Conseil de
l'Union européenne

Bruxelles, le 25 novembre 2022
(OR. en)

14954/22

Dossier interinstitutionnel:
2021/0106(COD)

LIMITE

TELECOM 472
JAI 1494
COPEN 396
CYBER 374
DATAPROTECT 320
EJUSTICE 89
COSI 293
IXIM 267
ENFOPOL 569
RELEX 1556
MI 843
COMPET 918
CODEC 1773

NOTE

Origine:	Comité des représentants permanents (1re partie)
Destinataire:	Conseil
N° doc. préc.:	14336/22
N° doc. Cion:	8115/21
Objet:	Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union - Orientation générale

I. INTRODUCTION

1. Le 21 avril 2021, la Commission a adopté la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (**législation sur l'intelligence artificielle**).

2. Les objectifs de la proposition de la Commission sont de: veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés dans l'Union soient sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union; garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA; renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et de sécurité; et faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, tout en empêchant la fragmentation du marché.

II. TRAVAUX MENÉS PAR LES AUTRES INSTITUTIONS

3. Au sein du Parlement européen, les discussions sont menées par la commission du marché intérieur et de la protection des consommateurs (IMCO; rapporteur: Brando Benifei, S&D, Italie) et la commission des libertés civiles, de la justice et des affaires intérieures (LIBE; rapporteur Dragos Tudorache, Renew, Roumanie) dans le cadre d'une procédure avec commissions conjointes. La commission des affaires juridiques (JURI), la commission de l'industrie, de la recherche et de l'énergie (ITRE) et la commission de la culture et de l'éducation (CULT) sont associées aux travaux législatifs avec des compétences partagées et/ou exclusives. Les deux corapporteurs ont dévoilé leur projet de rapport en avril 2022, et le vote sur le rapport conjoint IMCO-LIBE est prévu pour le premier trimestre de 2023.

4. Le Comité économique et social européen a rendu son avis sur la proposition le 22 septembre 2021, tandis que le Comité européen des régions a rendu le sien le 2 décembre 2021.

5. Le 18 juin 2021, le comité européen de la protection des données (EDPB) et le Contrôleur européen de la protection des données (CEPD) ont rendu un avis conjoint sur la proposition.

6. La Banque centrale européenne (BCE) a rendu son avis le 29 décembre 2021 et l'a présenté au groupe "Télécommunications et société de l'information" (ci-après dénommé "groupe TELECOM"), le 10 février 2022.

III. ÉTAT DES TRAVAUX AU SEIN DU CONSEIL

1. Au sein du Conseil, l'examen de la proposition a été réalisé par le groupe TELECOM. Le groupe TELECOM a commencé à examiner la proposition sous la présidence portugaise, au cours de plusieurs réunions et ateliers tenus entre avril et juin 2021. Les travaux sur la proposition se sont poursuivis sous la présidence slovène, qui a élaboré la première proposition de compromis partiel concernant les **articles 1 à 7 et les annexes I à III**. En outre, la présidence slovène a organisé un Conseil informel des ministres des télécommunications d'une demi-journée consacré exclusivement à la proposition de législation sur l'IA, au cours duquel les ministres ont confirmé leur soutien à l'approche horizontale et centrée sur l'humain de la réglementation de l'IA. La présidence française a poursuivi le processus d'examen et, à la fin de son mandat, elle a remanié les parties restantes du texte (**articles 8 à 85 et annexes IV à IX**) et a présenté la première proposition de compromis consolidée complète concernant la législation sur l'IA le 17 juin 2022.

2. Le 5 juillet 2022, la présidence tchèque a tenu, sur la base d'un document présentant les options stratégiques, un débat d'orientation au sein du groupe TELECOM dont les résultats ont servi à élaborer le **deuxième texte de compromis**. Sur la base des réactions des délégations à ce compromis, la présidence tchèque a élaboré le **troisième texte de compromis**, qui a été présenté au groupe TELECOM et examiné par celui-ci les 22 et 29 septembre 2022. À l'issue de ces discussions, les délégations ont été invitées à formuler d'autres observations écrites, qui ont été utilisées par la présidence tchèque pour élaborer la **quatrième proposition de compromis**. Sur la base des discussions sur la quatrième proposition de compromis, qui ont eu lieu au sein du groupe TELECOM le 25 octobre et le 8 novembre 2022, ainsi qu'en tenant compte des observations écrites finales formulées par les États membres, la présidence tchèque a élaboré la **version finale du texte de compromis**, qui figure en annexe. Le 18 novembre, le Coreper a examiné cette proposition de compromis et est **convenu à l'unanimité de la soumettre au Conseil TTE (Télécommunications), sans modification, en vue d'une orientation générale** lors de sa session du 6 décembre 2022.

IV. PRINCIPAUX ÉLÉMENTS DE LA PROPOSITION DE COMPROMIS

1. Définition d'un système d'IA, pratiques interdites en matière d'IA, liste des cas d'utilisation des systèmes d'IA à haut risque figurant à l'annexe III et classification de systèmes d'IA comme systèmes à haut risque

1.1. Afin de veiller à ce que la définition d'un système d'IA fournisse des critères suffisamment clairs pour distinguer l'IA des systèmes logiciels plus classiques, le texte de compromis restreint la définition figurant à l'**article 3, paragraphe 1**, à des systèmes développés au moyen d'approches d'apprentissage automatique et d'approches fondées sur la logique et les connaissances.

1.2. En ce qui concerne la délégation de pouvoirs à la Commission relative aux mises à jour de la définition d'un système d'IA, l'**annexe I** et l'habilitation correspondante de la Commission pour la modifier au moyen d'actes délégués ont été supprimées. En remplacement, les nouveaux **considérants 6 *bis* et 6 *ter*** ont été ajoutés afin de clarifier ce qu'il convient d'entendre par les approches d'apprentissage automatique et les approches fondées sur la logique et les connaissances. Afin de veiller à ce que la législation sur l'IA demeure souple et à l'épreuve du temps, une possibilité d'adopter des actes d'exécution pour préciser davantage et mettre à jour les techniques utilisées dans le cadre des approches d'apprentissage automatique et des approches fondées sur la logique et les connaissances a été ajoutée à l'**article 4**.

1.3. En ce qui concerne les pratiques interdites en matière d'IA, à l'**article 5**, le texte de compromis prévoit d'étendre également aux acteurs privés l'interdiction de recourir à l'IA à des fins de notation sociale. En outre, la disposition interdisant l'utilisation de systèmes d'IA qui exploitent les vulnérabilités d'un groupe de personnes donné couvre désormais également les personnes vulnérables en raison de leur situation sociale ou économique. En ce qui concerne l'interdiction de l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public par les autorités répressives, le texte de compromis clarifie les objectifs pour lesquels une telle utilisation est considérée comme strictement nécessaires à des fins répressives et pour lesquels les autorités répressives devraient donc être autorisées exceptionnellement à utiliser de tels systèmes.

1.4. En ce qui concerne la liste des cas d'utilisation des systèmes d'IA à haut risque figurant à l'**annexe III**, trois d'entre eux ont été supprimés (détection des hypertrucages par les autorités répressives, analyse de la criminalité, vérification de l'authenticité des documents de voyage), deux ont été ajoutés (infrastructures numériques critiques, assurance-vie et assurance maladie) et d'autres ont été affinés. Dans le même temps, l'**article 7, paragraphe 1**, a été modifié afin de prévoir la possibilité non seulement d'ajouter des cas d'utilisation à haut risque à la liste au moyen d'actes délégués, mais également de les supprimer. Afin de veiller à ce que les droits fondamentaux soient adéquatement protégés en cas de telles suppressions, des dispositions supplémentaires ont été ajoutées à l'**article 7, paragraphe 3**, qui précisent les conditions qui devraient être remplies avant qu'un acte délégué puisse être adopté.

1.5. En ce qui concerne la classification de systèmes d'IA comme des systèmes à haut risque, la proposition de compromis comprend désormais une couche horizontale supplémentaire au-delà de la classification à haut risque établie à l'**annexe III**, afin de ne pas englober les systèmes d'IA qui ne sont pas susceptibles de causer des violations graves des droits fondamentaux ou d'autres risques importants. Plus précisément, l'**article 6, paragraphe 3**, contient de nouvelles dispositions selon lesquelles l'importance des résultats d'un système d'IA par rapport à l'action pertinente ou à la décision à prendre devrait également être prise en compte lors de la classification de systèmes d'IA comme des systèmes à haut risque. L'importance des résultats d'un système d'IA serait évaluée en fonction de son caractère purement accessoire ou non par rapport à l'action pertinente ou à la décision à prendre.

2. Exigences applicables aux systèmes d'IA à haut risque et responsabilités de différents acteurs de la chaîne de valeur de l'IA

2.1. Nombre des exigences applicables aux systèmes d'IA à haut risque établies au **chapitre 2 du titre III** de la proposition ont été clarifiées et adaptées de sorte qu'il soit, pour les parties intéressées, techniquement plus faisable et moins contraignant de s'y conformer, par exemple en ce qui concerne la qualité des données ou la documentation technique que les PME devraient établir pour démontrer que leurs systèmes d'IA à haut risque sont conformes aux exigences.

2.2. Compte tenu du fait que les systèmes d'IA sont développés et distribués dans le cadre de chaînes de valeur complexes, le texte de compromis comprend des modifications clarifiant la répartition des responsabilités et des rôles. Par exemple, des dispositions supplémentaires ont été ajoutées aux **articles 13 et 14**, permettant une coopération plus efficace entre les fournisseurs et les utilisateurs. Le texte de compromis vise également à clarifier la relation entre les responsabilités au titre de la législation sur l'IA et celles qui existent déjà en vertu d'autres actes législatifs, tels que la législation pertinente de l'Union en matière de protection des données ou sectorielle, y compris en ce qui concerne le secteur des services financiers. En outre, le nouvel **article 23 *bis*** indique de manière plus claire les situations dans lesquelles d'autres acteurs de la chaîne de valeur sont tenus d'assumer les responsabilités d'un fournisseur.

3. **Systèmes d'IA à usage général**

3.1. Un nouveau **titre I *bis*** a été ajouté pour tenir compte de situations dans lesquelles les systèmes d'IA peuvent être utilisés à de nombreuses fins différentes (IA à usage général), et des situations dans lesquelles il pourrait exister des circonstances où une technologie d'IA à usage général est intégrée dans un autre système qui pourrait devenir à haut risque. Le texte de compromis précise à l'**article 4 *bis*, paragraphe 1**, que certaines exigences applicables aux systèmes d'IA à haut risque s'appliqueraient également aux systèmes d'IA à usage général. Toutefois, plutôt qu'une application directe de ces exigences, un acte d'exécution préciserait comment elles devraient être appliquées en ce qui concerne les systèmes d'IA à usage général, sur la base d'une consultation et d'une analyse d'impact détaillée et en tenant compte des caractéristiques spécifiques de ces systèmes et de la chaîne de valeur correspondante, de la faisabilité technique et des évolutions du marché et des technologies. Le recours à un acte d'exécution permettra que les États membres soient dûment associés et gardent le dernier mot sur la manière dont les exigences seront appliquées dans ce contexte.

3.2. En outre, le texte de compromis de l'**article 4 *ter*, paragraphe 5**, prévoit aussi la possibilité d'adopter de nouveaux actes d'exécution qui fixeraient les modalités de coopération entre les fournisseurs de systèmes d'IA à usage général et d'autres fournisseurs ayant l'intention de mettre en service de tels systèmes ou de les mettre sur le marché de l'Union en tant que systèmes d'IA à haut risque, en particulier en ce qui concerne la fourniture d'informations.

4. **Clarification du champ d'application de la proposition de législation sur l'IA et dispositions relatives aux autorités répressives**

4.1. À l'**article 2**, une référence explicite a été faite à l'exclusion des finalités ayant trait à la sécurité nationale, à la défense et aux forces armées du champ d'application de la législation sur l'IA. De même, il a été clarifié que la législation sur l'IA ne devrait pas s'appliquer aux systèmes d'IA et à leurs résultats utilisés uniquement à des fins de recherche et de développement, ni aux obligations incombant aux personnes qui utilisent l'IA à des fins non professionnelles, qui ne relèveraient pas du champ d'application de la législation sur l'IA, hormis pour ce qui est des obligations de transparence.

4.2. Afin de tenir compte des spécificités des autorités répressives, un certain nombre de modifications ont été apportées aux dispositions relatives à l'utilisation des systèmes d'IA à des fins répressives. En particulier, certaines des définitions connexes figurant à l'**article 3**, telles que celles de "système d'identification biométrique à distance" et de "système d'identification biométrique à distance "en temps réel"" ont été affinées afin de préciser quelles situations relèveraient ou non de l'interdiction connexe et du cas d'utilisation à haut risque. La proposition de compromis comporte également d'autres modifications qui visent, sous réserve de garanties appropriées, à assurer un niveau adéquat de souplesse dans l'utilisation des systèmes d'IA à haut risque par les autorités répressives ou à tenir compte de la nécessité de respecter la confidentialité des données opérationnelles sensibles dans le cadre de leurs activités.

5. **Évaluation de la conformité, cadre de gouvernance, surveillance du marché, contrôle de l'application et sanctions**

5.1. Afin de simplifier le cadre de conformité de la législation sur l'IA, le texte de compromis contient un certain nombre de clarifications et de simplifications apportées aux dispositions relatives aux procédures d'évaluation de la conformité. Les dispositions relatives à la surveillance du marché ont également été clarifiées et simplifiées afin de les rendre plus efficaces et plus faciles à mettre en œuvre, en tenant compte de la nécessité d'adopter une approche proportionnée à cet égard. En outre, l'**article 41** a été révisé en profondeur afin de limiter le pouvoir discrétionnaire de la Commission en ce qui concerne l'adoption d'actes d'exécution établissant des spécifications techniques communes pour les exigences applicables aux systèmes d'IA à haut risque et aux systèmes d'IA à usage général.

5.2. Le texte de compromis modifie également de manière substantielle les dispositions relatives au Comité de l'IA (ci-après dénommé "Comité"), dans le but d'assurer une plus grande autonomie de celui-ci et de renforcer son rôle dans l'architecture de gouvernance de la législation sur l'IA. Dans ce contexte, les **articles 56 et 58** ont été révisés afin de renforcer le rôle du Comité de sorte qu'il soit mieux à même de soutenir les États membres dans la mise en œuvre de la législation sur l'IA et le contrôle de son application. Plus spécifiquement, les tâches du Comité ont été élargies et sa composition a été précisée. Afin de veiller à ce que les parties intéressées soient associées à toutes les questions relatives à la mise en œuvre de la législation sur l'IA, y compris l'élaboration des actes d'exécution et des actes délégués, une nouvelle exigence a été ajoutée, qui impose au Comité de créer un sous-groupe permanent servant de plateforme pour un large éventail de parties intéressées. Deux autres sous-groupes permanents pour les autorités de surveillance du marché et les autorités notifiantes devraient également être établis afin de renforcer la cohérence de la gouvernance et du contrôle de l'application de la législation sur l'IA dans l'ensemble de l'Union.

5.3. Afin d'améliorer encore le cadre de gouvernance, le texte de compromis comprend de nouveaux **articles 68 *bis* et 68 *ter***. L'**article 68 *bis*** prévoit l'obligation pour la Commission de désigner une ou plusieurs installations d'essai de l'Union dans le domaine de l'intelligence artificielle, qui devraient fournir des avis techniques ou scientifiques indépendants à la demande du Comité ou des autorités de surveillance du marché, tandis que l'**article 68 *ter*** crée une obligation pour la Commission de créer une réserve centrale d'experts indépendants destinée à soutenir les activités de contrôle de l'application menées au titre de la législation sur l'IA. Enfin, un nouvel **article 58 *bis*** prévoit l'obligation pour la Commission d'élaborer des lignes directrices sur la mise en œuvre de la législation sur l'IA.

5.4. En ce qui concerne les sanctions en cas de violations des dispositions de la législation sur l'IA, l'**article 71** du texte de compromis prévoit des plafonds plus proportionnés pour les montants des amendes administratives infligées aux PME et aux jeunes entreprises. En outre, quatre critères supplémentaires ont été ajoutés à l'**article 71, paragraphe 6**, pour décider du montant de l'amende administrative afin de préserver davantage leur proportionnalité globale.

6. **Transparence et autres dispositions en faveur des personnes concernées**

6.1. La proposition de compromis comprend un certain nombre de modifications qui renforcent la transparence en ce qui concerne l'utilisation des systèmes d'IA à haut risque. En particulier, l'**article 51** a été mis à jour afin de spécifier que certains utilisateurs de systèmes d'IA à haut risque qui sont des autorités, des agences ou des organismes publics seront également tenus de s'enregistrer dans la base de données de l'UE pour les systèmes d'IA à haut risque énumérés à l'annexe III. En outre, le nouvel **article 52, paragraphe 2 *bis***, met l'accent sur l'obligation faite aux utilisateurs d'un système de reconnaissance des émotions d'informer les personnes physiques lorsque celles-ci sont exposées à un tel système.

6.2. La proposition de compromis précise également dans le nouvel **article 63, paragraphe 11**, que toute personne physique ou morale ayant des raisons de penser qu'une infraction aux dispositions de la législation sur l'IA a été commise peut déposer une réclamation auprès de l'autorité de surveillance du marché compétente et peut s'attendre à ce que cette réclamation soit traitée conformément aux procédures spécifiques de cette autorité.

7. **Mesures de soutien à l'innovation**

7.1. Dans le but de créer un cadre juridique plus propice à l'innovation et afin de promouvoir un apprentissage réglementaire fondé sur des données probantes, les dispositions relatives aux mesures de soutien à l'innovation figurant à l'**article 53** ont été substantiellement modifiées dans le texte de compromis. Notamment, il a été précisé que les bacs à sable réglementaires de l'IA, qui sont censés établir un environnement contrôlé pour le développement, l'essai et la validation de systèmes d'IA innovants sous la supervision directe et les orientations des autorités nationales compétentes, devraient également permettre de tester des systèmes d'IA innovants dans des conditions réelles. En outre, de nouvelles dispositions ont été ajoutées aux **articles 54 *bis* et 54 *ter***, qui permettent des essais en conditions réelles non supervisés de systèmes d'IA, sous certaines conditions et garanties. Dans les deux cas, le texte de compromis précise comment ces nouvelles règles doivent être interprétées par rapport à d'autres législations sectorielles existantes sur les bacs à sable réglementaires.

7.2. Enfin, afin d'alléger la charge administrative pesant sur les petites entreprises, le texte de compromis contient, à l'**article 55**, une liste d'actions que la Commission doit engager pour soutenir ces opérateurs, et prévoit, à l'**article 55** ***bis***, certaines dérogations limitées et clairement définies.

V. CONCLUSION

1. Compte tenu de ce qui précède, le Conseil est invité à:
   - examiner le texte de compromis figurant à l'annexe de la présente note;
   - confirmer une orientation générale sur la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) lors de la session du Conseil TTE (Télécommunications) du 6 décembre 2022.

ANNEXE

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

ÉTABLISSANT DES RÈGLES HARMONISÉES CONCERNANT L'INTELLIGENCE ARTIFICIELLE (LÉGISLATION SUR L'INTELLIGENCE ARTIFICIELLE) ET MODIFIANT CERTAINS ACTES LÉGISLATIFS DE L'UNION

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

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment ses articles 16 et 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

vu l'avis du Comité des régions[2],

vu l'avis de la Banque centrale européenne[3],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

[1] JO C […] du […], p. […].
[2] JO C […] du […], p. […].
[3] Référence à l'avis de la BCE

(1) L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la commercialisation et l'utilisation de l'intelligence artificielle dans le respect des valeurs de l'Union. Le présent règlement poursuit un objectif justifié par un certain nombre de raisons impérieuses d'intérêt général, telles que la nécessité d'un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux, et il garantit la libre circulation transfrontière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions concernant le développement, la commercialisation et l'utilisation de systèmes d'IA, sauf autorisation expresse du présent règlement.

(2) Les systèmes d'intelligence artificielle (ci-après les "systèmes d'IA") peuvent être facilement déployés dans plusieurs secteurs de l'économie et de la société, y compris transfrontières, et circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales destinées à faire en sorte que l'intelligence artificielle soit sûre et à ce qu'elle soit développée et utilisée dans le respect des obligations en matière de droits fondamentaux. La disparité des règles nationales peut entraîner une fragmentation du marché intérieur et réduire la sécurité juridique pour les opérateurs qui développent, importent ou utilisent des systèmes d'IA. Il convient donc de garantir un niveau de protection cohérent et élevé dans toute l'Union, tandis que les divergences qui entravent la libre circulation des systèmes d'IA et des produits et services connexes au sein du marché intérieur devraient être évitées, en établissant des obligations uniformes pour les opérateurs et en garantissant la protection uniforme des raisons impérieuses d'intérêt général et des droits des citoyens dans l'ensemble du marché intérieur conformément à l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE). Dans la mesure où le présent règlement contient des règles spécifiques sur la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel, à savoir notamment des restrictions portant sur l'utilisation de systèmes d'IA pour l'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives, il convient de fonder le présent règlement, dès lors que ces règles spécifiques sont concernées, sur l'article 16 du TFUE. Compte tenu de ces règles spécifiques et du recours à l'article 16 du TFUE, il convient de consulter le comité européen de la protection des données.

(3) L'intelligence artificielle est une famille de technologies en évolution rapide, susceptible de contribuer à un large éventail de bienfaits économiques et sociétaux touchant l'ensemble des secteurs économiques et des activités sociales. En fournissant de meilleures prédictions, en optimisant les processus et l'allocation des ressources et en personnalisant les solutions numériques disponibles pour les particuliers et les organisations, le recours à l'intelligence artificielle peut donner des avantages concurrentiels décisifs aux entreprises et produire des résultats bénéfiques pour la société et l'environnement, dans des domaines tels que les soins de santé, l'agriculture, l'éducation et la formation, la gestion des infrastructures, l'énergie, les transports et la logistique, les services publics, la sécurité, la justice, l'utilisation efficace des ressources et de l'énergie ainsi que l'atténuation du changement climatique et l'adaptation à celui-ci.

(4) Cependant, en fonction des circonstances concernant son application et son utilisation, l'intelligence artificielle peut générer des risques et porter atteinte aux intérêts et droits publics protégés par le droit de l'Union. Le préjudice causé peut être matériel ou immatériel.

(5) Un cadre juridique de l'Union établissant des règles harmonisées sur l'intelligence artificielle est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'intelligence artificielle dans le marché intérieur, tout en garantissant un niveau élevé de protection des intérêts publics, comme la santé, la sécurité et la protection des droits fondamentaux, tels qu'ils sont reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, des règles régissant la mise sur le marché et la mise en service de certains systèmes d'IA devraient être établies, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des marchandises et des services. En établissant ces règles et dans le prolongement des travaux menés par le groupe d'experts de haut niveau sur l'intelligence artificielle, qui trouvent leur expression dans les lignes directrices en matière d'éthique pour une IA digne de confiance dans l'UE, le présent règlement contribue à la réalisation de l'objectif formulé par le Conseil européen[4] de faire de l'Union un acteur mondial de premier plan dans le développement d'une intelligence artificielle sûre, fiable et éthique, et il garantit la protection de principes éthiques expressément demandée par le Parlement européen[5].

