

2. Une description des éléments du modèle et de son processus de développement, notamment:

   a) les moyens techniques (p. ex.: la notice d'utilisation, l'infrastructure, les outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;

   b) les modalités (p. ex.: texte, image, etc.) et le format des entrées et des sorties, ainsi que leur taille maximale (p. ex.: taille de la fenêtre de contexte, etc.);

   c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation.

▼B

ANNEXE XIII

Critères de désignation des modèles d'IA à usage général présentant un risque systémique visés à l'article 51

Aux fins de déterminer si un modèle d'IA à usage général a des capacités ou un impact équivalents à ceux énoncés à l'article 51, paragraphe 1, point a), la Commission tient compte des critères suivants:

a) le nombre de paramètres du modèle;

b) la qualité ou la taille du jeu de données, par exemple mesurée en tokens;

c) la quantité de calcul utilisée pour l'entraînement du modèle, mesurée en nombre d'opérations en virgule flottante ou indiquée par une combinaison d'autres variables telles que le coût estimé de l'entraînement, le temps estimé nécessaire à l'entraînement ou la consommation d'énergie estimée pour l'entraînement;

d) les modalités d'entrée et de sortie du modèle, telles que la conversion de texte en texte (grands modèles de langage), la conversion de texte en image, la multimodalité et les seuils de l'état de l'art pour déterminer les capacités à fort impact pour chaque modalité, ainsi que le type spécifique d'entrées et de sorties (p. ex.: séquences biologiques);

e) les critères de référence et les évaluations des capacités du modèle, y compris en tenant compte du nombre de tâches ne nécessitant pas d'entraînement supplémentaire, sa capacité d'adaptation à apprendre de nouvelles tâches distinctes, son niveau d'autonomie et d'extensibilité, ainsi que les outils auxquels il a accès;

f) si le modèle a un impact important sur le marché intérieur en raison de sa portée, qui est présumée lorsqu'il a été mis à la disposition d'au moins 10 000 utilisateurs professionnels enregistrés établis dans l'Union;

g) le nombre d'utilisateurs finaux inscrits.