---

4 Conseil européen, réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) - Conclusions, EUCO 13/20, 2020, p. 6.

5 Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, 2020/2012(INL).

(5 *bis*) Les règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA énoncées dans le présent règlement devraient s'appliquer dans tous les secteurs et, conformément à son approche relative au nouveau cadre législatif, être sans préjudice du droit de l'Union en vigueur, notamment en ce qui concerne la protection des données, la protection des consommateurs, les droits fondamentaux, l'emploi et la sécurité des produits, que le présent règlement vient compléter. En conséquence, tous les droits et recours conférés par ce droit de l'Union aux consommateurs et aux autres personnes susceptibles d'être négativement touchés par les systèmes d'IA, y compris en ce qui concerne la réparation de dommages éventuels conformément à la directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux, restent inchangés et pleinement applicables. De plus, le présent règlement vise à renforcer l'efficacité de ces droits et recours existants en établissant des exigences et des obligations spécifiques, y compris en ce qui concerne la transparence, la documentation technique et la tenue de registres des systèmes d'IA. En outre, les obligations imposées aux différents opérateurs intervenant dans la chaîne de valeur de l'IA en vertu du présent règlement devraient s'appliquer sans préjudice des législations nationales, dans le respect du droit de l'Union, ayant pour effet de limiter l'utilisation de certains systèmes d'IA lorsque ces législations ne relèvent pas du champ d'application du présent règlement ou poursuivent d'autres objectifs légitimes d'intérêt public que ceux poursuivis par le présent règlement. Ainsi, le droit national du travail et les lois sur la protection des mineurs (c'est-à-dire des personnes âgées de moins de 18 ans) tenant compte de l'observation générale n° 25 (2021) des Nations unies sur les droits de l'enfant, dans la mesure où ils ne sont pas spécifiques aux systèmes d'IA et poursuivent d'autres objectifs légitimes d'intérêt public, ne devraient pas être affectés par le présent règlement.

(6) La notion de système d'IA devrait être clairement définie afin d'assurer la sécurité juridique, tout en offrant la flexibilité nécessaire pour s'adapter aux progrès technologiques à venir. La définition devrait être basée sur les caractéristiques fonctionnelles clés de l'intelligence artificielle, telles que ses capacités d'apprentissage, de raisonnement ou de modélisation, la distinguant de systèmes logiciels et d'approches de programmation plus simples. En particulier, aux fins du présent règlement, les systèmes d'IA devraient avoir la capacité, sur la base de données et d'entrées générées par la machine et/ou par l'homme, de déduire la manière d'atteindre un ensemble donné d'objectifs définis par l'homme, en utilisant des approches fondées sur l'apprentissage automatique et/ou la logique et les connaissances, et de produire des résultats tels que des contenus pour des systèmes d'IA générative (texte, vidéo ou images, par exemple), des prédictions, des recommandations ou des décisions qui influencent l'environnement avec lequel le système interagit, que ce soit dans une dimension physique ou numérique. Un système qui utilise des règles définies uniquement par des personnes physiques pour exécuter automatiquement des opérations ne devrait pas être considéré comme un système d'IA. Les systèmes d'IA peuvent être conçus pour fonctionner à différents niveaux d'autonomie et être utilisés seuls ou en tant que composant d'un produit, que le système soit physiquement incorporé dans le produit (intégré) ou qu'il serve la fonctionnalité du produit sans y être incorporé (non intégré). La notion d'autonomie d'un système d'IA se rapporte à la mesure dans laquelle un tel système fonctionne sans intervention humaine.

(6 *bis*) Les approches d'apprentissage automatique se concentrent sur le développement de systèmes capables d'apprendre et de déduire des données pour résoudre un problème d'application sans être explicitement programmés avec une série d'instructions étape par étape, de la saisie à la sortie. L'apprentissage fait référence au processus de calcul consistant à optimiser, à partir des données, les paramètres du modèle, qui est une construction mathématique générant un résultat basé sur les données d'entrée. L'éventail des problèmes abordés par l'apprentissage automatique mobilise généralement des tâches que d'autres approches ne permettent pas d'effectuer, soit parce qu'il n'est pas possible de formaliser le problème de façon appropriée, soit parce que la résolution du problème présente des difficultés inextricables avec des approches sans apprentissage. Les approches d'apprentissage automatique comprennent, par exemple, l'apprentissage supervisé, non supervisé et par renforcement, qui utilise diverses méthodes, parmi lesquelles l'apprentissage profond au moyen de réseaux neuronaux, les techniques statistiques d'apprentissage et d'inférence (y compris, par exemple, la régression logistique, l'estimation bayésienne) et les méthodes de recherche et d'optimisation.

(6 *ter*) Les approches fondées sur la logique et les connaissances sont axées sur le développement de systèmes dotés de capacités de raisonnement logique en matière de connaissances pour résoudre un problème d'application. Ces systèmes comportent généralement une base de connaissances et un moteur d'inférence qui génère des résultats en raisonnant sur la base de connaissances. La base de connaissances, généralement encodée par des experts humains, représente des entités et des relations logiques pertinentes pour le problème d'application, recourant à des formalismes fondés sur des règles, des ontologies ou des graphes de connaissances. Le moteur d'inférence agit sur la base de connaissances et extrait de nouvelles informations au moyen d'opérations telles que le tri, la recherche, la mise en correspondance ou le chaînage. Les approches fondées sur la logique et les connaissances comprennent, par exemple, la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et de déduction, le raisonnement (symbolique), les systèmes experts et les méthodes de recherche et d'optimisation.

(6 *quater*) Afin d'assurer des conditions uniformes d'exécution du présent règlement en ce qui concerne les approches d'apprentissage automatique et les approches fondées sur la logique et les connaissances, et de tenir compte des évolutions du marché et des technologies, il convient de conférer des compétences d'exécution à la Commission.

(6 *quinquies*) Il convient d'interpréter la notion d' "utilisateur" visée dans le présent règlement comme désignant toute personne physique ou morale, y compris une autorité publique, une agence ou un autre organisme, utilisant un système d'IA sous l'autorité de laquelle le système est utilisé. En fonction du type de système d'IA, l'utilisation du système peut affecter des personnes autres que l'utilisateur.

(7) Il convient d'interpréter la notion de données biométriques utilisée dans le présent règlement de manière cohérente avec la notion de données biométriques telle qu'elle est définie à l'article 4, point 14), du règlement (UE) 2016/679 du Parlement européen et du Conseil[6], à l'article 3, point 18), du règlement (UE) 2018/1725 du Parlement européen et du Conseil[7] et à l'article 3, point 13), de la directive (UE) 2016/680 du Parlement européen et du Conseil[8].

[6] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[7] Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

[8] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (directive en matière de protection des données dans le domaine répressif) (JO L 119 du 4.5.2016, p. 89).

(8) La notion de système d'identification biométrique à distance telle qu'elle est utilisée dans le présent règlement devrait être définie, sur le plan fonctionnel, comme un système d'IA destiné à identifier des personnes physiques, en règle générale à distance, sans leur participation active, par la comparaison des données biométriques d'une personne avec celles contenues dans un référentiel de données, quels que soient la technologie, les processus ou les types de données biométriques utilisés. Ces systèmes d'identification biométrique à distance sont généralement utilisés pour percevoir (scanner) plusieurs personnes ou leur comportement simultanément afin de faciliter sensiblement l'identification d'un certain nombre de personnes sans leur participation active. Une telle définition exclut les systèmes de vérification/d'authentification dont la seule finalité serait de confirmer qu'une personne physique est bien celle qu'elle prétend être, ainsi que les systèmes utilisés pour confirmer l'identité d'une personne physique à la seule fin d'avoir accès à un service, à un dispositif ou à des locaux. Cette exclusion est justifiée par le fait que ces systèmes sont susceptibles d'avoir une incidence mineure sur les droits fondamentaux des personnes physiques par rapport aux systèmes d'identification biométrique à distance qui peuvent être utilisés pour le traitement des données biométriques d'un grand nombre de personnes. Dans le cas des systèmes "en temps réel", la capture des données biométriques, la comparaison et l'identification se font toutes instantanément, quasi instantanément ou en tout état de cause sans décalage significatif. À cet égard, il convient, en prévoyant la possibilité de légers décalages, d'empêcher le contournement des règles du présent règlement relatives à l'utilisation "en temps réel" des systèmes d'IA en question. Les systèmes "en temps réel" reposent sur l'utilisation d'éléments "en direct" ou "en léger différé", comme des séquences vidéo, générés par une caméra ou un autre appareil doté de fonctionnalités similaires. Dans le cas des systèmes "a posteriori", en revanche, les données biométriques sont prélevées dans un premier temps et la comparaison et l'identification n'ont lieu qu'après un délai significatif. Cela suppose des éléments tels que des images ou des séquences vidéo, qui ont été générés par des caméras de télévision en circuit fermé ou des appareils privés avant l'utilisation du système à l'égard des personnes physiques concernées.

(9) Aux fins du présent règlement, la notion d'espace accessible au public devrait s'entendre comme désignant tout lieu physique accessible à un nombre indéterminé de personnes physiques, que le lieu en question soit privé ou public, et indépendamment de l'activité pour laquelle il peut être utilisé, comme pour un commerce (par exemple, magasins, restaurants, cafés), pour la prestation de services (par exemple, banques, activités professionnelles, hôtellerie), pour la pratique de sports (piscines, salles de sport, stades, par exemple), pour les transports (gares routières, stations de métro et gares ferroviaires, aéroports, moyens de transport, par exemple), pour les divertissements (par exemple, cinémas, théâtres, musées, salles de concert et de conférence), pour les loisirs ou autres (par exemple, routes et places publiques, parcs, forêts, terrains de jeux). Un lieu devrait également être classé comme accessible au public si, indépendamment de la capacité potentielle ou des restrictions de sécurité, l'accès est soumis à certaines conditions prédéterminées, qui peuvent être remplies par un nombre indéterminé de personnes, telles que l'achat d'un billet ou d'un titre de transport, l'enregistrement préalable ou le fait d'avoir un certain âge. En revanche, un lieu ne devrait pas être considéré comme accessible au public si l'accès est limité à certaines personnes physiques définies, soit par le droit de l'Union, soit par le droit national directement lié à la sûreté ou à la sécurité publiques, ou par la manifestation claire de la volonté de la personne disposant de l'autorité compétente sur le lieu. Le seul fait d'avoir une possibilité d'accès (par exemple, une porte déverrouillée ou une porte ouverte dans une clôture) n'implique pas que le lieu soit accessible au public en présence d'indications ou de circonstances suggérant le contraire (par exemple, des signes d'interdiction ou de restriction d'accès). Les locaux des entreprises et des usines, ainsi que les bureaux et les lieux de travail qui sont destinés à être accessibles uniquement aux employés et prestataires de services concernés sont des lieux qui ne sont pas accessibles au public. Les espaces accessibles au public ne devraient pas inclure les prisons ni les zones de contrôle aux frontières. D'autres zones peuvent être composées à la fois de zones non accessibles au public et de zones accessibles au public, comme le hall d'un bâtiment d'habitation privé par lequel il faut passer pour accéder au bureau d'un médecin ou le hall d'un aéroport. Les espaces en ligne ne sont pas non plus couverts, car ce ne sont pas des espaces physiques. Le caractère accessible ou non au public d'un espace donné devrait cependant être déterminé au cas par cas, en tenant compte des particularités de la situation en question.

(10) Afin de garantir des conditions de concurrence équitables et une protection efficace des droits et libertés des citoyens dans toute l'Union, les règles établies par le présent règlement devraient s'appliquer de manière non discriminatoire aux fournisseurs de systèmes d'IA, qu'ils soient établis dans l'Union ou dans un pays tiers, et aux utilisateurs de systèmes d'IA établis dans l'Union.

(11) Compte tenu de leur nature numérique, certains systèmes d'IA devraient relever du présent règlement même lorsqu'ils ne sont ni mis sur le marché, ni mis en service, ni utilisés dans l'Union. Cela devrait notamment être le cas lorsqu'un opérateur établi dans l'Union confie à un opérateur externe établi en dehors de l'Union la tâche d'exécuter certains services ayant trait à une activité devant être réalisée par un système d'IA, qui serait considéré comme étant à haut risque. Dans ces circonstances, l'opérateur établi en dehors de l'Union pourrait utiliser un système d'IA pour traiter des données légalement collectées et transférées depuis l'Union, et fournir à l'opérateur contractant établi dans l'Union le résultat de ce traitement, sans que ce système d'IA soit mis sur le marché, mis en service ou utilisé dans l'Union. Afin d'éviter le contournement des règles du présent règlement et d'assurer une protection efficace des personnes physiques situées dans l'Union, le présent règlement devrait également s'appliquer aux fournisseurs et aux utilisateurs de systèmes d'IA qui sont établis dans un pays tiers, dans la mesure où le résultat produit par ces systèmes est utilisé dans l'Union. Néanmoins, pour tenir compte des dispositions existantes et des besoins particuliers de coopération future avec les partenaires étrangers avec lesquels des informations et des preuves sont échangées, le présent règlement ne devrait pas s'appliquer aux autorités publiques d'un pays tiers ni aux organisations internationales lorsqu'elles agissent dans le cadre d'accords internationaux conclus au niveau national ou au niveau européen pour la coopération des services répressifs et judiciaires avec l'Union ou avec ses États membres. De tels accords ont été conclus bilatéralement entre des États membres et des pays tiers ou entre l'Union européenne, Europol et d'autres agences de l'UE, des pays tiers et des organisations internationales. Les autorités des États membres bénéficiaires et les institutions, organes et organismes de l'Union et les organismes qui utilisent ces résultats dans l'Union demeurent responsables de veiller à ce que leur utilisation soit conforme au droit de l'Union. Lors de la révision de ces accords internationaux ou de la conclusion de nouveaux accords à l'avenir, les parties contractantes devraient tout mettre en œuvre pour aligner ces accords sur les exigences du présent règlement.

(12) Le présent règlement devrait également s'appliquer aux institutions, organes et organismes de l'Union lorsqu'ils agissent en tant que fournisseurs ou utilisateurs d'un système d'IA.

(-12 *bis*) Si et dans la mesure où des systèmes d'IA sont mis sur le marché, mis en service ou utilisés avec ou sans modification de ces systèmes à des fins militaires, de défense ou de sécurité nationale, ces systèmes devraient être exclus du champ d'application du présent règlement, indépendamment du type d'entité exerçant ces activités, par exemple qu'il s'agisse d'une entité publique ou privée. En ce qui concerne les finalités militaires et de défense, une telle exclusion est justifiée tant par l'article 4, paragraphe 2, du TUE que par les spécificités de la politique de défense des États membres et la politique de défense commune de l'Union relevant du titre V, chapitre 2, du traité sur l'Union européenne (TUE) qui sont soumises au droit international public, qui constitue donc le cadre juridique le plus approprié pour la réglementation des systèmes d'IA dans le contexte de l'utilisation de la force létale et d'autres systèmes d'IA dans le cadre d'activités militaires et de défense. En ce qui concerne les objectifs de sécurité nationale, l'exclusion est justifiée tant par le fait que la sécurité nationale reste de la seule responsabilité de chaque État membre, conformément à l'article 4, paragraphe 2, du TUE, que par la nature spécifique et les besoins opérationnels des activités liées à la sécurité nationale et par les règles nationales spécifiques applicables à ces activités. Néanmoins, si un système d'IA développé, mis sur le marché, mis en service ou utilisé à des fins militaires, de défense ou de sécurité nationale est, temporairement ou définitivement, utilisé en dehors de ce cadre à d'autres fins (par exemple, à des fins civiles ou humanitaires, à des fins répressives ou de sécurité publique), un tel système relèverait du champ d'application du présent règlement. Dans ce cas, l'entité qui utilise le système à des fins autres que militaires, de défense ou de sécurité nationale devrait veiller à la conformité du système avec le présent règlement, à moins que le système n'y soit déjà conforme. Les systèmes d'IA mis sur le marché ou mis en service à des fins exclues (par exemple, militaire, de défense ou de sécurité nationale) et à une ou plusieurs fins non exclues (par exemple, à des fins civiles, répressives, etc.) relèvent du champ d'application du présent règlement et les fournisseurs de ces systèmes devraient veiller au respect du présent règlement. En l'occurrence, le fait qu'un système d'IA puisse relever du champ d'application du présent règlement ne devrait pas affecter la possibilité pour les entités exerçant des activités de sécurité nationale, de défense et militaires, indépendamment du type d'entité exerçant ces activités, d'utiliser des systèmes d'IA à des fins de sécurité nationale, militaires et de défense, dont l'utilisation est exclue du champ d'application du présent règlement. Un système d'IA mis sur le marché à des fins civiles ou répressives qui est utilisé avec ou sans modification à des fins militaires, de défense ou de sécurité nationale ne devrait pas relever du champ d'application du présent règlement, indépendamment du type d'entité exerçant ces activités.

(12 *bis*) Le présent règlement ne devrait pas porter atteinte aux dispositions relatives à la responsabilité des prestataires de services intermédiaires énoncées dans la directive 2000/31/CE du Parlement européen et du Conseil (modifiée par la législation sur les services numériques).

(12 *ter*) Le présent règlement ne devrait pas porter atteinte aux activités de recherche et de développement et devrait respecter la liberté scientifique. Il est donc nécessaire d'exclure de son champ d'application les systèmes d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques et de veiller à ce que le règlement n'affecte pas autrement les activités de recherche et de développement scientifiques relatives aux systèmes d'IA. En ce qui concerne les activités de recherche axées sur les produits menées par les fournisseurs, les dispositions du présent règlement ne devraient pas non plus s'appliquer. Cette disposition est sans préjudice de l'obligation de se conformer au présent règlement lorsqu'un système d'IA relevant du champ d'application du présent règlement est mis sur le marché ou mis en service à la suite de cette activité de recherche et de développement, et sans préjudice de l'application des dispositions relatives aux sas réglementaires et aux essais en conditions réelles. En outre, sans préjudice de ce qui précède en ce qui concerne les systèmes d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques, tout autre système d'IA susceptible d'être utilisé pour mener une activité de recherche et de développement devrait rester soumis aux dispositions du présent règlement. En tout état de cause, toute activité de recherche et de développement devrait être menée conformément à des normes éthiques et professionnelles reconnues en matière de recherche scientifique.

(12 *quater*) Compte tenu de la nature et de la complexité de la chaîne de valeur des systèmes d'IA, il est essentiel de clarifier le rôle des acteurs susceptibles de contribuer au développement des systèmes d'IA, notamment des systèmes d'IA à haut risque. En particulier, il est nécessaire de préciser que les systèmes d'IA à usage général sont des systèmes d'IA destinés par le fournisseur à exécuter des fonctions de portée générale, telles que la reconnaissance d'images/de la parole, et dans une pluralité de contextes. Ils peuvent être utilisés comme des systèmes d'IA à haut risque en tant que tels ou comme des composants d'autres systèmes d'IA à haut risque. Par conséquent, en raison de leur nature particulière et afin de garantir un partage équitable des responsabilités tout au long de la chaîne de valeur de l'IA, ces systèmes devraient être soumis à des exigences et obligations proportionnées et plus spécifiques au titre du présent règlement, tout en garantissant un niveau élevé de protection des droits fondamentaux, de la santé et de la sécurité. En outre, les fournisseurs de systèmes d'IA à usage général, indépendamment du fait que ces systèmes puissent être utilisés comme des systèmes d'IA à haut risque en tant que tels par d'autres fournisseurs ou comme des composants de systèmes d'IA à haut risque, devraient coopérer, le cas échéant, avec les fournisseurs des systèmes d'IA à haut risque correspondants afin de leur permettre de se conformer aux obligations pertinentes au titre du présent règlement et avec les autorités compétentes établies en vertu du présent règlement. Afin de tenir compte des caractéristiques spécifiques des systèmes d'IA à usage général et de l'évolution rapide du marché et des avancées technologiques dans ce domaine, il convient de conférer des compétences d'exécution à la Commission pour préciser et adapter l'application des exigences établies au titre du présent règlement aux systèmes d'IA à usage général et pour préciser les informations à partager par les fournisseurs de systèmes d'IA à usage général afin de permettre aux fournisseurs de systèmes d'IA à haut risque correspondants de se conformer aux obligations qui leur incombent en vertu du présent règlement.

(13) Afin d'assurer un niveau cohérent et élevé de protection des intérêts publics en ce qui concerne la santé, la sécurité et les droits fondamentaux, il convient d'établir des normes communes pour l'ensemble des systèmes d'IA à haut risque. Ces normes devraient être conformes à la charte des droits fondamentaux de l'Union européenne (ci-après la "charte"), non discriminatoires et compatibles avec les engagements commerciaux internationaux de l'Union.

(14) Afin d'introduire un ensemble proportionné et efficace de règles contraignantes pour les systèmes d'IA, il convient de suivre une approche clairement définie fondée sur les risques. Cette approche devrait adapter le type et le contenu de ces règles à l'intensité et à la portée des risques que les systèmes d'IA peuvent générer. Il est donc nécessaire d'interdire certaines pratiques en matière d'intelligence artificielle, de fixer des exigences pour les systèmes d'IA à haut risque et des obligations pour les opérateurs concernés, ainsi que de fixer des obligations de transparence pour certains systèmes d'IA.

(15) Si l'intelligence artificielle peut être utilisée à de nombreuses fins positives, cette technologie peut aussi être utilisée à mauvais escient et fournir des outils nouveaux et puissants à l'appui de pratiques de manipulation, d'exploitation et de contrôle social. De telles pratiques sont particulièrement néfastes et devraient être interdites, car elles sont contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'État de droit, et elles portent atteinte aux droits fondamentaux de l'Union, y compris le droit à la non-discrimination, le droit à la protection des données et à la vie privée et les droits de l'enfant.

(16) Des techniques de manipulation fondées sur l'IA peuvent être utilisées pour persuader des personnes d'adopter des comportements indésirables ou pour les tromper en les poussant à prendre des décisions d'une manière qui met à mal et compromet leur autonomie, leur libre arbitre et leur liberté de choix. La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA qui altèrent substantiellement les comportements humains d'une manière qui est susceptible de causer un préjudice psychologique ou physique sont particulièrement dangereuses et devraient être interdites. Ces systèmes d'IA font intervenir des composants subliminaux tels que des stimuli sonores, visuels ou vidéo qui échappent à la perception humaine car ils se trouvent sous le seuil de la conscience, ou d'autres techniques subliminales qui mettent à mal ou altèrent l'autonomie de la personne, son libre arbitre ou sa liberté de choix, d'une manière dont l'individu n'est pas conscient ou, à supposer qu'il puisse en prendre conscience, sans qu'il puisse la contrôler ou y résister, comme avec une interface cerveau-machine ou la réalité virtuelle. En outre, des systèmes d'IA peuvent également exploiter les vulnérabilités d'un groupe particulier de personnes en raison de leur âge, d'un handicap au sens de la directive (UE) 2019/882, ou d'une situation sociale ou économique spécifique susceptible de rendre ces personnes plus vulnérables à l'exploitation, telles que les personnes vivant dans une extrême pauvreté ou appartenant à des minorités ethniques ou religieuses. De tels systèmes d'IA peuvent être mis sur le marché, mis en service ou utilisés avec pour objectif ou pour effet d'altérer substantiellement le comportement d'une personne d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice physique ou psychologique à cette personne ou à une autre personne ou à des groupes de personnes, y compris des dommages susceptibles de s'accumuler au fil du temps. L'intention d'altérer le comportement ne peut être présumée si l'altération résulte de facteurs externes au système d'IA qui échappent au contrôle du fournisseur ou de l'utilisateur, c'est-à-dire des facteurs qui ne peuvent être raisonnablement prévus et atténués par le fournisseur ou l'utilisateur du système d'IA. En tout état de cause, il n'est pas nécessaire que le fournisseur ou l'utilisateur ait l'intention de causer le préjudice physique ou psychologique, pour autant que ce préjudice résulte des pratiques de manipulation ou d'exploitation fondées sur l'IA. Les interdictions de telles pratiques en matière d'IA complètent les dispositions de la directive 2005/29/CE, notamment concernant le fait que les pratiques commerciales déloyales entraînant des préjudices économiques ou financiers pour les consommateurs sont interdites en toutes circonstances, qu'elles soient mises en place au moyen de systèmes d'IA ou autrement. Les interdictions des pratiques de manipulation et d'exploitation prévues par le présent règlement ne devraient pas affecter les pratiques licites dans le cadre de traitements médicaux tels que le traitement psychologique d'une maladie mentale ou la rééducation physique, lorsque ces pratiques sont effectuées conformément aux normes et à la législation médicales applicables. En outre, les pratiques commerciales courantes et légitimes qui sont conformes au droit applicable ne devraient pas en soi être considérées comme constituant des pratiques de manipulation préjudiciables en matière d'IA.

(17) Les systèmes d'IA permettant la notation sociale des personnes physiques par des autorités publiques ou par des acteurs privés peuvent conduire à des résultats discriminatoires et à l'exclusion de certains groupes. Ils peuvent porter atteinte au droit à la dignité et à la non-discrimination et sont contraires aux valeurs d'égalité et de justice. Ces systèmes d'IA évaluent ou classent les personnes physiques en fonction de leur comportement social dans plusieurs contextes ou en fonction de caractéristiques personnelles ou de traits de personnalité connus ou prédits. La note sociale obtenue à partir de ces systèmes d'IA peut conduire au traitement préjudiciable ou défavorable de personnes physiques ou de groupes entiers dans des contextes sociaux qui sont dissociés du contexte dans lequel les données ont été initialement générées ou collectées, ou à un traitement préjudiciable disproportionné ou injustifié au regard de la gravité de leur comportement social. Les systèmes d'IA impliquant de telles pratiques de notation inacceptables devraient donc être interdits. Cette interdiction ne devrait pas avoir d'incidence sur les évaluations licites des personnes physiques qui sont pratiquées dans un ou plusieurs buts précis, dans le respect de la loi.

(18) L'utilisation de systèmes d'IA pour l'identification biométrique à distance "en temps réel" de personnes physiques dans des espaces accessibles au public à des fins répressives est considérée comme particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux. En outre, du fait de l'immédiateté des effets et des possibilités limitées d'effectuer des vérifications ou des corrections supplémentaires, l'utilisation de systèmes fonctionnant "en temps réel" engendre des risques accrus pour les droits et les libertés des personnes concernées par les activités répressives.

(19) L'utilisation de ces systèmes à des fins répressives devrait donc être interdite, sauf dans des situations précisément répertoriées et rigoureusement définies, dans lesquelles l'utilisation se limite au strict nécessaire à la réalisation d'objectifs d'intérêt général dont l'importance est considérée comme supérieure aux risques encourus. Ces situations comprennent la recherche de victimes potentielles d'actes criminels, y compris des enfants disparus; certaines menaces pour la vie ou la sécurité physique des personnes physiques, y compris les attaques terroristes; et la détection, la localisation, l'identification ou les poursuites à l'encontre des auteurs ou des suspects d'infractions pénales visées dans la décision-cadre 2002/584/JAI du Conseil[9] si ces infractions pénales telles qu'elles sont définies dans le droit de l'État membre concerné sont passibles d'une peine ou d'une mesure de sûreté privative de liberté pour une période maximale d'au moins trois ans. Le seuil fixé pour la peine ou la mesure de sûreté privative de liberté prévue par le droit national contribue à garantir que l'infraction soit suffisamment grave pour justifier l'utilisation de systèmes d'identification biométrique à distance "en temps réel". En outre, sur les 32 infractions pénales énumérées dans la décision-cadre 2002/584/JAI du Conseil, certaines sont en pratique susceptibles d'être plus pertinentes que d'autres, dans le sens où le recours à l'identification biométrique à distance "en temps réel" sera vraisemblablement nécessaire et proportionné, à des degrés très divers, pour les mesures pratiques de détection, de localisation, d'identification ou de poursuites à l'encontre d'un auteur ou d'un suspect de l'une des différentes infractions pénales répertoriées, compte tenu également des différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des éventuelles conséquences négatives. Par ailleurs, le présent règlement devrait préserver la capacité des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile d'effectuer des contrôles d'identité en présence de la personne concernée conformément aux conditions prévues par le droit de l'Union et le droit national pour ces contrôles. En particulier, les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile devraient pouvoir utiliser des systèmes d'information, conformément au droit de l'Union ou au droit national, pour identifier une personne qui, lors d'un contrôle d'identité, soit refuse d'être identifiée, soit n'est pas en mesure de décliner son identité ou de la prouver, sans qu'il leur soit fait obligation par le présent règlement d'obtenir une autorisation préalable. Il peut s'agir, par exemple, d'une personne impliquée dans une infraction, qui ne veut pas ou ne peut pas divulguer son identité aux services répressifs en raison d'un accident ou de son état de santé.

[9] Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

(20) Afin de s'assurer que ces systèmes soient utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune des situations précisément répertoriées et rigoureusement définies, certains éléments devraient être pris en considération, notamment en ce qui concerne la nature de la situation donnant lieu à la demande et les conséquences de l'utilisation pour les droits et les libertés de toutes les personnes concernées, ainsi que les garanties et les conditions associées à l'utilisation. En outre, l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives devrait être soumise à des limites appropriées dans le temps et dans l'espace, eu égard en particulier aux preuves ou aux indications concernant les menaces, les victimes ou les auteurs. La base de données de référence des personnes devrait être appropriée pour chaque cas d'utilisation dans chacune des situations mentionnées ci-dessus.

(21) Toute utilisation d'un système d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives devrait être subordonnée à l'autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre. Cette autorisation devrait en principe être obtenue avant l'utilisation du système en vue d'identifier une ou plusieurs personnes. Des exceptions à cette règle devraient être autorisées dans des situations d'urgence dûment justifiées, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est de nature à rendre effectivement et objectivement impossible l'obtention d'une autorisation avant le début de l'utilisation. Dans de telles situations d'urgence, l'utilisation devrait être limitée au strict nécessaire et être assorties de garanties et de conditions appropriées, telles qu'elles sont déterminées dans la législation nationale et spécifiées dans le contexte de chaque cas d'utilisation urgente par les autorités répressives elles-mêmes. De plus, les autorités répressives devraient, dans de telles situations, chercher à obtenir une autorisation dans les meilleurs délais, tout en indiquant les raisons pour lesquelles elles n'ont pas pu la demander plus tôt.

(22) En outre, il convient de prévoir, dans le cadre exhaustif établi par le présent règlement, qu'une telle utilisation sur le territoire d'un État membre conformément au présent règlement ne devrait être possible que dans la mesure où l'État membre en question a décidé de prévoir expressément la possibilité d'autoriser une telle utilisation dans des règles détaillées de son droit national. Par conséquent, les États membres restent libres, en vertu du présent règlement, de ne pas prévoir une telle possibilité, ou de prévoir une telle possibilité uniquement pour certains objectifs parmi ceux susceptibles de justifier l'utilisation autorisée définis dans le présent règlement.

(23) L'utilisation de systèmes d'IA pour l'identification biométrique à distance "en temps réel" de personnes physiques dans des espaces accessibles au public à des fins répressives passe nécessairement par le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, et qui sont fondées sur l'article 16 du TFUE, devraient s'appliquer en tant que *lex specialis* pour ce qui est des règles sur le traitement des données biométriques figurant à l'article 10 de la directive (UE) 2016/680, réglementant ainsi de manière exhaustive cette utilisation et le traitement des données biométriques qui en résulte. Par conséquent, une telle utilisation et un tel traitement ne devraient être possibles que dans la mesure où ils sont compatibles avec le cadre fixé par le présent règlement, sans qu'il soit possible pour les autorités compétentes, lorsqu'elles agissent à des fins répressives en dehors de ce cadre, d'utiliser ces systèmes et de traiter les données y afférentes pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement ne vise pas à fournir la base juridique pour le traitement des données à caractère personnel en vertu de l'article 8 de la directive (UE) 2016/680. Cependant, l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins autres que répressives, y compris par les autorités compétentes, ne devrait pas être couverte par le cadre spécifique concernant l'utilisation à des fins répressives établi par le présent règlement. L'utilisation à des fins autres que répressives ne devrait donc pas être subordonnée à l'exigence d'une autorisation au titre du présent règlement et des règles détaillées du droit national applicable susceptibles de lui donner effet.

(24) Tout traitement de données biométriques et d'autres données à caractère personnel mobilisées lors de l'utilisation de systèmes d'IA pour l'identification biométrique, qui n'est pas lié à l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives, réglementée par le présent règlement, devrait rester conforme à toutes les exigences découlant de l'article 10 de la directive (UE) 2016/680. À des fins autres que répressives, l'article 9, paragraphe 1, du règlement (UE) 2016/679 et l'article 10, paragraphe 1, du règlement (UE) 2018/1725 interdisent le traitement de données biométriques aux fins d'identifier une personne physique de manière unique, sauf si l'une des situations visées aux deuxièmes paragraphes de ces deux articles s'applique.

(25) Conformément à l'article 6 *bis* du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE, l'Irlande n'est pas liée par les règles fixées à l'article 5, paragraphe 1, point d), et à l'article 5, paragraphes 2, 3 et 4, du présent règlement et adoptées sur la base de l'article 16 du TFUE concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du TFUE, lorsque l'Irlande n'est pas liée par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du TFUE doivent être respectées.

(26) Conformément aux articles 2 et 2 *bis* du protocole nº 22 sur la position du Danemark, annexé au TUE et au TFUE, le Danemark n'est pas lié par les règles fixées à l'article 5, paragraphe 1, point d), et à l'article 5, paragraphes 2, 3 et 4, du présent règlement et adoptées sur la base de l'article 16 du TFUE, ni soumis à leur application, lorsqu'elles concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou du chapitre 5 du titre V de la troisième partie du TFUE.

(27) Les systèmes d'IA à haut risque ne devraient être mis sur le marché de l'Union ou mis en service que s'ils satisfont à certaines exigences obligatoires. Ces exigences devraient garantir que les systèmes d'IA à haut risque disponibles dans l'Union ou dont les résultats sont utilisés d'une autre manière dans l'Union ne présentent pas de risques inacceptables pour d'importants intérêts publics de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union. Les systèmes d'IA désignés comme étant à haut risque devraient être limités aux systèmes qui ont une incidence préjudiciable significative sur la santé, la sécurité et les droits fondamentaux des citoyens dans l'Union, une telle limitation permettant, le cas échéant, de réduire au minimum toute éventuelle restriction au commerce international.

(28) Les systèmes d'IA pourraient avoir des effets néfastes sur la santé et la sécurité des citoyens, en particulier lorsque ces systèmes sont utilisés en tant que composants de produits. Conformément aux objectifs de la législation d'harmonisation de l'Union visant à faciliter la libre circulation des produits sur le marché intérieur et à garantir que seuls des produits sûrs et conformes à d'autres égards soient mis sur le marché, il est important de dûment prévenir et atténuer les risques pour la sécurité susceptibles d'être associés à un produit dans son ensemble en raison de ses composants numériques, y compris les systèmes d'IA. Par exemple, des robots de plus en plus autonomes, que ce soit dans le secteur de l'industrie manufacturière ou des services de soins et d'aide aux personnes, devraient pouvoir opérer et remplir leurs fonctions en toute sécurité dans des environnements complexes. De même, dans le secteur de la santé, où les enjeux pour la vie et la santé sont particulièrement importants, les systèmes de diagnostic de plus en plus sophistiqués et les systèmes soutenant les décisions humaines devraient être fiables et précis. L'ampleur de l'incidence négative du système d'IA sur les droits fondamentaux protégés par la charte est un critère particulièrement pertinent lorsqu'il s'agit de classer un système d'IA en tant que système à haut risque. Ces droits comprennent le droit à la dignité humaine, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'expression et d'information, la liberté de réunion et d'association, ainsi que la non-discrimination, la protection des consommateurs, les droits des travailleurs, les droits des personnes handicapées, le droit à un recours effectif et à accéder à un tribunal impartial, les droits de la défense et la présomption d'innocence, et le droit à une bonne administration. En plus de ces droits, il est important de souligner que les enfants bénéficient de droits spécifiques, consacrés à l'article 24 de la charte et dans la convention des Nations unies relative aux droits de l'enfant (et précisés dans l'observation générale nº 25 de la CNUDE en ce qui concerne l'environnement numérique), et que ces deux textes considèrent la prise en compte des vulnérabilités des enfants et la fourniture d'une protection et de soins appropriés comme étant nécessaires au bien-être de l'enfant. Le droit fondamental à un niveau élevé de protection de l'environnement consacré dans la charte et mis en œuvre dans les politiques de l'Union devrait également être pris en considération lors de l'évaluation de la gravité du préjudice qu'un système d'IA peut causer, notamment en ce qui concerne les conséquences pour la santé et la sécurité des personnes.

(29) En ce qui concerne les systèmes d'IA à haut risque constituant des composants de sécurité de produits ou de systèmes, ou qui sont eux-mêmes des produits ou des systèmes entrant dans le champ d'application du règlement (CE) nº 300/2008 du Parlement européen et du Conseil[10], du règlement (UE) nº 167/2013 du Parlement européen et du Conseil[11], du règlement (UE) nº 168/2013 du Parlement européen et du Conseil[12], de la directive 2014/90/UE du Parlement européen et du Conseil[13], de la directive (UE) 2016/797 du Parlement européen et du Conseil[14], du règlement (UE) 2018/858 du Parlement européen et du Conseil[15], du règlement (UE) 2018/1139 du Parlement européen et du Conseil[16] ou du règlement (UE) 2019/2144 du Parlement européen et du Conseil[17], il convient de modifier ces actes pour veiller à ce que la Commission tienne compte, sur la base des spécificités techniques et réglementaires de chaque secteur, et sans interférer avec les mécanismes et les autorités de gouvernance, d'évaluation de la conformité et de contrôle de l'application déjà en place en vertu de ces règlements, des exigences obligatoires applicables aux systèmes d'IA à haut risque définis dans le présent règlement lors de l'adoption ultérieure d'actes délégués ou d'actes d'exécution pertinents sur la base de ces actes.

---

10 Règlement (CE) nº 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) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72).

11 Règlement (UE) nº 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).

12 Règlement (UE) nº 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).

13 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).

14 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).

15 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) nº 715/2007 et (CE) nº 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

16 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) nº 2111/2005, (CE) nº 1008/2008, (UE) nº 996/2010, (UE) nº 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) nº 552/2004 et (CE) nº 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) nº 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

17 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) nº 78/2009, (CE) nº 79/2009 et (CE) nº 661/2009 du Parlement européen et du Conseil et les règlements (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010, (UE) nº 1008/2010, (UE) nº 1009/2010, (UE) nº 19/2011, (UE) nº 109/2011, (UE) nº 458/2011, (UE) nº 65/2012, (UE) nº 130/2012, (UE) nº 347/2012, (UE) nº 351/2012, (UE) nº 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

(30) En ce qui concerne les systèmes d'IA qui constituent des composants de sécurité de produits relevant de certaines législations d'harmonisation de l'Union, ou qui sont eux-mêmes de tels produits, il convient de les classer comme étant à haut risque au titre du présent règlement si le produit en question est soumis à la procédure d'évaluation de la conformité par un organisme tiers d'évaluation de la conformité conformément à la législation d'harmonisation de l'Union correspondante. Ces produits sont notamment les machines, les jouets, les ascenseurs, les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles, les équipements radioélectriques, les équipements sous pression, les équipements pour bateaux de plaisance, les installations à câbles, les appareils brûlant des combustibles gazeux, les dispositifs médicaux et les dispositifs médicaux de diagnostic in vitro.

(31) La classification d'un système d'IA comme étant à haut risque en application du présent règlement ne devrait pas nécessairement signifier que le produit utilisant un système d'IA en tant que composant de sécurité, ou que le système d'IA lui-même en tant que produit, est considéré comme étant "à haut risque" selon les critères établis dans la législation d'harmonisation de l'Union correspondante qui s'applique au produit en question. Tel est notamment le cas pour le règlement (UE) 2017/745 du Parlement européen et du Conseil[18] et le règlement (UE) 2017/746 du Parlement européen et du Conseil[19], dans le cadre desquels une évaluation de la conformité par un tiers est prévue pour les produits à risque moyen et les produits à haut risque.

[18] 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 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

[19] 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).

(32) En ce qui concerne les systèmes d'IA à haut risque autres que ceux qui constituent des composants de sécurité de produits ou qui sont eux-mêmes des produits, il convient de les classer comme étant à haut risque si, au vu de leur destination, ils présentent un risque élevé de causer un préjudice à la santé, à la sécurité ou aux droits fondamentaux des citoyens, en tenant compte à la fois de la gravité et de la probabilité du préjudice éventuel, et s'ils sont utilisés dans un certain nombre de domaines spécifiquement prédéfinis dans le règlement. La définition de ces systèmes est fondée sur la même méthode et les mêmes critères que ceux également envisagés pour les modifications ultérieures de la liste des systèmes d'IA à haut risque. Il importe également de préciser que, dans les cas de figure à haut risque visés à l'annexe III, il peut exister des systèmes qui n'entraînent pas de risque important pour les intérêts juridiques protégés dans ces cas de figure, compte tenu des résultats produits par le système d'IA. Par conséquent, ce n'est que lorsque ces résultats revêtent une grande importance (c'est-à-dire qu'ils ne sont pas purement accessoires) par rapport à l'action ou à la décision concernée, de sorte qu'ils créent un risque important pour les intérêts juridiques protégés, que le système d'IA qui génère de tels résultats devrait être considéré comme à haut risque. Ainsi, lorsque les informations fournies à l'homme par un système d'IA consistent en un profilage de personnes physiques au sens de l'article 4, point 4), du règlement (UE) 2016/679, de l'article 3, point 4, de la directive (UE) 2016/680 et de l'article 3, point 5), du règlement (UE) 2018/1725, ces informations ne devraient généralement pas être considérées comme accessoires dans le contexte des systèmes d'IA à haut risque visés à l'annexe III. Toutefois, si le résultat du système d'IA n'a qu'une pertinence négligeable ou mineure pour l'action ou la décision humaines, il peut être considéré comme purement accessoire, y compris, par exemple, les systèmes d'IA utilisés pour la traduction à des fins informatives ou pour la gestion de documents.

(33) Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Cela est particulièrement important lorsqu'il s'agit de l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. Par conséquent, les systèmes d'identification biométrique à distance "en temps réel" et "a posteriori" devraient être classés comme étant à haut risque. Compte tenu des risques qu'ils présentent, les deux types de systèmes d'identification biométrique à distance devraient être soumis à des exigences spécifiques en matière de capacités de journalisation et de contrôle humain.

(34) En ce qui concerne la gestion et l'exploitation des infrastructures critiques, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans le cadre de la gestion et de l'exploitation des infrastructures numériques critiques visées à l'annexe I, point 8, de la directive sur la résilience des entités critiques, du trafic routier et de la fourniture d'eau, de gaz, de chauffage et d'électricité, car leur défaillance ou leur mauvais fonctionnement peut mettre en danger la vie et la santé de personnes à grande échelle et entraîner des perturbations importantes dans la conduite ordinaire des activités sociales et économiques. Les composants de sécurité des infrastructures critiques, y compris des infrastructures numériques critiques, sont des systèmes utilisés pour protéger directement l'intégrité physique des infrastructures critiques ou la santé et la sécurité des personnes et des biens, mais qui ne sont pas nécessaires au fonctionnement du système. La défaillance ou le mauvais fonctionnement de ces composants pourrait directement entraîner des risques pour l'intégrité physique des infrastructures critiques et, partant, des risques pour la santé et la sécurité des personnes et des biens. Les composants destinés à être utilisés uniquement à des fins de cybersécurité ne devraient pas être considérés comme des composants de sécurité. Les systèmes de surveillance de la pression de l'eau ou les systèmes de commande des alarmes incendie dans les centres d'informatique en nuage sont des exemples de composants de sécurité de ces infrastructures critiques.

(35) Les systèmes d'IA utilisés dans l'éducation ou la formation professionnelle, notamment pour la prise de décision concernant l'accès, l'admission ou l'affectation de personnes à des établissements d'enseignement et de formation professionnelle ou à des programmes à tous les niveaux, ou pour évaluer les acquis d'apprentissage des personnes, devraient être considérés comme étant à haut risque car ils peuvent déterminer le parcours éducatif et professionnel d'une personne et ont par conséquent une incidence sur la capacité de cette personne à assurer sa propre subsistance. Lorsqu'ils sont mal conçus et utilisés, ces systèmes peuvent mener à des violations du droit à l'éducation et à la formation ainsi que du droit à ne pas subir de discriminations, et perpétuer des schémas historiques de discrimination.

(36) Les systèmes d'IA utilisés pour des questions liées à l'emploi, à la gestion de la main-d'œuvre et à l'accès à l'emploi indépendant, notamment pour le recrutement et la sélection de personnes, pour la prise de décisions de promotion et de licenciement, pour l'attribution des tâches fondée sur le comportement individuel ou les traits ou caractéristiques personnels, et pour le suivi ou l'évaluation des personnes dans le cadre de relations professionnelles contractuelles, devraient également être classés comme étant à haut risque, car ces systèmes peuvent avoir une incidence considérable sur les perspectives de carrière et les moyens de subsistance de ces personnes. Les relations professionnelles contractuelles en question devraient concerner également celles qui lient les employés et les personnes qui fournissent des services sur des plateformes telles que celles visées dans le programme de travail de la Commission pour 2021. Ces personnes ne devraient en principe pas être considérées comme des utilisateurs au sens du présent règlement. Tout au long du processus de recrutement et lors de l'évaluation, de la promotion ou du maintien des personnes dans des relations professionnelles contractuelles, les systèmes d'IA peuvent perpétuer des schémas historiques de discrimination, par exemple à l'égard des femmes, de certains groupes d'âge et des personnes handicapées, ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle. Les systèmes d'IA utilisés pour surveiller les performances et le comportement de ces personnes peuvent aussi avoir une incidence sur leurs droits à la protection des données et à la vie privée.

(37) Un autre domaine dans lequel l'utilisation des systèmes d'IA mérite une attention particulière est l'accès et le droit à certains services et prestations essentiels, publics et privés, devant permettre aux citoyens de participer pleinement à la société ou d'améliorer leur niveau de vie. En particulier, les systèmes d'IA utilisés pour évaluer la note de crédit ou la solvabilité des personnes physiques devraient être classés en tant que systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes à des ressources financières ou à des services essentiels tels que le logement, l'électricité et les services de télécommunication. Les systèmes d'IA utilisés à cette fin peuvent conduire à la discrimination à l'égard de personnes ou de groupes et perpétuer des schémas historiques de discrimination, par exemple fondés sur les origines raciales ou ethniques, les handicaps, l'âge ou l'orientation sexuelle, ou créer de nouvelles formes d'incidences discriminatoires. Compte tenu de l'incidence très limitée et des solutions de remplacement disponibles sur le marché, il convient d'exempter les systèmes d'IA utilisés à des fins d'évaluation de la solvabilité et de notation de crédit lorsqu'ils sont mis en service par des microentreprises ou des petites entreprises, au sens de l'annexe de la recommandation 2003/361/CE de la Commission pour leur usage propre. Les personnes physiques sollicitant ou recevant des prestations sociales et des services essentiels fournis par des autorités publiques sont généralement tributaires de ces prestations et services et se trouvent dans une position vulnérable par rapport aux autorités responsables. Lorsque des systèmes d'IA sont utilisés pour déterminer si ces prestations et services devraient être refusés, réduits, révoqués ou récupérés par les autorités, y compris pour déterminer si les bénéficiaires y ont légitimement droit, ils peuvent avoir une grande incidence sur les moyens de subsistance des personnes et porter atteinte à leurs droits fondamentaux, tels que le droit à la protection sociale, le principe de non-discrimination, le droit à la dignité humaine ou le droit à un recours effectif. Il convient donc de classer ces systèmes comme étant à haut risque. Néanmoins, le présent règlement ne devrait pas entraver la mise en place et l'utilisation, dans l'administration publique, d'approches innovantes qui bénéficieraient d'une utilisation plus large de systèmes d'IA conformes et sûrs, à condition que ces systèmes n'entraînent pas de risque élevé pour les personnes morales et physiques. Enfin, les systèmes d'IA utilisés pour l'envoi de services d'intervention d'urgence ou l'établissement de priorités dans l'envoi de ces services devraient aussi être classés comme étant à haut risque, car ils prennent des décisions dans des situations très critiques pour la vie, la santé et les biens matériels des personnes. Les systèmes d'IA sont également de plus en plus utilisés pour l'évaluation des risques liés aux personnes physiques et la tarification dans le cas de l'assurance-vie et de l'assurance maladie, ce qui peut avoir de graves conséquences sur la vie et la santé des personnes, dont l'exclusion financière et la discrimination, si ces systèmes ne sont pas dûment conçus, développés et utilisés. Afin de veiller à une approche cohérente dans le secteur des services financiers, l'exception susmentionnée pour les microentreprises ou les petites entreprises concernant leur usage propre devrait s'appliquer dans la mesure où elles fournissent et mettent elles-mêmes en service un système d'IA aux fins de la vente de leurs propres produits d'assurance.

(38) Les actions des autorités répressives qui supposent certaines utilisations de systèmes d'IA sont caractérisées par un degré important de déséquilibre des forces et peuvent conduire à la surveillance, à l'arrestation ou à la privation de la liberté d'une personne physique ainsi qu'à d'autres conséquences négatives sur des droits fondamentaux garantis par la charte. En particulier, si le système d'IA n'est pas entraîné avec des données de haute qualité, ne répond pas aux exigences appropriées en matière d'exactitude ou de robustesse, ou n'est pas correctement conçu et mis à l'essai avant d'être mis sur le marché ou mis en service d'une autre manière, il risque de traiter des personnes de manière discriminatoire ou, plus généralement, incorrecte ou injuste. En outre, l'exercice d'importants droits fondamentaux procéduraux, tels que le droit à un recours effectif et à accéder à un tribunal impartial, ainsi que les droits de la défense et la présomption d'innocence, pourrait être entravé, en particulier lorsque ces systèmes d'IA ne sont pas suffisamment transparents, explicables et documentés. Il convient donc de classer comme systèmes à haut risque un certain nombre de systèmes d'IA destinés à être utilisés dans un contexte répressif où l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter les conséquences négatives, conserver la confiance du public et garantir que des comptes soient rendus et que des recours efficaces puissent être exercés. Compte tenu de la nature des activités en question et des risques y afférents, ces systèmes d'IA à haut risque devraient comprendre en particulier les systèmes d'IA destinés à être utilisés par les autorités répressives pour réaliser des évaluations individuelles des risques, pour servir de polygraphes ou d'outils similaires ou pour analyser l'état émotionnel de personnes physiques, pour évaluer la fiabilité des preuves dans les procédures pénales, pour prédire la survenance ou la répétition d'une infraction pénale réelle ou potentielle sur la base du profilage de personnes physiques, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents délictuels de personnes physiques ou de groupes à des fins de profilage dans le cadre d'activités de détection, d'enquête ou de poursuite relatives à des infractions pénales. Les systèmes d'IA spécifiquement destinés à être utilisés pour des procédures administratives par les autorités fiscales et douanières ainsi que par les cellules de renseignement financier effectuant des tâches administratives d'analyse d'informations dans le cadre de la législation de l'Union relative à la lutte contre le blanchiment des capitaux ne devraient pas être considérés comme des systèmes d'IA à haut risque utilisés par les autorités répressives dans le cadre d'activités de prévention, de détection, d'enquête et de poursuite relatives à des infractions pénales.

(39) Les systèmes d'IA utilisés dans le domaine de la gestion de la migration, de l'asile et des contrôles aux frontières touchent des personnes qui sont souvent dans une position particulièrement vulnérable et qui dépendent du résultat des actions des autorités publiques compétentes. L'exactitude, la nature non discriminatoire et la transparence des systèmes d'IA utilisés dans ces contextes sont donc particulièrement importantes pour garantir le respect des droits fondamentaux des personnes concernées, notamment leurs droits à la libre circulation, à la non-discrimination, à la protection de la vie privée et des données à caractère personnel, à une protection internationale et à une bonne administration. Il convient donc de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes chargées de tâches dans les domaines de la gestion de la migration, de l'asile et des contrôles aux frontières pour servir de polygraphes ou d'outils similaires ou pour analyser l'état émotionnel d'une personne physique; pour évaluer certains risques posés par des personnes physiques entrant sur le territoire d'un État membre ou faisant une demande de visa ou d'asile; et pour aider les autorités publiques compétentes à examiner les demandes d'asile, de visa et de permis de séjour ainsi que les réclamations connexes, l'objectif étant de vérifier l'éligibilité des personnes physiques qui demandent un statut. Les systèmes d'IA utilisés dans le domaine de la gestion de la migration, de l'asile et des contrôles aux frontières couverts par le présent règlement devraient être conformes aux exigences procédurales pertinentes fixées par la directive 2013/32/UE du Parlement européen et du Conseil[20], le règlement (CE) nº 810/2009 du Parlement européen et du Conseil[21] et toute autre législation pertinente.

[20] Directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (JO L 180 du 29.6.2013, p. 60).

[21] Règlement (CE) nº 810/2009 du Parlement européen et du Conseil du 13 juillet 2009 établissant un code communautaire des visas (code des visas) (JO L 243 du 15.9.2009, p. 1).

(40) Certains systèmes d'IA destinés à être utilisés pour l'administration de la justice et les processus démocratiques devraient être classés comme étant à haut risque, compte tenu de leur incidence potentiellement significative sur la démocratie, l'état de droit, les libertés individuelles ainsi que le droit à un recours effectif et à accéder à un tribunal impartial. En particulier, pour faire face aux risques de biais, d'erreurs et d'opacité, il convient de classer comme étant à haut risque les systèmes d'IA destinés à aider les autorités judiciaires à interpréter les faits et la loi, et à appliquer la loi à un ensemble concret de faits. Cette qualification ne devrait cependant pas s'étendre aux systèmes d'IA destinés à être utilisés pour des activités administratives purement accessoires qui n'ont aucune incidence sur l'administration réelle de la justice dans des cas individuels, telles que l'anonymisation ou la pseudonymisation de décisions judiciaires, de documents ou de données, la communication entre membres du personnel ou les tâches administratives.

(41) Le fait qu'un système d'IA soit classé comme étant à haut risque au titre du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système est licite au titre d'autres actes du droit de l'Union ou au titre du droit national compatible avec le droit de l'Union, s'agissant notamment de la protection des données à caractère personnel, de l'utilisation de polygraphes et d'outils similaires, ou de l'utilisation d'autres systèmes d'analyse de l'état émotionnel des personnes physiques. Toute utilisation de ce type devrait continuer à être subordonnée aux exigences applicables découlant de la charte et des actes applicables du droit dérivé de l'Union et du droit national. Le présent règlement ne devrait pas être compris comme constituant un fondement juridique pour le traitement des données à caractère personnel, y compris des catégories spéciales de données à caractère personnel, le cas échéant, sauf s'il est prévu expressément autre chose dans le présent règlement.

(42) Afin d'atténuer les risques liés aux systèmes d'IA à haut risque commercialisés ou mis en service d'une autre manière sur le marché de l'Union, certaines exigences obligatoires devraient s'appliquer, en tenant compte de la destination du système et en fonction du système de gestion des risques à mettre en place par le fournisseur. En particulier, le système de gestion des risques devrait consister en un processus itératif continu planifié et se dérouler sur l'ensemble du cycle de vie d'un système d'IA à haut risque. Ce processus devrait garantir que le fournisseur identifie et analyse les risques pour la santé, la sécurité et les droits fondamentaux des personnes susceptibles d'être affectées par le système au regard de sa destination, y compris les risques éventuels découlant de l'interaction entre le système d'IA et l'environnement dans lequel il opère, et adopte en conséquence des mesures appropriées de gestion des risques tenant compte des évolutions technologiques.

(43) Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la qualité des jeux de données utilisés, la documentation technique et la tenue de registres, la transparence et la fourniture d'informations aux utilisateurs, le contrôle humain, ainsi que la robustesse, l'exactitude et la cybersécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux, selon la destination du système, et, aucune autre mesure moins contraignante pour le commerce n'étant raisonnablement disponible, elles n'imposent pas de restriction injustifiée aux échanges.

(44) Une haute qualité des données est essentielle au bon fonctionnement de nombreux systèmes d'IA, en particulier lorsque des techniques axées sur l'entraînement de modèles sont utilisées, afin de garantir que le système d'IA à haut risque fonctionne comme prévu et en toute sécurité et qu'il ne devient pas une source de discrimination interdite par le droit de l'Union. Des jeux de données d'entraînement, de validation et de test de haute qualité nécessitent la mise en œuvre de pratiques de gouvernance et de gestion des données appropriées. Les jeux de données d'entraînement, de validation et de test devraient être suffisamment pertinents et représentatifs, et avoir les propriétés statistiques appropriées, notamment en ce qui concerne les personnes ou les groupes de personnes sur lesquels le système d'IA à haut risque est destiné à être utilisé. Ces jeux de données devraient également être aussi exempts d'erreurs et complets que possible au regard de la destination du système d'IA, en tenant compte, de façon proportionnée, de la faisabilité technique et des évolutions technologiques, de la disponibilité des données et de la mise en œuvre de mesures appropriées de gestion des risques de manière à ce qu'il soit dûment remédié aux éventuelles lacunes des jeux de données. Cette exigence que les jeux de données soient complets et exempts d'erreurs ne devrait pas avoir d'effet sur l'utilisation de techniques respectueuses de la vie privée dans le contexte du développement et de la mise à l'essai des systèmes d'IA. Les jeux de données d'entraînement, de validation et de test devraient prendre en considération, dans la mesure requise au regard de leur destination, les propriétés, les caractéristiques ou les éléments qui sont particuliers au cadre ou au contexte géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA est destiné à être utilisé. Afin de protéger le droit d'autres personnes contre la discrimination qui pourrait résulter des biais dans les systèmes d'IA, les fournisseurs devraient être en mesure de traiter également des catégories spéciales de données à caractère personnel, pour des motifs d'intérêt public important au sens de l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et de l'article 10, paragraphe 2, point g), du règlement (UE) 2018/1725, afin d'assurer la surveillance, la détection et la correction des biais liés aux systèmes d'IA à haut risque.

(44 *bis*) Lors de l'application des principes visés à l'article 5, paragraphe 1, point c), du règlement (UE) 2016/679 et à l'article 4, paragraphe 1, point c), du règlement (UE) 2018/1725, en particulier le principe de minimisation des données, en ce qui concerne les jeux de données d'entraînement, de validation et de test au titre du présent règlement, il convient de tenir dûment compte de l'ensemble du cycle de vie du système d'IA.

(45) Pour le développement de systèmes d'IA à haut risque, certains acteurs, tels que les fournisseurs, les organismes notifiés et d'autres entités pertinentes, telles que les pôles d'innovation numérique, les installations d'expérimentation et d'essai et les centres de recherche, devraient être en mesure d'obtenir et d'utiliser des jeux de données de haute qualité dans leurs domaines d'activité respectifs liés au présent règlement. Les espaces européens communs des données créés par la Commission et la facilitation du partage de données d'intérêt public entre les entreprises et avec le gouvernement seront essentiels pour fournir un accès fiable, responsable et non discriminatoire à des données de haute qualité pour l'entraînement, la validation et la mise à l'essai des systèmes d'IA. Par exemple, dans le domaine de la santé, l'espace européen des données de santé facilitera l'accès non discriminatoire aux données de santé et l'entraînement d'algorithmes d'intelligence artificielle à l'aide de ces jeux de données, d'une manière respectueuse de la vie privée, sûre, rapide, transparente et digne de confiance, et avec une gouvernance institutionnelle appropriée. Les autorités compétentes concernées, y compris les autorités sectorielles, qui fournissent ou facilitent l'accès aux données peuvent aussi faciliter la fourniture de données de haute qualité pour l'entraînement, la validation et la mise à l'essai des systèmes d'IA.

(46) Il est essentiel de disposer d'informations sur la manière dont les systèmes d'IA à haut risque ont été développés et sur leur fonctionnement tout au long de leur cycle de vie afin de vérifier le respect des exigences du présent règlement. Cela nécessite la tenue de registres et la mise à disposition d'une documentation technique contenant les informations nécessaires pour évaluer la conformité du système d'IA avec les exigences pertinentes. Ces informations devraient notamment porter sur les caractéristiques générales, les capacités et les limites du système, sur les algorithmes, les données et les processus d'entraînement, d'essai et de validation utilisés, ainsi que sur le système de gestion des risques mis en place. La documentation technique devrait être tenue à jour. En outre, les fournisseurs ou utilisateurs devraient assurer la tenue des journaux générés automatiquement par le système d'IA à haut risque, comprenant par exemple les données de sortie, les dates et heures de début etc., dans la mesure où ces systèmes et les journaux liés se trouvent sous leur contrôle, durant une période adéquate pour leur permettre de remplir leurs obligations.

(47) Afin de remédier à l'opacité qui peut rendre certains systèmes d'IA incompréhensibles ou trop complexes pour les personnes physiques, un certain degré de transparence devrait être requis pour les systèmes d'IA à haut risque. Les utilisateurs devraient être capables d'interpréter les résultats produits par le système et de les utiliser de manière appropriée. Les systèmes d'IA à haut risque devraient donc être accompagnés d'une documentation et d'instructions d'utilisation pertinentes et inclure des informations concises et claires, notamment en ce qui concerne les risques potentiels pour les droits fondamentaux et la discrimination des personnes susceptibles d'être affectées par le système eu égard à sa destination, ainsi qu'il convient. Afin de faciliter la compréhension des instructions d'utilisation par les utilisateurs, celles-ci devraient, au besoin, contenir des exemples.

(48) Les systèmes d'IA à haut risque devraient être conçus et développés de manière à ce que les personnes physiques puissent contrôler leur fonctionnement. À cette fin, des mesures appropriées de contrôle humain devraient être établies par le fournisseur du système avant sa mise sur le marché ou sa mise en service. En particulier, le cas échéant, de telles mesures devraient garantir que le système est soumis à des contraintes opérationnelles intégrées qui ne peuvent pas être ignorées par le système lui-même, que le système répond aux ordres de l'opérateur humain et que les personnes physiques auxquelles le contrôle humain a été confié ont les compétences, la formation et l'autorité nécessaires pour s'acquitter de ce rôle. Compte tenu des conséquences importantes pour les personnes en cas d'erreur dans des correspondances établies par certains systèmes d'identification biométrique, il convient de prévoir pour ces systèmes une obligation de contrôle humain accru, de manière à ce qu'aucune mesure ou décision ne puisse être prise par l'utilisateur sur la base d'une identification obtenue par le système, à moins qu'elle n'ait été vérifiée et confirmée séparément par au moins deux personnes physiques. Ces personnes pourraient provenir d'une ou de plusieurs entités et compter parmi elles la personne faisant fonctionner le système ou l'utilisant. Cette exigence ne devrait pas entraîner de charges ou de retards inutiles et il pourrait suffire que les vérifications effectuées séparément par différentes personnes soient automatiquement enregistrées dans les journaux générés par le système.

(49) Les systèmes d'IA à haut risque devraient produire des résultats d'une qualité constante tout au long de leur cycle de vie et assurer un niveau approprié d'exactitude, de robustesse et de cybersécurité conformément à l'état de la technique généralement reconnu. Le degré d'exactitude et les critères de mesure de l'exactitude devraient être communiqués aux utilisateurs.

(50) La robustesse technique est une exigence essentielle pour les systèmes d'IA à haut risque. Il convient qu'ils soient résilients face aux comportements préjudiciables ou, plus généralement, indésirables pouvant résulter de limites intrinsèques aux systèmes ou dues à l'environnement dans lequel les systèmes fonctionnent (par exemple les erreurs, les défauts, les incohérences, les situations inattendues). Les systèmes d'IA à haut risque devraient donc être conçus et développés avec des solutions techniques appropriées afin de prévenir ou de réduire au minimum ces comportements préjudiciables ou, plus généralement, indésirables, tels que, par exemple, des mécanismes permettant au système d'interrompre son fonctionnement en toute sécurité (mesures de sécurité après défaillance) en présence de certaines anomalies ou en cas de fonctionnement en dehors de certaines limites prédéterminées. L'absence de protection contre ces risques pourrait avoir des incidences sur la sécurité ou entraîner des violations des droits fondamentaux, par exemple en raison de décisions erronées ou de résultats inexacts ou biaisés générés par le système d'IA.

(51) La cybersécurité joue un rôle crucial pour garantir la résilience des systèmes d'IA face aux tentatives de détourner leur utilisation, leur comportement, leurs performances ou de compromettre leurs propriétés de sûreté par des tiers malveillants exploitant les vulnérabilités du système. Les cyberattaques contre les systèmes d'IA peuvent faire usage de ressources spécifiques à l'IA, telles que des jeux de données d'entraînement (par exemple l'empoisonnement de données) ou des modèles entraînés (par exemple les attaques adversaires), ou exploiter les vulnérabilités des ressources numériques du système d'IA ou de l'infrastructure TIC sous-jacente. Pour garantir un niveau de cybersécurité adapté aux risques, des mesures appropriées devraient donc être prises par les fournisseurs de systèmes d'IA à haut risque, en tenant également compte, si nécessaire, de l'infrastructure TIC sous-jacente.

(52) Dans le cadre de la législation d'harmonisation de l'Union, les règles applicables à la mise sur le marché, à la mise en service et à l'utilisation de systèmes d'IA à haut risque devraient être établies conformément au règlement (CE) nº 765/2008 du Parlement européen et du Conseil[22] fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits, à la décision nº 768/2008/CE du Parlement européen et du Conseil[23] relative à un cadre commun pour la commercialisation des produits et au règlement (UE) 2019/1020 du Parlement européen et du Conseil[24] sur la surveillance du marché et la conformité des produits ("nouveau cadre législatif pour la commercialisation des produits").

(52 *bis*) Conformément aux principes du nouveau cadre législatif, des obligations spécifiques pour les opérateurs concernés au sein de la chaîne de valeur de l'IA devraient être fixées pour garantir la sécurité juridique et faciliter le respect du présent règlement. Dans certaines situations, ces opérateurs pourraient jouer plus d'un rôle en même temps et devraient donc cumuler toutes les obligations pertinentes associées à ces rôles. Par exemple, un opérateur pourrait agir à la fois en tant que distributeur et importateur.

(53) Il convient qu'une personne physique ou morale spécifique, définie comme étant le fournisseur, assume la responsabilité de la mise sur le marché ou de la mise en service d'un système d'IA à haut risque, indépendamment du fait que cette personne physique ou morale soit ou non la personne qui a conçu ou développé le système.

---

22 Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

23 Décision nº 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

24 Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) nº 765/2008 et (UE) nº 305/2011 (Texte présentant de l'intérêt pour l'EEE) (JO L 169 du 25.6.2019, p. 1).

(54) Le fournisseur devrait mettre en place un système solide de gestion de la qualité, garantir le respect de la procédure d'évaluation de la conformité requise, rédiger la documentation pertinente et mettre en place un système solide de surveillance après commercialisation. Les autorités publiques qui mettent en service des systèmes d'IA à haut risque destinés à être utilisés exclusivement par elles peuvent adopter et mettre en œuvre les règles relatives au système de gestion de la qualité dans le cadre du système de gestion de la qualité adopté au niveau national ou régional, selon le cas, en tenant compte des spécificités du secteur, ainsi que des compétences et de l'organisation de l'autorité publique en question.

(54 *bis*) Afin de garantir la sécurité juridique, il est nécessaire de préciser que, dans certaines conditions particulières, toute personne physique ou morale devrait être considérée comme un fournisseur d'un nouveau système d'IA à haut risque et, par conséquent, assumer toutes les obligations pertinentes. Par exemple, tel serait le cas si cette personne met son nom ou sa marque sur un système d'IA à haut risque qui a déjà été mis sur le marché ou mis en service, ou si elle modifie la destination d'un système d'IA qui n'est pas à haut risque et qui est déjà mis sur le marché ou mis en service, d'une manière qui rend à haut risque le système d'IA modifié. Ces dispositions devraient s'appliquer sans préjudice de dispositions plus spécifiques établies dans certains actes législatifs sectoriels du nouveau cadre législatif avec lesquels le présent règlement devrait s'appliquer conjointement. Par exemple, l'article 16, paragraphe 2, du règlement (UE) 2017/745, qui dispose que certaines modifications ne devraient pas être considérées comme des modifications d'un dispositif susceptibles d'influer sur sa conformité avec les exigences applicables, devrait continuer de s'appliquer aux systèmes d'IA à haut risque constituant des dispositifs médicaux au sens dudit règlement.

(55) Lorsqu'un système d'IA à haut risque qui est un composant de sécurité d'un produit couvert par un acte législatif sectoriel pertinent du nouveau cadre législatif n'est pas mis sur le marché ou mis en service indépendamment du produit, le fabricant du produit tel que défini par l'acte législatif pertinent du nouveau cadre législatif devrait se conformer aux obligations du fournisseur établies dans le présent règlement et garantir notamment que le système d'IA intégré dans le produit final est conforme aux exigences du présent règlement.

(56) Pour permettre le contrôle de l'application du présent règlement et créer des conditions de concurrence équitables pour les opérateurs, et compte tenu des différentes formes de mise à disposition de produits numériques, il est important de veiller à ce que, en toutes circonstances, une personne établie dans l'Union puisse fournir aux autorités toutes les informations nécessaires sur la conformité d'un système d'IA. Par conséquent, préalablement à la mise à disposition sur le marché de l'Union de leurs systèmes d'IA, et lorsqu'aucun importateur ne peut être identifié, les fournisseurs établis en dehors de l'Union sont tenus de nommer, par mandat écrit, un mandataire établi dans l'Union.

(56 *bis*) Pour les fournisseurs qui ne sont pas établis dans l'Union, le mandataire joue un rôle capital en ce sens qu'il veille à la conformité des systèmes d'IA à haut risque mis sur le marché ou mis en service dans l'Union par ces fournisseurs et sert à ces derniers de point de contact établi ans l'Union. Compte tenu de ce rôle capital, et afin de garantir que la responsabilité est assumée aux fins de l'application du présent règlement, il convient de rendre le mandataire conjointement et solidairement responsable avec le fournisseur de systèmes d'IA à haut risque défectueux. La responsabilité du mandataire prévue par le présent règlement est sans préjudice des dispositions de la directive 85/374/CEE relative à la responsabilité du fait des produits défectueux.

(57) [supprimé]

(58) Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux potentiellement associés à leur utilisation, notamment en ce qui concerne la nécessité d'assurer un suivi adéquat des performances d'un système d'IA dans un contexte réel, il convient de définir des responsabilités spécifiques pour les utilisateurs. Les utilisateurs devraient en particulier être tenus d'utiliser les systèmes d'IA à haut risque conformément à la notice d'utilisation, et certaines autres obligations devraient être prévues en ce qui concerne la surveillance du fonctionnement des systèmes d'IA et la tenue de registres, selon le cas. Ces obligations devraient être sans préjudice d'autres obligations de l'utilisateur en ce qui concerne les systèmes d'IA à haut risque en vertu du droit de l'Union ou du droit national, et ne devraient pas s'appliquer lorsque l'utilisation s'inscrit dans le cadre d'une activité personnelle à caractère non professionnel.

(58 *bis*) Il convient de préciser que le présent règlement n'affecte pas les obligations des fournisseurs et des utilisateurs de systèmes d'IA en leur qualité de responsables du traitement ou de sous-traitants découlant du droit de l'Union relatif à la protection des données à caractère personnel dans la mesure où la conception, le développement ou l'utilisation de systèmes d'IA implique le traitement de données à caractère personnel. Il convient également de préciser que les personnes concernées continuent de jouir de tous les droits et garanties qui leur sont conférés par le droit de l'Union, dont les droits liés à la prise de décision individuelle entièrement automatisée, y compris le profilage. Des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA établies en vertu du présent règlement devraient faciliter la mise en œuvre effective et permettre aux personnes concernées de faire valoir leurs droits et d'autres voie de recours garantis par le droit de l'Union relatif à la protection des données à caractère personnel et d'autres droits fondamentaux.

(59) [supprimé]

(60) [supprimé]

(61) La normalisation devrait jouer un rôle essentiel pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec présent règlement, suivant les technologies les plus récentes. Le respect des normes harmonisées telles que définies dans le règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[25], qui doivent normalement tenir compte des évolutions technologiques les plus récentes, devrait être un moyen pour les fournisseurs de démontrer la conformité aux exigences du présent règlement. Toutefois, en l'absence de références pertinentes à des normes harmonisées, la Commission devrait être en mesure d'établir, au moyen d'actes d'exécution, des spécifications communes pour certaines exigences au titre du présent règlement en tant que solution de repli exceptionnelle pour faciliter l'obligation du fournisseur de se conformer aux exigences du présent règlement, lorsque le processus de normalisation est bloqué ou lorsque l'établissement d'une norme harmonisée appropriée accuse des retards. Si un tel retard est dû à la complexité technique de la norme en question, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes. Une participation appropriée des petites et moyennes entreprises à l'élaboration de normes soutenant la mise en œuvre du présent règlement est essentielle pour promouvoir l'innovation et la compétitivité dans le domaine de l'intelligence artificielle au sein de l'Union. Il convient de veiller à cette participation de manière appropriée, conformément aux articles 5 et 6 du règlement (UE) n° 1025/2012.

[25] Règlement (UE) nº 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision nº 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

(61 *bis*) Il convient que, sans préjudice de l'utilisation de normes harmonisées et de spécifications communes, les fournisseurs bénéficient d'une présomption de conformité aux exigences applicables en matière de données lorsque leur système d'IA à haut risque a été entraîné et testé avec des données tenant compte du contexte géographique, comportemental ou fonctionnel spécifique dans lequel il est destiné à être utilisé. De même, conformément à l'article 54, paragraphe 3, du règlement (UE) 2019/881 du Parlement européen et du Conseil, 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 en vertu dudit règlement et dont les références ont été publiées au Journal officiel de l'Union européenne devraient être présumés conformes aux exigences de cybersécurité du présent règlement. Cet aspect demeure sans préjudice du caractère volontaire dudit schéma de cybersécurité.

(62) Afin de garantir un niveau élevé de fiabilité des systèmes d'IA à haut risque, ces systèmes devraient être soumis à une évaluation de la conformité avant leur mise sur le marché ou leur mise en service.

(63) Afin de réduire au minimum la charge pesant sur les opérateurs et d'éviter les éventuels doubles emplois, la conformité avec les exigences du présent règlement des systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation existante de l'Union relevant du nouveau cadre législatif devrait être évaluée dans le cadre de l'évaluation de la conformité déjà prévue en vertu de cette législation. L'applicabilité des exigences du présent règlement ne devrait donc pas avoir d'incidence sur la logique, la méthode ou la structure générale propres à l'évaluation de la conformité au titre des actes législatifs spécifiques pertinents relevant du nouveau cadre législatif. Cette approche se reflète parfaitement dans l'interaction entre le présent règlement et le [règlement relatif aux machines et équipements]. Les exigences du présent règlement traitent des risques pour la sécurité posés par les systèmes d'IA assurant les fonctions de sécurité des machines, tandis que certaines exigences spécifiques du [règlement relatif aux machines et équipements] garantiront l'intégration sûre du système d'IA dans la machine de façon à ne pas compromettre la sécurité de la machine dans son ensemble. Le [règlement relatif aux machines et équipements] applique la même définition pour le système d'IA que le présent règlement. En ce qui concerne les systèmes d'IA à haut risque liés aux produits couverts par les règlements (UE) 2017/745 et 2017/746 relatifs aux dispositifs médicaux, l'applicabilité des exigences du présent règlement devrait être sans préjudice et tenir compte de la logique de gestion des risques et de la détermination du rapport bénéfice/risque effectuée au titre du cadre relatif aux dispositifs médicaux.

(64) Étant donné l'expérience plus étendue des organismes professionnels de certification avant mise sur le marché dans le domaine de la sécurité des produits et de la nature différente des risques encourus, il convient de limiter, au moins dans une phase initiale d'application du présent règlement, le champ d'application des évaluations de la conformité réalisées par un tiers aux systèmes d'IA à haut risque autres que ceux liés à des produits. Par conséquent, l'évaluation de la conformité de ces systèmes devrait en règle générale être réalisée par le fournisseur sous sa propre responsabilité, à la seule exception des systèmes d'IA destinés à être utilisés pour l'identification biométrique à distance de personnes, pour lesquels l'intervention d'un organisme notifié dans l'évaluation de la conformité devrait être prévue, pour autant qu'ils ne soient pas interdits.

(65) Afin de procéder à une évaluation de la conformité par un tiers des systèmes d'IA destinés à être utilisés pour l'identification biométrique à distance de personnes, les organismes notifiés devraient être notifiés en vertu du présent règlement par les autorités nationales compétentes, sous réserve qu'ils soient conformes à un ensemble d'exigences portant notamment sur leur indépendance, leur compétence et l'absence de conflits d'intérêts. La notification de ces organismes devrait être envoyée par les autorités nationales compétentes à la Commission et aux autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission, conformément à l'article R23 de la décision n° 768/2008/CE.

(66) Conformément à la notion communément établie de modification substantielle pour les produits réglementés par la législation d'harmonisation de l'Union, il convient que chaque fois que survient une modification susceptible d'avoir une incidence sur la conformité d'un système d'IA à haut risque avec le présent règlement (par exemple, un changement de système d'exploitation ou d'architecture logicielle) ou que la destination du système change, il convient de considérer ledit système d'IA comme un nouveau système d'IA devant être soumis à nouvelle procédure d'évaluation de la conformité. Cependant, les changements intervenant sur l'algorithme et les performances de systèmes d'IA qui continuent à "apprendre" après avoir été mis sur le marché ou mis en service (qui donc, en d'autres mots, adaptent automatiquement la façon dont les fonctions sont exécutées) ne devraient pas constituer une modification substantielle, à condition que ces changements aient été prédéterminés par le fournisseur et évalués au moment de l'évaluation de la conformité.

(67) Le marquage "CE" devrait être apposé sur les systèmes d'IA à haut risque pour indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement dans le marché intérieur. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché ou à la mise en service de systèmes d'IA à haut risque qui satisfont aux exigences fixées dans le présent règlement et portent le marquage "CE".

(68) Dans certaines conditions, la disponibilité rapide de technologies innovantes peut être cruciale pour la santé et la sécurité des personnes et pour la société dans son ensemble. Il convient donc que, pour des motifs exceptionnels liés à la sécurité publique, à la protection de la vie et de la santé des personnes physiques et à la protection de la propriété industrielle et commerciale, les États membres puissent autoriser la mise sur le marché ou la mise en service de systèmes d'IA qui n'ont pas fait l'objet d'une évaluation de la conformité.

(69) Afin de faciliter les travaux de la Commission et des États membres dans le domaine de l'intelligence artificielle et d'accroître la transparence à l'égard du public, les fournisseurs de systèmes d'IA à haut risque autres que ceux liés à des produits relevant du champ d'application de la législation d'harmonisation existante de l'Union en la matière devraient être tenus de s'enregistrer elles-mêmes et d'enregistrer les informations relatives à leur système d'IA à haut risque dans une base de données de l'UE, qui sera établie et gérée par la Commission. Avant d'utiliser un système d'IA à haut risque inscrit à l'annexe III, les utilisateurs de systèmes d'IA à haut risque qui sont des autorités, agences ou organismes publics, à l'exception des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile, et les autorités qui sont utilisatrices de systèmes d'IA à haut risque dans le domaine des infrastructures critiques s'enregistrent également dans cette base de données et sélectionnent le système qu'ils envisagent d'utiliser. La Commission devrait faire fonction de responsable du traitement pour cette base de données, conformément au règlement (UE) 2018/1725 du Parlement européen et du Conseil[26]. Afin de garantir que la base de données soit pleinement opérationnelle une fois déployée, la procédure de création de la base de données devrait prévoir l'élaboration de spécifications fonctionnelles par la Commission et d'un rapport d'audit indépendant.

[26] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

(70) Certains systèmes d'IA destinés à interagir avec des personnes physiques ou à générer du contenu peuvent présenter des risques spécifiques d'usurpation d'identité ou de tromperie, qu'ils soient ou non considérés comme étant à haut risque. Dans certaines circonstances, l'utilisation de ces systèmes devrait donc être soumise à des obligations de transparence spécifiques sans préjudice des exigences et obligations relatives aux systèmes d'IA à haut risque. En particulier, les personnes physiques devraient être avisées 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. Lors de la mise en œuvre de cette obligation, les caractéristiques des personnes appartenant à des groupes vulnérables en raison de leur âge ou d'un handicap devraient être prises en compte dans la mesure où le système d'IA est destiné à interagir également avec ces groupes. En outre, les personnes physiques devraient être mises au courant lorsqu'elles sont exposées à des systèmes qui, en traitant leurs données biométriques, peuvent identifier ou déduire les émotions ou intentions de ces personnes ou les affecter à des catégories spécifiques. Ces catégories spécifiques peuvent avoir trait à des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits personnels, l'origine ethnique, les préférences et les intérêts personnels ou d'autres aspects tels que l'orientation sexuelle ou politique. Ces informations devraient être fournies dans des formats accessibles aux personnes handicapées. En outre, les utilisateurs qui se servent d'un système d'IA pour générer ou manipuler des images ou des contenus audio ou vidéo dont la ressemblance avec des personnes, des lieux ou des événements existants pourrait porter à croire qu'il s'agit de documents authentiques, devraient déclarer que le contenu a été créé ou manipulé artificiellement en étiquetant le résultat produit par le système d'intelligence artificielle en conséquence et en mentionnant son origine artificielle. Le respect des obligations d'information susmentionnées ne devrait pas être interprété comme indiquant que l'utilisation du système ou des résultats qu'il génère est licite en vertu du présent règlement ou d'autres législations de l'Union et des États membres et devrait être sans préjudice d'autres obligations de transparence pour les utilisateurs de systèmes d'IA prévues par le droit de l'Union ou le droit national. En outre, il ne devrait pas non plus être interprété comme indiquant que l'utilisation du système ou des résultats qu'il génère entrave le droit à la liberté d'expression et au droit à la liberté des arts et des sciences garantis par la charte des droits fondamentaux de l'UE, en particulier lorsque le contenu fait partie d'un travail ou d'un programme manifestement créatif, satirique, artistique ou de fiction, sous réserve de garanties appropriées pour les droits et libertés de tiers.

(71) L'intelligence artificielle est une famille de technologies en évolution rapide qui nécessite la mise en place de nouvelles formes de contrôle réglementaire et d'un espace sûr pour l'expérimentation, garantissant également une innovation responsable et l'intégration de garanties et de mesures d'atténuation des risques appropriées. Pour garantir un cadre juridique propice à l'innovation, à l'épreuve du temps et résilient face aux perturbations, les autorités nationales compétentes d'un ou de plusieurs États membres devraient être encouragées à mettre en place des bacs à sable réglementaires sur l'intelligence artificielle pour faciliter le développement et la mise à l'essai de systèmes d'IA innovants sous un contrôle réglementaire strict avant que ces systèmes ne soient mis sur le marché ou mis en service d'une autre manière.

(72) Les bacs à sable réglementaires de l'IA devraient avoir pour objectif de favoriser l'innovation dans le domaine de l'IA en créant un environnement contrôlé d'expérimentation et d'essai au stade du développement et de la pré-commercialisation afin de garantir la conformité des systèmes d'IA innovants avec le présent règlement et d'autres législations pertinentes de l'Union et des États membres; de renforcer la sécurité juridique pour les innovateurs ainsi que le contrôle et la compréhension, par les autorités compétentes, des possibilités, des risques émergents et des conséquences de l'utilisation de l'IA; et d'accélérer l'accès aux marchés, notamment en supprimant les obstacles pour les petites et moyennes entreprises (PME), notamment des jeunes entreprises. La participation au bac à sable réglementaire de l'IA devrait se concentrer sur les questions qui créent une insécurité juridique pour les fournisseurs et les fournisseurs potentiels avant d'innover, d'expérimenter l'IA dans l'Union et de contribuer à un apprentissage réglementaire fondé sur des données probantes. La surveillance des systèmes d'IA dans le bac à sable réglementaire de l'IA devrait donc porter sur leur développement, leur entraînement, leur mise à l'essai et leur validation avant que les systèmes ne soient mis sur le marché ou mis en service, ainsi que sur la notion et la survenance de modifications substantielles susceptibles de nécessiter une nouvelle procédure d'évaluation de la conformité. Au besoin, les autorités nationales compétentes mettant en place des bacs à sable réglementaires de l'IA devraient coopérer avec d'autres autorités concernées, y compris celles qui supervisent la protection des droits fondamentaux, et pourraient permettre la participation d'autres acteurs de l'écosystème de l'IA, tels que les organisations nationales ou européennes de normalisation, les organismes notifiés, les installations d'essai et d'expérimentation, les laboratoires de recherche et d'expérimentation, les pôles d'innovation, et les parties prenantes et les organisations de la société civile concernés. Pour assurer une mise en œuvre uniforme dans toute l'Union et des économies d'échelle, il convient d'établir des règles communes pour la mise en place des bacs à sable réglementaires ainsi qu'un cadre de coopération entre les autorités compétentes intervenant dans la surveillance des bacs à sable. Les bacs à sable réglementaires de l'IA établis en vertu du présent règlement devraient être sans préjudice d'autres actes législatifs autorisant la création d'autres bacs à sable en vue de garantir le respect de dispositions législatives autres que le présent règlement. Le cas échéant, les autorités compétentes concernées chargées de ces autres bacs à sable réglementaires devraient prendre en considération les avantages de l'utilisation de ces bacs à sable également aux fins d'assurer la conformité des systèmes d'IA avec le présent règlement. Sous réserve d'un accord entre les autorités nationales compétentes et les participants au bac à sable réglementaire de l'IA, il peut également être procédé à des essais en conditions réelles supervisés dans le cadre du bac à sable réglementaire de l'IA.

(-72 *bis*) Le présent règlement devrait constituer la base juridique pour l'utilisation, par les participants au bacs à sable réglementaires de l'IA, des données à caractère personnel collectées à d'autres fins pour le développement de certains systèmes d'IA d'intérêt public dans le cadre du bac à sable réglementaire de l'IA, conformément à l'article 6, paragraphe 4, et à l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et aux articles 5 et 10 du règlement (UE) 2018/1725, et sans préjudice de l'article 4, paragraphe 2, et de l'article 10 de la directive (UE) 2016/680. Toutes les autres obligations des responsables du traitement et tous les autres droits des personnes concernées en vertu du règlement (UE) 2016/679, du règlement (UE) 2018/1725 et de la directive (UE) 2016/680 restent applicables. En particulier, le présent règlement ne devrait pas constituer une base juridique au sens de l'article 22, paragraphe 2, point b), du règlement (UE) 2016/679 et de l'article 24, paragraphe 2, point b), du règlement (UE) 2018/1725. Les participants au bac à sable réglementaire devraient fournir des garanties appropriées et coopérer avec les autorités compétentes, notamment en suivant leurs orientations et en agissant rapidement et de bonne foi pour atténuer tout risque important pour la sécurité et les droits fondamentaux susceptible de survenir au cours du développement et de l'expérimentation dans le bac à sable. La conduite des participants dans le cadre du bac à sable réglementaire devrait être prise en considération lorsque les autorités compétentes décident d'infliger ou non une amende administrative au titre de l'article 83, paragraphe 2, du règlement (UE) 2016/679 et de l'article 57 de la directive (UE) 2016/680.

(72 *bis*) Afin d'accélérer le processus de développement et de mise sur le marché des systèmes d'IA à haut risque inscrits sur la liste figurant à l'annexe III, il importe que les fournisseurs ou fournisseurs potentiels de ces systèmes puissent également bénéficier d'un régime particulier pour soumettre ces systèmes à des essais en conditions réelles, sans participer à un bac à sable réglementaire de l'IA. Toutefois, dans de tels cas et compte tenu des conséquences possibles de ces essais sur des personnes physiques, il convient de veiller à ce que le règlement introduise des garanties et des conditions appropriées et suffisantes pour les fournisseurs ou fournisseurs potentiels. Ces garanties devraient comprendre, notamment, une demande de consentement éclairé de la part des personnes physiques pour participer à des essais en conditions réelles, sauf en ce qui concerne les services répressifs dans les cas où la recherche d'un consentement éclairé empêcherait que le système d'IA ne soit essayé. Le consentement des personnes concernées à participer à ces essais au titre du présent règlement est distinct et sans préjudice du consentement des personnes concernées au traitement de leurs données à caractère personnel en vertu de la législation applicable en matière de protection des données.

(73) Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des PME fournisseuses ou utilisatrices de systèmes d'IA bénéficient d'une attention particulière. Pour atteindre cet objectif, les États membres devraient prendre des initiatives à l'intention de ces opérateurs, notamment en matière de sensibilisation et de communication d'informations. En outre, les intérêts et les besoins spécifiques des PME fournisseuses doivent être pris en considération lorsque les organismes notifiés fixent les redevances d'évaluation de la conformité. Les frais de traduction liés à la documentation obligatoire et à la communication avec les autorités peuvent constituer un coût important pour les fournisseurs et d'autres opérateurs, en particulier pour ceux de plus petite envergure. Les États membres devraient éventuellement veiller à ce qu'une des langues qu'ils choisissent et acceptent pour la documentation pertinente des fournisseurs et pour la communication avec les opérateurs soit une langue comprise par le plus grand nombre possible d'utilisateurs transfrontières.

(73 *bis*) Afin de promouvoir et de protéger l'innovation, la plateforme d'IA à la demande, tous les programmes et projets de financement pertinents de l'UE, tels que le programme pour une Europe numérique et Horizon Europe, mis en œuvre par la Commission et les États membres au niveau national ou de l'UE devraient contribuer à la réalisation des objectifs du présent règlement.

(74) En particulier, afin de réduire au minimum les risques pour la mise en œuvre résultant du manque de connaissances et d'expertise sur le marché, ainsi que de faciliter la mise en conformité des fournisseurs, notamment des PME, et des organismes notifiés avec les obligations qui leur incombent au titre du présent règlement, la plateforme d'IA à la demande, les pôles européens d'innovation numérique et les installations d'expérimentation et d'essai mis en place par la Commission et les États membres au niveau national ou de l'UE devraient éventuellement contribuer à la mise en œuvre du présent règlement. Dans le cadre de leurs missions et domaines de compétence respectifs, ils peuvent notamment apporter un soutien technique et scientifique aux fournisseurs et aux organismes notifiés.

(74 *bis*) En outre, afin de veiller au principe de proportionnalité compte tenu de la très petite taille de certains opérateurs au regard des coûts de l'innovation, il convient d'exempter les microentreprises des obligations les plus coûteuses telles que, par exemple, celle de mettre en place un système de gestion de la qualité, de manière à réduire la charge administrative et les coûts pour ces entreprises sans affecter le niveau de protection et la nécessité de se conformer aux exigences applicables aux systèmes d'IA à haut risque.

(75) Il convient que la Commission facilite, dans la mesure du possible, l'accès aux installations d'expérimentation et d'essai pour les organismes, groupes ou laboratoires qui ont été créés ou accrédités en vertu d'une législation d'harmonisation de l'Union pertinente et qui accomplissent des tâches dans le cadre de l'évaluation de la conformité des produits ou dispositifs couverts par la législation d'harmonisation de l'Union en question. C'est notamment le cas des groupes d'experts, des laboratoires spécialisés et des laboratoires de référence dans le domaine des dispositifs médicaux conformément au règlement (UE) 2017/745 et au règlement (UE) 2017/746.

(76) Afin de faciliter une mise en œuvre aisée, efficace et harmonisée du présent règlement, il convient de créer un Comité européen de l'intelligence artificielle. Ce comité devrait tenir compte des différents intérêts de l'écosystème de l'IA et être composé de représentants des États membres. Afin de garantir la participation des parties prenantes concernées, il convient de créer un sous-groupe permanent du Comité. Le Comité devrait être chargé d'un certain nombre de tâches consultatives, parmi lesquelles la formulation d'avis, de recommandations, de conseils ou la contribution à des orientations sur des questions liées à la mise en œuvre du présent règlement, y compris sur les questions relatives à l'exécution, les spécifications techniques ou les normes existantes concernant les exigences établies dans le présent règlement, et la fourniture de conseils à la Commission et aux États membres ainsi qu'à leurs autorités nationales compétentes sur des questions spécifiques liées à l'intelligence artificielle. Afin d'offrir une certaine souplesse aux États membres dans la désignation de leurs représentants au sein du Comité de l'IA, ces représentants peuvent être toute personne appartenant à des entités publiques qui devraient avoir les compétences et les pouvoirs nécessaires pour faciliter la coordination au niveau national et contribuer à l'accomplissement des tâches du comité. Le Comité devrait établir 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 sur des questions liées respectivement à la surveillance du marché et aux organismes notifiés. 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. Conformément aux rôles et missions de la Commission en vertu de l'article 33 du règlement (UE) 2019/1020, la Commission devrait apporter son soutien aux activités du sous-groupe permanent en procédant à des évaluations ou à des études du marché, notamment en vue de recenser les aspects du présent règlement appelant une coordination particulière urgente entre les autorités de surveillance du marché. Le Comité peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le Comité devrait également coopérer, le cas échéant, avec les organes, groupes d'experts et réseaux compétents de l'UE actifs dans le contexte de dispositions législatives pertinentes de l'UE, notamment ceux qui agissent au titre de la réglementation applicable de l'UE en matière de données, et de produits et services numériques.

(76 *bis*) La Commission devrait apporter un soutien actif aux États membres et aux opérateurs dans la mise en œuvre et l'application du présent règlement. À cet égard, elle devrait élaborer des lignes directrices sur des sujets particuliers dans l'objectif de faciliter l'application du présent règlement, tout en accordant une attention particulière aux besoins des PME et des jeunes entreprises dans les secteurs les plus susceptibles d'être touchés. En soutien à une application adéquate et aux capacités des États membres, il convient que des installations d'essai de l'Union dans le domaine de l'IA ainsi qu'une réserve d'experts pertinents soient mises en place et à la disposition des États membres.

(77) Les États membres jouent un rôle clé dans l'application et le contrôle du respect du présent règlement. À cet égard, chaque État membre devrait désigner une ou plusieurs autorités nationales compétentes chargées de contrôler l'application et la mise en œuvre du présent règlement. Les États membres peuvent décider de désigner une entité publique, quel qu'en soit le type, qui soit chargée d'exécuter les tâches des autorités nationales compétentes au sens du présent règlement, en fonction de leurs caractéristiques et besoins organisationnels nationaux spécifiques.

(78) Afin de garantir que les fournisseurs de systèmes d'IA à haut risque puissent prendre en considération l'expérience acquise dans l'utilisation de systèmes d'IA à haut risque pour améliorer leurs systèmes et le processus de conception et de développement, ou qu'ils puissent prendre d'éventuelles mesures correctives en temps utile, tous les fournisseurs devraient avoir mis en place un système de surveillance après commercialisation. Ce système est aussi essentiel pour garantir que les risques potentiels découlant des systèmes d'IA qui continuent à "apprendre" après avoir été mis sur le marché ou mis en service puissent être traités plus efficacement et en temps utile. Dans ce contexte, les fournisseurs devraient également être tenus de mettre en place un système pour signaler aux autorités compétentes tout incident grave résultant de l'utilisation de leurs systèmes d'IA.

(79) Afin de garantir un contrôle approprié et efficace du respect des exigences et obligations énoncées par le présent règlement, qui fait partie de la législation d'harmonisation de l'Union, le système de surveillance du marché et de mise en conformité des produits établi par le règlement (UE) 2019/1020 devrait s'appliquer dans son intégralité. Les autorités de surveillance du marché désignées en vertu du présent règlement devraient disposer de tous les pouvoirs d'exécution prévus par le présent règlement et le règlement (UE) 2019/1020, et elles devraient exercer leurs pouvoirs et s'acquitter de leurs tâches de manière indépendante, impartiale et sans parti pris. Bien que la majorité des systèmes d'IA ne fassent pas l'objet d'exigences et obligations particulières au titre du présent règlement, les autorités de surveillance du marché peuvent prendre des mesures à l'égard de tous les systèmes d'IA lorsqu'ils présentent un risque conformément au présent règlement. En raison de la nature spécifique des institutions, agences et organes de l'Union relevant du champ d'application du présent règlement, il convient de désigner le Contrôleur européen de la protection des données comme autorité compétente pour la surveillance du marché en ce qui les concerne. Cela devrait être sans préjudice de la désignation des autorités nationales compétentes par les États membres. Les activités de surveillance du marché ne devraient pas affecter la capacité des entités surveillées à s'acquitter de leurs tâches de manière indépendante, lorsque cette indépendance constitue une exigence du droit de l'Union.

(79 *bis*) Le présent règlement est sans préjudice des compétences, des tâches, des pouvoirs et de l'indépendance des autorités ou organismes publics nationaux compétents qui contrôlent l'application du droit de l'Union en matière de protection des droits fondamentaux, y compris les organismes chargés des questions d'égalité et les autorités de protection des données. Lorsque leur mandat l'exige, ces autorités ou organismes publics nationaux devraient également avoir accès à toute documentation créée en vertu du présent règlement. Une procédure de sauvegarde spécifique devrait être mise en place pour garantir une application adéquate et en temps utile opposable aux systèmes d'IA présentant un risque pour la santé, la sécurité et les droits fondamentaux. La procédure applicable à ces systèmes d'IA présentant un risque devrait être appliquée aux systèmes d'IA à haut risque présentant un risque, aux systèmes interdits qui ont été mis sur le marché, mis en service ou utilisés en violation des interdictions concernant des pratiques définies par le présent règlement, et aux systèmes d'IA qui ont été mis à disposition en violation des exigences de transparence énoncées dans le présent règlement et qui présentent un risque.

(80) La législation de l'Union sur les services financiers comprend des règles et des exigences en matière de gouvernance interne et de gestion des risques qui sont applicables aux établissements financiers réglementés dans le cadre de la fourniture de ces services, y compris lorsqu'ils font usage de systèmes d'IA. Afin d'assurer l'application et la mise en œuvre cohérentes des obligations découlant du présent règlement et des règles et exigences pertinentes de la législation de l'Union sur les services financiers, les autorités chargées de la surveillance et du contrôle de l'application de la législation sur les services financiers devraient être désignées comme les autorités compétentes aux fins de la surveillance de la mise en œuvre du présent règlement, y compris pour les activités de surveillance du marché, en ce qui concerne les systèmes d'IA fournis ou utilisés par des établissements financiers réglementés et surveillés, à moins que les États membres ne décident de désigner une autre autorité pour remplir ces tâches de surveillance du marché. Ces autorités compétentes devraient disposer, en vertu du présent règlement et du règlement (UE) 2019/1020 en matière de surveillance du marché, de tous les pouvoirs nécessaires pour faire respecter les exigences et obligations du présent règlement, y compris le pouvoir d'effectuer des activités de surveillance du marché ex post qui peuvent être intégrées, le cas échéant, dans leurs mécanismes et procédures de surveillance existants au titre de la législation pertinente de l'Union sur les services financiers. Il convient d'envisager que lorsqu'elles agissent en tant qu'autorités de surveillance du marché au titre du présent règlement, les autorités nationales responsables de la surveillance des établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique (MSU) institué par le règlement (UE) n° 1024/2013 du Conseil, doivent communiquer sans délai à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt pour les missions de surveillance prudentielle de la Banque centrale européenne telles qu'elles sont définies dans ledit règlement. Pour renforcer encore la cohérence entre le présent règlement et les règles applicables aux établissements de crédit régis par la directive 2013/36/UE du Parlement européen et du Conseil[27], il convient aussi d'intégrer certaines des obligations procédurales des fournisseurs en ce qui concerne la gestion des risques, la surveillance après commercialisation et la documentation dans les obligations et procédures existantes au titre de la directive 2013/36/UE. Afin d'éviter les chevauchements, des dérogations limitées devraient aussi être envisagées en ce qui concerne le système de gestion de la qualité des fournisseurs et l'obligation de suivi imposée aux utilisateurs de systèmes d'IA à haut risque dans la mesure où les dispositions y afférentes s'appliquent aux établissements de crédit régis par la directive 2013/36/UE. Le même régime devrait s'appliquer aux entreprises d'assurance et de réassurance et aux sociétés holding d'assurance relevant de la

[27] Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE (JO L 176 du 27.6.2013, p. 338).

directive 2009/138/UE (solvabilité II) et aux intermédiaires d'assurance relevant de la directive (UE) 2016/97, ainsi qu'aux autres types d'établissements financiers soumis à des exigences en matière de gouvernance, de dispositifs ou de processus internes établis en vertu de la législation pertinente de l'Union sur les services financiers afin de garantir la cohérence et l'égalité de traitement dans le secteur financier.

(81) Le développement de systèmes d'IA autres que les systèmes d'IA à haut risque dans le respect des exigences du présent règlement peut conduire à une plus large adoption d'une intelligence artificielle digne de confiance dans l'Union. Les fournisseurs de systèmes d'IA qui ne sont pas à haut risque devraient être encouragés à créer des codes de conduite destinés à favoriser l'application volontaire des exigences applicables aux systèmes d'IA à haut risque, adaptés en fonction de la destination des systèmes et des faibles risques encourus. Les fournisseurs devraient aussi être encouragés à appliquer sur une base volontaire des exigences supplémentaires liées, par exemple, à la durabilité environnementale, à l'accessibilité pour les personnes handicapées, à la participation des parties prenantes à la conception et au développement des systèmes d'IA et à la diversité des équipes de développement. La Commission peut élaborer des initiatives, y compris de nature sectorielle, pour faciliter la suppression des obstacles techniques entravant l'échange transfrontière de données pour le développement de l'IA, notamment en ce qui concerne l'infrastructure d'accès aux données et l'interopérabilité sémantique et technique des différents types de données.

(82) Il est important que les systèmes d'IA liés à des produits qui ne sont pas à haut risque au titre du présent règlement et qui ne sont donc pas tenus d'être conformes aux exigences y afférentes soient néanmoins sûrs lorsqu'ils sont mis sur le marché ou mis en service. Pour contribuer à cet objectif, l'application de la directive 2001/95/CE du Parlement européen et du Conseil[28] constituerait un filet de sécurité.

(83) Afin d'assurer une coopération constructive et en toute confiance entre les autorités compétentes au niveau de l'Union et au niveau national, toutes les parties intervenant dans l'application du présent règlement devraient respecter la confidentialité des informations et des données obtenues dans le cadre de l'exécution de leurs tâches, conformément au droit de l'Union et au droit national.

[28] Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits (JO L 11 du 15.1.2002, p. 4).

(84) Les États membres devraient prendre toutes les mesures nécessaires pour que les dispositions du présent règlement soient mises en œuvre et, notamment, prévoir des sanctions effectives, proportionnées et dissuasives en cas de violation de ces dispositions, et dans le respect du principe *non bis in idem*. Pour certaines infractions spécifiques, les États membres devraient tenir compte des marges et des critères définis dans le présent règlement. Le Contrôleur européen de la protection des données devrait avoir le pouvoir d'infliger des amendes aux institutions, agences et organes de l'Union relevant du présent règlement.

(85) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, le pouvoir d'adopter des actes conformément à l'article 290 du TFUE devrait être délégué à la Commission pour lui permettre de modifier les actes législatifs d'harmonisation de l'Union énumérés à l'annexe II, les systèmes d'IA à haut risque énumérés à l'annexe III, les dispositions relatives à la documentation technique énumérées à l'annexe IV, le contenu de la déclaration "UE" de conformité à l'annexe V, les dispositions relatives aux procédures d'évaluation de la conformité des annexes VI et VII et les dispositions établissant les systèmes d'IA à haut risque auxquels devrait s'appliquer la procédure d'évaluation de la conformité fondée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer"[29]. En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués. Ces consultations et ce soutien consultatif devraient également être menés dans le cadre des activités du Comité de l'IA et de ses sous-groupes.

[29] JO L 123 du 12.5.2016, p. 1.

(86) Afin de garantir des conditions uniformes de mise en œuvre du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) nº 182/2011 du Parlement européen et du Conseil[30]. Il importe particulièrement que, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer", si des connaissances plus vastes sont requises à un stade précoce de la préparation de projets d'actes d'exécution, la Commission fasse appel à des groupes d'experts, consulte certaines parties intéressées ou mène des consultations publiques, selon le cas. Ces consultations et ce soutien consultatif devraient également être menés dans le cadre des activités du Comité de l'IA et de ses sous-groupes, y compris l'élaboration des actes d'exécution en ce qui concerne les articles 4, 4 *ter* et 6.

(87) Étant donné que l'objectif du présent règlement ne peut pas être atteint de manière suffisante par les États membres, mais peut, en raison des dimensions et des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du TUE. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(87 *bis*) Afin d'assurer la sécurité juridique, de veiller à ce que les opérateurs disposent d'une période d'adaptation appropriée et d'éviter toute perturbation du marché, y compris en assurant la continuité de l'utilisation des systèmes d'IA, il convient que le présent règlement s'applique aux systèmes d'IA à haut risque qui ont été mis sur le marché ou mis en service avant la date générale d'application de celui-ci, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leur conception ou de leur destination. Il convient de préciser qu'à cet égard, la notion d'importante modification devrait être comprise comme équivalente sur le fond à celle de modification substantielle, qui est utilisée uniquement en ce qui concerne les systèmes d'IA à haut risque tels que définis dans le présent règlement.

[30] Règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

(88) Le présent règlement devrait s'appliquer à compter du ... [*OP – veuillez insérer la date fixée à l'article 85*]. Toutefois, l'infrastructure liée à la gouvernance et au système d'évaluation de la conformité devrait être opérationnelle avant cette date, et les dispositions relatives aux organismes notifiés et à la structure de gouvernance devraient donc s'appliquer à compter du ... [*OP – veuillez insérer la date – trois mois après l'entrée en vigueur du présent règlement*]. En outre, les États membres devraient définir et notifier à la Commission les règles relatives aux sanctions, y compris les amendes administratives, et veiller à ce qu'elles soient correctement et efficacement mises en œuvre à la date d'application du présent règlement. Par conséquent, les dispositions relatives aux sanctions devraient s'appliquer à compter du ... [*OP – veuillez insérer la date – douze mois après l'entrée en vigueur du présent règlement*].

(89) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725 et ont rendu un avis le [...],

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

TITRE I

DISPOSITIONS GÉNÉRALES

Article premier Objet

Le présent règlement établit:

a) des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle (ci-après dénommés "systèmes d'IA") dans l'Union;

a) l'interdiction de certaines pratiques en matière d'intelligence artificielle;

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

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

d) des règles relatives au suivi du marché, à la surveillance du marché et à la gouvernance;

e) des mesures de soutien à l'innovation.

Article 2 Champ d'application

1. Le présent règlement s'applique:

a) aux fournisseurs physiquement présents ou établis dans l'Union ou dans un pays tiers, qui mettent sur le marché ou mettent en service des systèmes d'IA dans l'Union;

b) aux utilisateurs de systèmes d'IA qui sont physiquement présents ou établis dans l'Union;

c) aux fournisseurs et aux utilisateurs de systèmes d'IA physiquement présents ou établis dans un pays tiers, lorsque les résultats générés par le système sont utilisés 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 représentants autorisés des fournisseurs qui sont établis dans l'Union.

2. En ce qui concerne les systèmes d'IA classés à haut risque conformément à l'article 6, paragraphe 1, et à l'article 6, paragraphe 2, qui sont liés aux produits couverts par les actes législatifs d'harmonisation de l'Union énumérés à l'annexe II, section B, seul l'article 84 du présent règlement s'applique. L'article 53 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 lesdits actes législatifs d'harmonisation de l'Union.

3. 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 aux fins d'activités qui ne relèvent pas du champ d'application du droit de l'Union et, en tout état de cause, d'activités ayant trait aux forces armées, à la défense ou à la sécurité nationale, quel que soit le type d'entité exerçant ces activités.

   En outre, 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 résultats générés sont utilisés dans l'Union aux fins d'activités ne relevant pas du champ d'application du droit de l'Union et, en tout état de cause, d'activités ayant trait aux forces armées, à la défense ou à la sécurité nationale, quel que soit le type d'entité exerçant ces activités.

4. Le présent règlement ne s'applique pas 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 d'accords internationaux de coopération des services répressifs et judiciaires avec l'Union ou avec un ou plusieurs États membres.

5. Le présent règlement n'affecte pas l'application des dispositions relatives à la responsabilité des prestataires intermédiaires énoncées au chapitre II, section 4, de la directive 2000/31/CE du Parlement européen et du Conseil[31] [qui doivent être remplacées par les dispositions correspondantes de la législation sur les services numériques].

6. Le présent règlement ne s'applique pas aux systèmes d'IA spécifiquement développés et mis en service uniquement à des fins de recherche et développement scientifiques, ni aux résultats qu'ils génèrent.

7. Le présent règlement ne s'applique pas aux activités de recherche et de développement concernant les systèmes d'IA.

8. Le présent règlement ne s'applique pas aux obligations incombant aux utilisateurs qui sont des personnes physiques utilisant des systèmes d'IA dans le cadre d'une activité strictement personnelle à caractère non professionnel, sauf pour ce qui est de l'article 52.

---

[31] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ("directive sur le commerce électronique") (JO L 178 du 17.7.2000, p. 1).

Article 3 Définitions

Aux fins du présent règlement, on entend par:

(1) "système d'intelligence artificielle" (système d'IA), un système qui est conçu pour fonctionner avec des éléments d'autonomie et qui, sur la base des données et des entrées générées par la machine et/ou par l'homme, déduit la manière d'atteindre un ensemble donné d'objectifs en faisant appel à l'apprentissage automatique et/ou à des approches axées sur la logique et les connaissances, et produit des résultats générés par le système sous la forme de contenu (systèmes d'IA générative), ainsi que de prédictions, de recommandations ou de décisions qui influencent l'environnement avec lequel le système interagit;

(1 *bis*) "cycle de vie d'un système d'IA", la durée de fonctionnement d'un système d'IA, depuis sa conception jusqu'à son retrait. Sans préjudice des compétences des autorités de surveillance du marché, ce retrait peut intervenir à tout moment au cours de la phase de surveillance après commercialisation sur décision du fournisseur et implique que le système ne peut plus être utilisé. Le cycle de vie d'un système d'IA prend également fin lorsqu'une modification substantielle est apportée au système d'IA par le fournisseur ou toute autre personne physique ou morale, auquel cas le système d'IA substantiellement modifié est considéré comme un nouveau système d'IA.

(1 *ter*) "système d'IA à usage général", un système d'IA qui, indépendamment de la manière dont il est mis sur le marché ou mis en service, y compris sous la forme d'un logiciel libre, dont son fournisseur prévoit qu'il exécute des fonctions de portée générale telles que la reconnaissance d'images ou de la parole, la génération de contenus audio ou vidéo, la détection de modèles, le traitement de requêtes, la traduction, etc.; un système d'IA à usage général peut être utilisé dans une pluralité de contextes et peut être intégré dans une pluralité d'autres systèmes d'IA;

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

(3) [supprimé];

(3 *bis*) "petites et moyennes entreprises" (PME), les entreprises telles qu'elles sont définies à l'annexe de la recommandation 2003/361/CE de la Commission du concernant la définition des micro, petites et moyennes entreprises;

(4) "utilisateur", toute personne physique ou morale, y compris une autorité publique, agence ou autre organisme sous l'autorité de laquelle ou duquel le système est utilisé;

(5) "mandataire", toute personne physique ou morale physiquement présente ou établie dans l'Union ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement;

(5 *bis*) "fabricant de produits", un fabricant au sens de tout acte législatif d'harmonisation de l'Union énuméré à l'annexe II;

(6) "importateur", toute personne physique ou morale physiquement présente 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 en dehors de l'Union;

(7) "distributeur", toute 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", le fournisseur, le fabricant du produit, l'utilisateur, le mandataire, l'importateur ou le distributeur;

(9) "mise sur le marché", la première mise à disposition d'un système d'IA sur le marché de l'Union;

(10) "mise à disposition sur le marché", toute fourniture d'un système d'IA 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 directement à l'utilisateur en vue d'une première utilisation ou pour usage propre dans l'Union, conformément à la destination du système;

(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, telles que précisées dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente, 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;

(14) "composant de sécurité d'un produit ou d'un système", un composant d'un produit ou d'un système qui remplit une fonction de sécurité pour ce produit ou ce système 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 l'utilisateur, en particulier, de la destination et de l'utilisation correcte d'un système d'IA;

(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 des utilisateurs 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) "évaluation de la conformité", la procédure permettant de vérifier que les exigences relatives à un système d'IA à haut risque énoncées au titre III, chapitre 2, du présent règlement ont été respectées;

(20) "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;

(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 désigné en application du présent règlement et d'autres actes législatifs d'harmonisation de l'Union pertinents;

(23) "modification substantielle", une modification apportée au système d'IA à la suite de sa mise sur le marché ou de sa mise en service, qui a une incidence sur la conformité de ce système avec les exigences énoncées au titre III, chapitre 2, du présent règlement, ou une modification de la destination pour laquelle le système d'IA a été évalué; 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 ses performances 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.

(24) "marquage de conformité CE" ou "marquage CE", un marquage par lequel le fournisseur indique qu'un système d'IA est conforme aux exigences du titre III, chapitre 2, ou de l'article 4 *ter* du présent règlement et d'autres actes juridiques applicables de l'Union visant à harmoniser les conditions de commercialisation des produits (législation d'harmonisation de l'Union) 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 européenne au sens de l'article 2, paragraphe 1, point c), du règlement (UE) nº 1025/2012;

(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 et son processus d'apprentissage, notamment, afin d'éviter tout surajustement; le jeu de données de validation pouvant être un jeu de données distinct ou faire partie du jeu de données d'apprentissage, selon une division variable ou fixe;

(31) "données de test", les données utilisées pour fournir une évaluation indépendante du système d'IA entraîné et validé afin de confirmer les performances attendues de ce système avant sa mise sur le marché ou sa mise en service;

(32) "données d'entrée", les données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit un résultat;

(33) "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;

(34) "système de reconnaissance des émotions", un système d'IA permettant la reconnaissance ou la déduction des états psychologiques, des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques;

(35) "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;

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

(37) '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 instantanément ou quasi instantanément;

(38) [supprimé]

(39) "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 ou circonstances d'accès à cet espace qui aient été prédéterminées, et indépendamment d'éventuelles restrictions de capacité;

(40) "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;

(41) "fins répressives", des fins ayant trait aux 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;

(42) [supprimé]

(43) "autorité nationale compétente", l'une quelconque des suivantes: l'autorité notifiante et l'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, le Contrôleur européen de la protection des données assume les responsabilités qui, dans les États membres, sont confiées à l'autorité nationale compétente et, le cas échéant, toute référence aux autorités nationales compétentes ou aux autorités de surveillance du marché dans le présent règlement s'entend comme une référence au Contrôleur européen de la protection des données;

(44) "incident grave", tout 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 et du fonctionnement d'infrastructures critiques;

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

d) une atteinte grave à des biens ou à l'environnement.

(45) "infrastructure critique", un bien, un système ou une partie de celui-ci, qui est nécessaire à la fourniture d'un service essentiel au maintien de fonctions sociétales ou d'activités économiques vitales au sens de l'article 2, paragraphes 4 et 5, de la directive …/… sur la résilience des entités critiques;

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

(47) "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;

(48) "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 sont pas considérés comme constituant 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 53 ou à l'article 54 *bis* soient remplies;

(49) "plan d'essais en conditions réelles", un document décrivant les objectifs, la méthodologie, le champ d'application géographique et la portée dans le temps, le suivi, l'organisation et la conduite des essais en conditions réelles, ainsi que la population concernée;

(50) "participant", aux fins des essais en conditions réelles, une personne physique qui participe à des essais en conditions réelles;

(51) "consentement éclairé", l'expression, par un participant, de son plein gré et en toute liberté, de sa volonté de participer à un essai en conditions réelles particulier, après avoir pris connaissance de tous les éléments de l'essai qui lui permettent de prendre sa décision concernant sa participation; dans le cas des mineurs et des personnes incapables, le consentement éclairé est donné par leur représentant légal;

(52) "bac à sable réglementaire de l'IA", un cadre concret mis en place par une autorité nationale compétente qui offre aux fournisseurs ou fournisseurs potentiels de systèmes d'IA la possibilité de développer, d'entraîner, de valider et de tester, le cas échéant en conditions réelles, un système d'IA innovant, selon un plan spécifique pour une durée limitée sous surveillance réglementaire.

Article 4

Actes d'exécution

Afin d'assurer des conditions uniformes d'exécution du présent règlement en ce qui concerne les approches d'apprentissage automatique et les approches fondées sur la logique et les connaissances visées à l'article 3, point 1), la Commission peut adopter des actes d'exécution pour préciser les éléments techniques desdites approches, en tenant compte des évolutions du marché et des technologies. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.

TITRE I *BIS*

SYSTÈMES D'IA À USAGE GÉNÉRAL

Article 4 bis

Conformité des systèmes d'IA à usage général avec le présent règlement

1. Sans préjudice des articles 5, 52, 53 et 69 du présent règlement, les systèmes d'IA à usage général sont conformes uniquement aux exigences et obligations énoncées à l'article 4 *ter*.

2. Lesdites exigences et obligations s'appliquent indépendamment du fait que le système d'IA à usage général soit mis sur le marché ou mis en service en tant que modèle pré-entraîné ou que l'utilisateur doive procéder au réglage fin du modèle.

Article 4 ter

Exigences applicables aux systèmes d'IA à usage général et obligations à respecter par les fournisseurs de ces systèmes

1. Les systèmes d'IA à usage général susceptibles d'être utilisés comme systèmes d'IA à haut risque ou comme composants de systèmes d'IA à haut risque au sens de l'article 6 sont conformes les exigences établies au titre III, chapitre 2, du présent règlement à partir de la date d'application des actes d'exécution adoptés par la Commission en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2, au plus tard dix-huit mois après l'entrée en vigueur du présent règlement. Ces actes d'exécution précisent et adaptent l'application des exigences établies au titre III, chapitre 2, aux systèmes d'IA à usage général à la lumière de leurs caractéristiques, de la faisabilité technique, des spécificités de la chaîne de valeur de l'IA et des évolutions du marché et des technologies. Aux fins de la conformité auxdites exigences, il est tenu compte de l'état de la technique généralement reconnu.

2. Les fournisseurs de systèmes d'IA à usage général visés au paragraphe 1 se conforment, à partir de la date d'application des actes d'exécution visés au paragraphe 1, aux obligations énoncées aux articles 16 *bis bis*, 16 *sexies*, 16 *septies*, 16 *octies*, 16 *decies*, 16 *undecies*, 25, 48 et 61.

3. Afin de se conformer aux obligations énoncées à l'article 16 *sexies*, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne décrite à l'annexe VI, points 3 et 4.

4. Les fournisseurs de ces systèmes tiennent également la documentation technique visée à l'article 11 à la disposition des autorités nationales compétentes pendant une période prenant fin dix ans après que le système d'IA à usage général a été mis sur le marché dans l'Union ou mis en service dans l'Union.

5. Les fournisseurs de systèmes d'IA à usage général coopèrent avec les autres fournisseurs ayant l'intention de mettre en service ces systèmes ou de mettre ces systèmes sur le marché dans l'Union en tant que systèmes d'IA à haut risque ou composants de systèmes d'IA à haut risque, et leur fournissent les informations nécessaires, en vue de leur permettre de se conformer aux obligations qui leur incombent en vertu du présent règlement. Cette coopération entre fournisseurs préserve, le cas échéant, les droits de propriété intellectuelle et les informations commerciales confidentielles ou les secrets d'affaires, conformément à l'article 70. Afin d'assurer des conditions uniformes d'exécution du présent règlement en ce qui concerne les informations devant être partagées par les fournisseurs de systèmes d'IA à usage général, la Commission peut adopter des actes d'exécution en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.

6. Aux fins de la conformité aux exigences et obligations visées aux paragraphes 1, 2 et 3:

- toute référence à la destination s'entend comme une référence à l'utilisation éventuelle des systèmes d'IA à usage général en tant que systèmes d'IA à haut risque ou en tant que composants de systèmes d'IA à haut risque au sens de l'article 6;

- toute référence aux exigences applicables aux systèmes d'IA à haut risque figurant au titre III, chapitre 2, s'entend comme visant exclusivement les exigences énoncées au présent article.

Article 4 quater
Exceptions à l'article 4 ter

1. L'article 4 *ter* ne s'applique pas lorsque le fournisseur a expressément exclu toutes les utilisations à haut risque dans la notice d'utilisation ou les informations accompagnant le système d'IA à usage général.

2. Cette exclusion est formulée de bonne foi et n'est pas réputée justifiée si le fournisseur a des raisons suffisantes de penser que le système peut être l'objet d'une mauvaise utilisation.

3. Lorsque le fournisseur décèle une mauvaise utilisation sur le marché ou en est informé, il prend toutes les mesures nécessaires et proportionnées pour prévenir une telle mauvaise utilisation à l'avenir, en particulier en tenant compte de l'ampleur de la mauvaise utilisation et de la gravité des risques associés.

TITRE II

PRATIQUES INTERDITES EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE

Article 5

1. Les pratiques en matière d'intelligence artificielle 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 avec pour objectif ou effet d'altérer substantiellement son comportement d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers;

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'un groupe de personnes donné avec pour objectif ou effet d'altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers;

c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA destinés à évaluer ou à établir un classement de personnes physiques au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues 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 physiques 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 physiques ou de groupes de personnes physiques, qui est injustifié ou disproportionné par rapport à leur comportement social ou à la gravité de celui-ci;

d) l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public par les autorités répressives ou pour leur compte 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 potentielles spécifiques de la criminalité;

ii) la prévention d'une menace spécifique et substantielle pour les infrastructures critiques, pour la vie, la santé ou la sécurité physique des personnes physiques ou la prévention d'une attaque terroriste;

iii) la localisation ou l'identification d'une personne physique aux fins de mener une enquête pénale, d'engager des poursuites ou d'exécuter une sanction pénale pour des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI[32] du Conseil 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 trois ans, ou d'autres infractions spécifiques punies dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins cinq ans, déterminées par le droit de cet État membre.

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, point d), 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 causé en l'absence d'utilisation du système;

[32] Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

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, point d), respecte les garanties et conditions nécessaires et proportionnées en ce qui concerne cette utilisation, notamment eu égard aux limitations temporelles, géographiques et relatives aux personnes.

3. En ce qui concerne le paragraphe 1, point d), et le 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 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 4. Toutefois, dans une situation d'urgence dûment justifiée, il est possible de commencer à utiliser le système sans autorisation à condition que cette autorisation soit demandée sans délai excessif en cours de l'utilisation du système d'IA et que, si cette demande d'autorisation est rejetée, il soit mis fin à l'utilisation avec effet immédiat.

L'autorité judiciaire ou administrative compétente 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" en cause est nécessaire et proportionnée à la réalisation de l'un des objectifs énumérés au paragraphe 1, point d), tels qu'indiqués dans la demande. Lorsqu'elle statue sur la demande, l'autorité judiciaire ou administrative compétente tient compte des éléments visés au paragraphe 2.

4. 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, point d), et aux paragraphes 2 et 3. L'État membre en question établit dans son droit national les modalités 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, point d), et notamment pour quelles infractions pénales visées au point iii) dudit paragraphe, les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives.

TITRE III

SYSTÈMES D'IA À HAUT RISQUE

CHAPITRE 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 qui constitue lui-même un produit couvert par les actes législatifs d'harmonisation de l'Union énumérés à l'annexe II est considéré comme étant à haut risque s'il doit être 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 aux actes législatifs susmentionnés.

2. Un système d'IA destiné à être utilisé comme composant de sécurité d'un produit couvert par les actes législatifs visés au paragraphe 1 est considéré comme étant à haut risque s'il doit être 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 aux actes législatifs susmentionnés.

Cette disposition s'applique que le système d'IA soit ou non mis sur le marché ou mis en service indépendamment du produit.

3. Les systèmes d'IA visés à l'annexe III sont considérés comme à haut risque, à moins que les résultats générés par le système ne soient purement accessoires par rapport à l'action ou à la décision à prendre et ne soient donc pas susceptibles d'entraîner un risque significatif pour la santé, la sécurité ou les droits fondamentaux.

Afin d'assurer des conditions uniformes d'exécution du présent règlement, la Commission adopte, au plus tard un an après l'entrée en vigueur du présent règlement, des actes d'exécution pour préciser les circonstances dans lesquelles les résultats générés par les systèmes d'IA visés à l'annexe III seraient purement accessoires par rapport à l'action ou à la décision à prendre. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.

Article 7

Modifications de l'annexe III

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 afin de modifier la liste figurant à l'annexe III en y ajoutant des systèmes d'IA à haut risque 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, points 1 à 8;

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, qui, eu égard à sa gravité et à sa probabilité d'occurrence, 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.

2. Lorsqu'elle évalue, aux fins du paragraphe 1, si un système d'IA présente un risque de préjudice pour la santé et la sécurité ou un risque d'incidence négative sur les droits fondamentaux équivalent ou supérieur au risque de préjudice que présentent les systèmes d'IA à haut risque déjà visés à l'annexe III, la Commission tient compte des critères suivants:

a) la destination prévue du système d'IA;

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

c) 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 matérialisation de ce préjudice ou de cette incidence négative, tel qu'il ressort des rapports ou allégations documentées soumis aux autorités nationales compétentes;

d) 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;

e) 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;

f) la mesure dans laquelle les personnes ayant potentiellement subi un préjudice ou une incidence négative se trouvent dans une situation vulnérable par rapport à l'utilisateur d'un système d'IA, notamment en raison d'un déséquilibre de pouvoir, de connaissances, de circonstances économiques ou sociales ou d'âge;

g) la mesure dans laquelle les résultats obtenus au moyen d'un système d'IA ne sont pas facilement réversibles, les résultats ayant une incidence sur la santé ou la sécurité des personnes ne devant pas être considérés comme facilement réversibles;

h) la mesure dans laquelle la législation existante 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;

i) la probabilité que l'utilisation de l'IA présente des avantages pour certaines personnes, certains groupes de personnes ou la société dans son ensemble et la portée de ces avantages.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 afin de modifier la liste figurant à l'annexe III en en supprimant des systèmes d'IA à haut risque lorsque les deux conditions suivantes sont remplies:

a) le ou les systèmes d'IA à haut risque concernés ne présentent plus de risques significatifs 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.

CHAPITRE 2

EXIGENCES APPLICABLES AUX SYSTEMES D'IA A HAUT RISQUE

Article 8

Respect des exigences

1. Les systèmes d'IA à haut risque respectent les exigences établies dans le présent chapitre, compte tenu de l'état de la technique généralement reconnu.

2. Pour garantir le respect de ces exigences, il est tenu compte de la destination du système d'IA à haut risque et du système de gestion des risques prévu à l'article 9.

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 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'une mise à jour méthodique. Il comprend les éléments suivants:

   a) l'identification et l'analyse des risques connus et prévisibles les plus probables pour la santé, la sécurité et les droits fondamentaux compte tenu de la destination du système d'IA à haut risque;

   b) [supprimé];

   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 61;

   d) l'adoption de mesures appropriées de gestion des risques conformément aux dispositions des paragraphes suivants.

   Les risques visés au présent paragraphe 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.

3. 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 le présent chapitre 2, 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.

4. Les mesures de gestion des risques visées au paragraphe 2, point d), sont telles que tout risque résiduel 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 possible 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 concernant les risques impossibles à éliminer;

c) fournir aux utilisateurs des informations adéquates conformément à l'article 13, notamment en ce qui concerne les risques visés au paragraphe 2, point b), du présent article, et, le cas échéant, 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, de la formation pouvant être attendues de l'utilisateur et de l'environnement dans lequel le système est destiné à être utilisé.

5. Les systèmes d'IA à haut risque sont soumis à des essais afin de garantir qu'ils fonctionnent de manière conforme à leur destination et qu'ils sont conformes aux exigences énoncées dans le présent chapitre.

6. Les procédures d'essai peuvent comprendre des essais en conditions réelles conformément à l'article 54 *bis*.

7. 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 la mise sur le marché ou la mise en service. Les tests sont effectués sur la base de métriques et de seuils probabilistes préalablement définis, qui sont adaptés à la destination du système d'IA à haut risque.

8. Le système de gestion des risques décrit aux paragraphes 1 à 7 accorde une attention particulière à la probabilité que des personnes âgées de moins de 18 ans puissent avoir accès au système d'IA à haut risque ou que ce dernier ait une incidence sur elles.

9. 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 de la législation sectorielle pertinente de l'Union, les aspects décrits aux paragraphes 1 à 8 peuvent faire partie des procédures de gestion des risques établies conformément à ladite législation.

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 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.

2. Les jeux de données d'entraînement, de validation et de test sont assujettis à des pratiques appropriées en matière de gouvernance et de gestion des données. Ces pratiques concernent en particulier:

   a) les choix de conception pertinents;

   b) les processus de collecte de données;

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

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

e) une évaluation préalable 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 physiques ou de se traduire par une discrimination interdite par le droit de l'Union;

g) la détection d'éventuelles lacunes ou déficiences dans les données, 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, représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets. Ils possèdent les propriétés statistiques appropriées, y compris, le cas 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 présentes au niveau des jeux de données pris individuellement ou d'une combinaison de ceux-ci.

4. Les jeux de données d'entraînement, de validation et de test tiennent compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au contexte géographique, 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 surveillance, de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, les fournisseurs de ces systèmes peuvent traiter des catégories particulières 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, sous réserve de garanties appropriées pour les droits et libertés fondamentaux des personnes physiques, y compris des limitations techniques relatives à la réutilisation ainsi que l'utilisation des mesures les plus avancées en matière de sécurité et de protection de la vie privée, telles que la pseudonymisation, ou le cryptage lorsque l'anonymisation peut avoir une incidence significative sur l'objectif poursuivi.

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, les paragraphes 2 à 5 s'appliquent uniquement aux jeux de données de test.

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 le présent chapitre et à fournir aux autorités nationales compétentes et aux organismes notifiés toutes 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 ou, dans le cas des PME, y compris les jeunes entreprises, toute documentation équivalente répondant aux mêmes objectifs, à moins que cela ne soit considéré comme inapproprié par l'autorité compétente.

2. Lorsqu'un système d'IA à haut risque lié à un produit auquel s'appliquent les actes juridiques énumérés à l'annexe II, section A, est mis sur le marché ou mis en service, une seule documentation technique est établie, contenant toutes les informations visées à l'annexe IV 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 73 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 le présent chapitre.

Article 12

Enregistrement

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

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

i) repérer les situations susceptibles d'avoir pour effet que le système d'IA présente un risque au sens de l'article 65, paragraphe 1, ou d'entraîner une modification substantielle;

ii) faciliter la surveillance après commercialisation visée à l'article 61; et

iii) surveiller le fonctionnement du système d'IA à haut risque comme prévu à l'article 29, paragraphe 4.

4. Pour les systèmes d'IA à haut risque visés à l'annexe III, paragraphe 1, point a), les fonctionnalités d'enregistrement 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 utilisateurs

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 assurer au respect des obligations pertinentes incombant à l'utilisateur et au fournisseur énoncées au chapitre 3 du présent titre et permettre aux utilisateurs de comprendre et d'utiliser correctement le système.

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 utilisateurs.

3. Les informations visées au paragraphe 2 comprennent:

   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, y compris le contexte géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé;

      ii) le niveau d'exactitude, y compris les paramètres 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, 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, son comportement en ce qui concerne des personnes ou groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé;

v) 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.

vi) le cas échéant, la description des résultats attendus du système;

c) les modifications du système d'IA à haut risque et de ses performances 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 résultats des systèmes d'IA par les utilisateurs;

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) une description du mécanisme compris dans le système d'IA qui permet aux utilisateurs de collecter, stocker et interpréter correctement les journaux, le cas échéant.

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 la période d'utilisation du système d'IA.

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 nonobstant l'application d'autres exigences énoncées dans le présent chapitre.

3. Le contrôle humain est assuré au moyen d'une ou de la totalité des types de mesures suivants:

   a) lorsque cela est techniquement possible, des mesures identifiées et 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 l'utilisateur.

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 à l'utilisateur de telle manière que les personnes physiques chargées d'effectuer un contrôle humain, en fonction des circonstances et dans la mesure où cela est proportionné, ont la possibilité:

   a) d'appréhender les capacités et les limites du système d'IA à haut risque et d'être en mesure de surveiller correctement son fonctionnement;

   b) d'avoir conscience d'une éventuelle tendance à se fier automatiquement ou excessivement aux résultats produits par un système d'IA à haut risque ("biais d'automatisation");

   c) d'interpréter correctement les résultats 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 de négliger, passer outre ou inverser le résultat fourni par ce système;

   e) d'intervenir sur le fonctionnement du système d'IA à haut risque ou d'interrompre ce fonctionnement au moyen d'un bouton d'arrêt ou d'une procédure similaire.

5. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les mesures prévues au paragraphe 3 sont de nature à garantir qu'en outre, aucune mesure ou décision n'est prise par l'utilisateur sur la base de l'identification résultant du système sans vérification et confirmation distinctes par au moins deux personnes physiques. 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, dans les cas où 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, compte tenu de leur destination, d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de manière cohérente à cet égard tout au long de leur cycle de vie.

2. Les niveaux d'exactitude et les métriques pertinents en matière d'exactitude des systèmes d'IA à haut risque sont indiqués dans la notice d'utilisation jointe.

3. Les systèmes d'IA à haut risque font preuve de résilience 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 solutions techniques redondantes, telles que des plans de sauvegarde ou des mesures de sécurité après défaillance, permettent 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 résultats éventuellement biaisés n'influencent les données d'entrée pour les opérations futures ("boucles de rétroaction") fassent l'objet d'un traitement adéquat au moyen de mesures d'atténuation appropriées.

4. Les systèmes d'IA à haut risque résistent aux tentatives de tiers non autorisés visant à modifier leur utilisation ou leurs performances 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, le cas échéant, des mesures ayant pour but de prévenir et de maîtriser les attaques visant à manipuler le jeu de données d'entraînement ("empoisonnement des données"), les données d'entrée destinées à induire le modèle en erreur ("exemples adverses") ou les défauts du modèle.

CHAPITRE 3

OBLIGATIONS INCOMBANT AUX FOURNISSEURS ET AUX UTILISATEURS 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 au chapitre 2 du présent titre;

a *bis*) indiquent leur nom, raison sociale ou marque déposée et l'adresse à laquelle ils peuvent être contactés, 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;

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

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

d) 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 20;

e) 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;

f) respectent les obligations en matière d'enregistrement prévues à l'article 51, paragraphe 1;

g) prennent les mesures correctives nécessaires visées à l'article 21 si le système d'IA à haut risque n'est pas conforme aux exigences énoncées au chapitre 2 du présent titre;

h) informent l'autorité nationale compétente concernée des États membres dans lesquels ils ont mis le système d'IA à disposition ou en service et, le cas échéant, l'organisme notifié, de la non-conformité et de toute mesure corrective prise;

i) apposent le marquage CE sur leurs systèmes d'IA à haut risque afin d'indiquer la conformité au présent règlement, conformément à l'article 49;

j) à la demande d'une autorité nationale compétente, apportent la preuve de la conformité du système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent titre.

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;

e) des spécifications techniques, notamment des normes, à appliquer et, lorsque les normes harmonisées pertinentes ne sont pas appliquées intégralement, les moyens à utiliser pour faire en sorte que le système d'IA à haut risque satisfasse aux exigences énoncées au chapitre 2 du présent titre;

f) les systèmes et procédures de gestion des données, notamment 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 maintien d'un système de surveillance après commercialisation conformément à l'article 61;

i) les procédures relatives à la notification d'un incident grave conformément à l'article 62;

j) la gestion des communications avec les autorités nationales compétentes, les autorités compétentes, y compris les autorités sectorielles, 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.

2 *bis*. Si les fournisseurs de systèmes d'IA à haut risque sont soumis à des obligations concernant les systèmes de gestion de la qualité en vertu de la législation sectorielle pertinente de l'Union, les aspects décrits au paragraphe 1 peuvent faire partie des systèmes de gestion de la qualité conformément à ladite législation.

3. Si les fournisseurs sont des établissements financiers soumis à des exigences relatives à leur gouvernance, à leurs dispositifs et 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 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). Dans ce contexte, toute norme harmonisée visée à l'article 40 du présent règlement est prise en considération.

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, 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 48.

1 *bis*. 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.

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 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

Évaluation de la conformité

1. Les fournisseurs de systèmes d'IA à haut risque veillent à ce que leurs systèmes soient soumis à la procédure d'évaluation de la conformité applicable conformément à l'article 43, avant leur mise sur le marché ou leur mise en service. Lorsqu'il a été démontré, à la suite de cette évaluation de la conformité, que les systèmes d'IA satisfont aux exigences énoncées au chapitre 2 du présent titre, les fournisseurs établissent une déclaration UE de conformité conformément à l'article 48 et apposent le marquage de conformité CE conformément à l'article 49.

2. [supprimé]

Article 20

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 en vertu d'un arrangement contractuel avec l'utilisateur ou d'autres modalités prévues par la loi. Ils les conservent pendant une période d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicables, 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 21

Mesures correctives

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 recherchent immédiatement les causes de cette non-conformité, le cas échéant, en collaboration avec l'utilisateur qui l'a signalée et prennent les mesures correctives nécessaires pour le mettre en conformité, le retirer ou le rappeler, selon le cas. Ils informent les distributeurs du système d'IA à haut risque en question et, le cas échéant, le mandataire et les importateurs en conséquence.

Article 22

Devoir d'information

Lorsque le système d'IA à haut risque présente un risque au sens de l'article 65, paragraphe 1, et que ce risque est connu du fournisseur du système, celui-ci en informe immédiatement les autorités nationales compétentes des États membres dans lesquels il a mis le système à disposition et, le cas échéant, l'organisme notifié qui a délivré un certificat pour le système d'IA à haut risque, en précisant notamment le cas de non-conformité et les éventuelles mesures correctives prises.

Article 23

Coopération avec les autorités compétentes

À la demande d'une autorité nationale 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 au chapitre 2 du présent titre, dans une langue aisément compréhensible par l'autorité de l'État membre concerné. À la demande motivée d'une autorité nationale compétente, les fournisseurs accordent également à cette autorité 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 se trouvent sous leur contrôle en vertu d'un arrangement contractuel avec l'utilisateur ou d'autres modalités prévues par la loi.

Article 23 bis

Conditions dans lesquelles un tiers est soumis aux mêmes obligations que le fournisseur

1. Toute personne physique ou morale est considérée comme le fournisseur d'un nouveau système d'IA à haut risque aux fins du présent règlement et est soumise aux obligations incombant au fournisseur au titre de l'article 16 dans toutes les circonstances suivantes:

   a) elle 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) [supprimé]

c) elle apporte une modification substantielle à un système d'IA à haut risque déjà mis sur le marché ou mis en service;

d) elle modifie la destination d'un système d'IA qui n'est pas à haut risque et qui est déjà mis sur le marché ou mis en service de telle sorte qu'il devient un système à haut risque;

e) elle met sur le marché ou met en service un système d'IA à usage général en tant que système d'IA à haut risque ou que composant d'un système d'IA à haut risque.

2. Lorsque les circonstances visées au paragraphe 1, point a) ou c), se produisent, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA à haut risque n'est plus considéré comme un fournisseur aux fins du présent règlement.

3. Pour les systèmes d'IA à haut risque constituant des composants de sécurité de produits auxquels s'appliquent les actes juridiques énumérés à l'annexe II, 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:

i) 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;

ii) 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.

Article 24

[supprimé]

Article 25

Mandataires

1. Avant de mettre leurs systèmes à disposition sur le marché de l'Union, les fournisseurs établis en dehors de l'Union désignent, par mandat écrit, un mandataire établi dans l'Union.

2. Le mandataire exécute les tâches indiquées dans le mandat que lui a confié le fournisseur. Aux fins du présent règlement, le mandat habilite le mandataire à exécuter uniquement les tâches suivantes:

-a) vérifier que la déclaration UE de conformité et la documentation technique ont été établies et que le fournisseur a suivi une procédure appropriée d'évaluation de la conformité;

a) tenir à la disposition des autorités nationales compétentes et des autorités nationales visées à l'article 63, paragraphe 7, pendant une période prenant fin dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les coordonnées du fournisseur par lequel le mandataire a été désigné, une copie de la déclaration UE de conformité, la documentation technique et, le cas échéant, le certificat délivré par l'organisme notifié;

b) à la demande motivée d'une autorité nationale compétente, communiquer à cette dernière toutes les informations et tous les documents, y compris ceux conservés conformément au point b), nécessaires à la démonstration de la conformité d'un système d'IA à haut risque avec les exigences énoncées au chapitre 2 du présent titre, et notamment lui donner accès aux journaux automatiquement générés 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 en vertu d'un arrangement contractuel avec l'utilisateur ou d'autres modalités prévues par la loi;

c) à la demande motivée des autorités nationales compétentes, coopérer avec elles à toute mesure prise par ces dernières à l'égard du système d'IA à haut risque;

d) respecter les obligations en matière d'enregistrement prévues à l'article 51, paragraphe 1, et, si l'enregistrement du système est effectué par le fournisseur lui-même, vérifier que les informations visées à l'annexe VIII, partie II, points 1 à 11, sont correctes.

Le mandataire met fin au mandat s'il a des raisons suffisantes de considérer que le fournisseur agit de manière contraire aux obligations qui lui incombent au titre du présent règlement. Dans ce cas, il informe en outre immédiatement l'autorité de surveillance du marché de l'État membre dans lequel il est établi et, selon le cas, l'organisme notifié compétent de la cessation du mandat et des motifs qui la sous-tendent.

Le mandataire est légalement responsable des systèmes d'IA défectueux conjointement et solidairement avec le fournisseur, et sur la même base que lui, eu égard à sa responsabilité potentielle au titre de la directive 85/374/CEE.

Article 26

Obligations des importateurs

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

a) le fournisseur de ce système d'IA a suivi la procédure d'évaluation de la conformité applicable visée à l'article 43;

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

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

d) le mandataire visé à l'article 25 a été désigné par le fournisseur.

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, a été falsifié ou s'accompagne de documents falsifiés, il ne met ce 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 65, paragraphe 1, l'importateur en informe le fournisseur du système d'IA, 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 ou, lorsque cela n'est pas possible, 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, le cas échéant, que les conditions de stockage ou de transport ne compromettent pas sa conformité aux exigences énoncées au chapitre 2 du présent titre.

4 *bis*. Pendant une période prenant fin dix ans après la mise sur le marché ou la mise en place du système d'IA, 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.

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

5 *bis*. Les importateurs coopèrent avec les autorités nationales compétentes à toute mesure prise par ces autorités à l'égard d'un système d'IA dont ils sont l'importateur.

Article 27

Obligations des distributeurs

1. Avant de mettre un système d'IA à haut risque à disposition sur le marché, les distributeurs vérifient que le système d'IA à haut risque porte le marquage de conformité CE requis, qu'il est accompagné d'une copie de la déclaration UE de conformité et de la notice d'utilisation, et que le fournisseur et l'importateur du système, selon le cas, ont respecté les obligations qui leur incombent en vertu respectivement de l'article 16, point b), et de l'article 26, paragraphe 3.

2. Lorsqu'un distributeur considère ou a des raisons de considérer qu'un système d'IA à haut risque n'est pas conforme aux exigences énoncées au chapitre 2 du présent titre, il ne met ce système sur le marché qu'après la mise en conformité de celui-ci avec lesdites exigences. De plus, lorsque le système présente un risque au sens de l'article 65, paragraphe 1, le distributeur en informe le fournisseur ou l'importateur du système, selon le cas.

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

4. Lorsqu'un distributeur considère ou a des raisons de considérer qu'un système d'IA à haut risque qu'il a mis à disposition sur le marché n'est pas conforme aux exigences énoncées au chapitre 2 du présent titre, 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 65, paragraphe 1, le distributeur en informe immédiatement les autorités nationales compétentes des États membres dans lesquels il a mis le produit à disposition et précise, notamment, le cas de non-conformité et les éventuelles mesures correctives prises.

5. À la demande motivée d'une autorité nationale compétente, les distributeurs de systèmes d'IA à haut risque communiquent à cette autorité toutes les informations et tous les documents nécessaires relatifs à ses activités mentionnés aux paragraphes 1 à 4.

5 *bis*. Les distributeurs coopèrent avec les autorités nationales compétentes à toute mesure prise par ces autorités à l'égard d'un système d'IA dont ils sont le distributeur.

Article 28

[supprimé]

Article 29

Obligations des utilisateurs de systèmes d'IA à haut risque

1. Les utilisateurs de systèmes d'IA à haut risque utilisent ces systèmes conformément aux notices d'utilisation accompagnant les systèmes, conformément aux paragraphes 2 et 5.

1 *bis*. Les utilisateurs confient le contrôle humain à des personnes physiques qui disposent des compétences, de la formation et de l'autorité nécessaires.

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

3. Sans préjudice du paragraphe 1, pour autant que l'utilisateur exerce un contrôle sur les données d'entrée, il veille à ce que ces dernières soient pertinentes au regard de la destination du système d'IA à haut risque.

4. Les utilisateurs mettent en œuvre un contrôle humain et surveillent le fonctionnement du système d'IA à haut risque sur la base de la notice d'utilisation. Lorsqu'ils ont des raisons de considérer que l'utilisation conformément à la notice d'utilisation peut avoir pour effet que le système d'IA présente un risque au sens de l'article 65, paragraphe 1, ils en informent le fournisseur ou le distributeur et suspendent l'utilisation du système. Ils informent également le fournisseur ou le distributeur lorsqu'ils constatent un incident grave et ils interrompent l'utilisation du système d'IA. Si l'utilisateur n'est pas en mesure de joindre le fournisseur, l'article 62 s'applique par analogie. Cette obligation ne couvre pas les données opérationnelles sensibles des utilisateurs de systèmes d'IA qui sont des autorités répressives.

Si les utilisateurs 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.

5. Les utilisateurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par ce système d'IA à haut risque, visés à l'article 12, paragraphe 1, dans la mesure où ces journaux se trouvent sous leur contrôle. Ils les conservent pendant une période d'au moins six mois, sauf disposition contraire dans le droit de l'Union ou le droit national applicables, en particulier dans le droit de l'Union sur la protection des données à caractère personnel.

Si les utilisateurs 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.

5 *bis*. Si les utilisateurs de systèmes d'IA à haut risque sont des autorités, des agences ou des organismes publics, à l'exception des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétences en matière d'asile, ils respectent les obligations en matière d'enregistrement prévues à l'article 51. Dans le cas où ils constatent que le système qu'ils envisagent d'utiliser n'a pas été enregistré dans la base de données de l'UE visée à l'article 60, ils n'utilisent pas ce système et informent le fournisseur ou le distributeur.

6. Les utilisateurs de systèmes d'IA à haut risque utilisent les informations fournies en application de l'article 13 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, le cas échéant.

6 *bis*. Les utilisateurs coopèrent avec les autorités nationales compétentes à toute mesure prise par ces autorités à l'égard d'un système d'IA dont ils sont l'utilisateur.

CHAPITRE 4

AUTORITÉS NOTIFIANTES ET ORGANISMES NOTIFIÉS

Article 30

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.

2. Les États membres peuvent décider que l'évaluation et le contrôle visés au paragraphe 1 sont effectués par un organisme national d'accréditation au sens du règlement (CE) nº 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 70.

7. Les autorités notifiantes disposent d'un personnel compétent en nombre suffisant pour la bonne exécution de leurs tâches.

8. [supprimé]

Article 31

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 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 33. 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 aux exigences définies à l'article 33. 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 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 33 demeurent observées.

Article 32

Procédure de notification

1. Les autorités notifiantes ne peuvent notifier que les organismes d'évaluation de la conformité qui ont satisfait aux exigences définies à l'article 33.

2. Les autorités notifiantes notifient ces organismes à la Commission et aux autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission.

3. La notification visée au paragraphe 2 comprend des informations complètes sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et les 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 31, 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 33.

4. L'organisme d'évaluation de la conformité 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 31, 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 31, paragraphe 3.

5. [supprimé]

Article 33

Exigences concernant les organismes notifiés

1. Un organisme notifié est constitué en vertu du droit national 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.

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

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 le système d'IA à haut risque qui fait l'objet de l'évaluation, ainsi que de tout concurrent du fournisseur.

5. 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.

6. 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 respectent la confidentialité des informations auxquelles ils accèdent durant l'exercice de leurs activités d'évaluation de la conformité, conformément à l'article 70, 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.

7. Les organismes notifiés disposent de procédures pour accomplir leurs activités qui tiennent dûment compte de la taille des entreprises, du secteur dans lequel elles exercent leurs activités, de leur structure et du degré de complexité du système d'IA en question.

8. 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 situés sur la base de la législation nationale ou que l'évaluation de la conformité ne soit réalisée directement par cet État membre lui-même.

9. Les organismes notifiés sont en mesure d'accomplir toutes les tâches qui leur incombent 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.

10. 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 technologies d'intelligence artificielle en cause et aux exigences énoncées au chapitre 2 du présent titre.

11. 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.

12. [supprimé]

Article 33 bis

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 33 dans la mesure où les normes harmonisées applicables couvrent ces exigences.

Article 34

Filiales et sous-traitants des organismes notifiés

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 33 et en informe l'autorité notifiante.

2. Les organismes notifiés assument l'entière responsabilité des tâches effectuées par des sous-traitants ou des filiales, quel que soit leur lieu d'établissement.

3. Des activités ne peuvent être sous-traitées ou réalisées par une filiale qu'avec l'accord du fournisseur.

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 l'activité sous-traitée.

Article 34 bis

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 accomplissent leurs activités tout en évitant les charges inutiles pour les fournisseurs et en tenant dûment compte de la taille de l'entreprise, du secteur dans lequel elle exercent leurs activités, de sa structure et du degré de complexité du système d'IA en question. Ce faisant, l'organisme notifié respecte néanmoins le degré de rigueur et le niveau de protection requis pour la conformité du système d'IA à haut risque aux exigences du présent règlement.

3. Les organismes notifiés mettent à la disposition de l'autorité notifiante visée à l'article 30 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 au présent chapitre.

Article 35

Numéros d'identification et listes des organismes notifiés désignés au titre du présent règlement

1. La Commission attribue un numéro d'identification aux organismes notifiés. Elle attribue un seul numéro, même si un même organisme est notifié au titre de plusieurs actes de l'Union.

2. La Commission rend publique la liste des organismes notifiés au titre du présent règlement et y mentionne les numéros d'identification qui leur ont été attribués 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 32, paragraphe 2.

2. Les procédures décrites aux articles 31 et 32 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 ci-après s'appliquent.

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, un an avant de mettre un terme à ses activités. Les certificats peuvent rester valables pendant une période temporaire 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 concernés par ces certificats. Le nouvel organisme notifié procède à une évaluation complète des systèmes d'IA concernés avant la fin de cette période, 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.

3. Lorsqu'une autorité notifiante a des raisons suffisantes de considérer qu'un organisme notifié ne répond plus aux exigences définies à l'article 33, ou qu'il ne s'acquitte pas de ses obligations, elle soumet la notification à des restrictions, la suspend ou la retire, en fonction de la gravité du manquement, pour autant que l'organisme notifié ait eu la possibilité de faire connaître son point de vue. Elle en informe immédiatement la Commission et les autres États membres.

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

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

6. 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 notification;

   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 des systèmes d'IA 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 compétente prend les mesures appropriées si cela est nécessaire pour éviter un risque potentiel pour la santé, la sécurité ou les droits fondamentaux.

7. À l'exception des certificats délivrés à tort, et lorsqu'une notification a été suspendue ou restreinte, les certificats restent valables dans les 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 et les mesures prévues pour remédier à la suspension ou à la restriction; ou

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 responsable des organismes notifiés considère que l'organisme notifié n'est pas en mesure de confirmer les certificats existants délivrés, le fournisseur adresse aux autorités nationales compétentes de l'État membre dans lequel le fournisseur du système faisant l'objet du certificat a son siège social, dans un délai de trois mois suivant la suspension ou la restriction, la confirmation écrite 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.

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

b) lorsqu'un autre organisme notifié a confirmé par écrit qu'il assumera la responsabilité immédiate de ces systèmes et qu'il achèvera leur 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 notification 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 conformité d'un organisme notifié avec les exigences énoncées à l'article 33.

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

3. La Commission veille à ce que toutes les informations confidentielles obtenues au cours des enquêtes qu'elle mène au titre du présent article soient traitées de manière confidentielle conformément à l'article 70.

4. Lorsque la Commission établit qu'un organisme notifié ne répond pas ou ne répond plus aux exigences fixées à l'article 33, elle informe l'autorité notifiante des raisons d'une telle constatation et lui demande de prendre les mesures correctives qui s'imposent, y compris la suspension, la restriction ou le retrait de la désignation si nécessaire. Si l'autorité notifiante ne prend pas les mesures correctives qui s'imposent, la Commission peut, au moyen d'actes d'exécution, suspendre, restreindre ou retirer la notification. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 74, 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. L'autorité notifiante veille à ce que les organismes qu'ils ont notifiés participent aux travaux de ce groupe, directement ou par l'intermédiaire de représentants désignés.

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 énoncées à l'article 33.

CHAPITRE 5

NORMES, ÉVALUATION DE LA CONFORMITÉ, CERTIFICATS, ENREGISTREMENT

Article 40

Normes harmonisées

1. Les systèmes d'IA à haut risque ou 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* sont présumés conformes aux exigences visées au chapitre 2 du présent titre ou, le cas échéant, aux exigences énoncées aux articles 4 *bis* et 4 *ter*, dans la mesure où celles-ci sont couvertes par ces normes.

2. Lorsqu'elle présente une demande de normalisation aux organisations européennes de normalisation conformément à l'article 10 du règlement (UE) nº 1025/2012, la Commission précise que les normes doivent être cohérentes, claires et conçues de telle sorte qu'elles visent à atteindre notamment les objectifs suivants:

   a) veiller à ce que les systèmes d'IA mis sur le marché ou mis en service dans l'Union soient sûrs et qu'ils respectent les valeurs de l'Union et renforcent l'autonomie stratégique ouverte de l'Union;

   b) 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;

   c) renforcer la gouvernance multipartite en veillant à ce que toutes les parties prenantes européennes concernées (par exemple l'industrie, les PME, la société, les chercheurs) soient représentées;

   d) contribuer à renforcer la coopération mondiale en faveur d'une normalisation dans le domaine de l'IA qui soit conforme aux valeurs et aux intérêts de l'Union.

La Commission demande aux organisations européennes de normalisation de démontrer qu'elles mettent tout en œuvre pour réaliser les objectifs susmentionnés.

Article 41

Spécifications communes

1. La Commission est habilitée à adopter, après consultation du Comité de l'IA visé à l'article 56, des actes d'exécution conformément à la procédure d'examen visée à l'article 74, paragraphe 2, établissant des spécifications techniques communes pour les exigences énoncées au chapitre 2 du présent titre ou, le cas échéant, aux exigences énoncées aux articles 4 *bis* et 4 *ter*, lorsque les conditions suivantes sont remplies:

   a) aucune référence à des normes harmonisées couvrant les préoccupations essentielles en matière de sécurité et de droits fondamentaux n'a été publiée au *Journal officiel de l'Union européenne* conformément au règlement (UE) nº 1025/2012;

   b) la Commission, en vertu de l'article 10, paragraphe 1, du règlement (UE) nº 1025/2012, a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée pour les exigences énoncées au chapitre 2 du présent titre;

   c) la demande visée au point b) n'a été acceptée par aucune des organisations européennes de normalisation, 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) nº 1025/2012 ou ces normes ne sont pas conformes à la demande.

1 *bis*. Avant d'élaborer un projet d'acte d'exécution, la Commission informe le comité visé à l'article 22 du règlement (UE) nº 1025/2012 qu'elle considère que les conditions énoncées au paragraphe 1 sont remplies.

2. Au début de l'élaboration du projet d'acte d'exécution établissant les spécifications communes, la Commission satisfait aux objectifs visés à l'article 40, paragraphe 2, et recueille les avis des organismes ou groupes d'experts concernés établis en vertu de la législation sectorielle pertinente de l'Union. Sur la base de cette consultation, la Commission élabore le projet d'acte d'exécution.

3. Les systèmes d'IA à haut risque ou à usage général conformes aux spécifications communes visées au paragraphe 1 sont présumés conformes aux exigences visées au chapitre 2 du présent titre ou, le cas échéant, aux exigences énoncées aux articles 4 *bis* et 4 *ter*, dans la mesure où celles-ci sont couvertes par ces normes.

4. Lorsque les références d'une norme harmonisée sont publiées au *Journal officiel de l'Union européenne*, les actes d'exécution visés au paragraphe 1, qui couvrent les exigences énoncées au chapitre 2 du présent titre ou les exigences énoncées aux articles 4 *bis* et 4 *ter*, sont abrogés, selon le cas.

5. Lorsqu'un État membre considère qu'une spécification commune ne satisfait pas entièrement aux exigences énoncées au chapitre 2 du présent titre ou aux exigences énoncées aux articles 4 *bis* et 4 *ter*, selon le cas, il en informe la Commission au moyen d'une explication détaillée et la Commission évalue ces informations et, le cas échéant, modifie l'acte d'exécution établissant la spécification commune en question.

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 contexte géographique, comportemental ou fonctionnel spécifique dans lequel ils sont destinés à être utilisés sont présumés conformes aux exigences respectives énoncées à l'article 10, paragraphe 4.

2. Les systèmes d'IA à haut risque ou à usage général 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 du Parlement européen et du Conseil[33] 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 au chapitre 2 du présent titre, 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 suivantes:

   a) la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI; ou

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

   Lorsque, pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées au chapitre 2 du présent titre, le fournisseur n'a pas appliqué ou n'a appliqué qu'en partie les normes harmonisées visées à l'article 40, ou lorsque ces normes harmonisées n'existent pas et que les spécifications communes visées à l'article 41 font défaut, le fournisseur suit la procédure d'évaluation de la conformité prévue à l'annexe VII.

[33] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) nº 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

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 est destiné à être mis en service par les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile ainsi que les institutions, organes ou agences de l'UE, l'autorité de surveillance du marché visée à l'article 63, paragraphe 5 ou 6, 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, et les systèmes d'IA à usage général visés au titre 1 *bis*, 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 auxquels s'appliquent les actes juridiques énumérés à l'annexe II, section A, le fournisseur procède à l'évaluation de la conformité selon les modalités requises par ces actes juridiques. Les exigences énoncées au chapitre 2 du présent titre 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 cette évaluation, 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 au chapitre 2 du présent titre, à condition que le respect, par ces organismes notifiés, des exigences énoncées à l'article 33, paragraphes 4, 9 et 10, ait été évalué dans le cadre de la procédure de notification prévue par ces actes juridiques.

Lorsque les actes juridiques énumérés à l'annexe II, section A, confèrent 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 les exigences énoncées au chapitre 2 du présent titre.

4. [supprimé]

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 aux fins de la mise à jour des annexes VI et VII compte tenu du progrès technique.

6. La Commission est habilitée à adopter des actes délégués visant à modifier les paragraphes 1 et 2 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. 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, sur la base d'une nouvelle évaluation suivant les procédures d'évaluation de la conformité applicables. Tout document complémentaire à un certificat est valable aussi longtemps que l'est le certificat qu'il complète.

3. Lorsqu'un organisme notifié constate qu'un système d'IA ne répond plus aux exigences énoncées au chapitre 2 du présent titre, 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.

Article 45

Recours contre les décisions des organismes notifiés

Une procédure de recours contre les décisions des organismes notifiés est disponible.

Article 46

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, toute approbation d'un système de gestion de la qualité délivrée conformément aux exigences de l'annexe VII;

   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, des 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 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 obligations visées aux paragraphes 1 à 3 sont respectées conformément à l'article 70.

Article 47

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 et 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 un laps de temps limité, 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 dans les meilleurs délais.

1 *bis*. 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, et, si la demande est rejetée, le système cesse immédiatement d'être utilisé et les produits de l'utilisation sont immédiatement mis au rebut.

2. 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 du chapitre 2 du présent titre. L'autorité de surveillance du marché informe la Commission et les autres États membres de toute autorisation délivrée conformément au paragraphe 1. Cette obligation ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives.

3. [supprimé]

4. [supprimé]

5. [supprimé]

6. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation de l'Union en matière d'harmonisation visée à l'annexe II, section A, seules les dérogations à la procédure d'évaluation de la conformité établies dans cette législation s'appliquent.

Article 48

Déclaration UE de conformité

1. Le fournisseur établit une déclaration UE de conformité signée à la main ou électroniquement concernant chaque système d'IA 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 a été mis sur le marché ou mis en service. La déclaration UE de conformité identifie le système d'IA 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 en question satisfait aux exigences énoncées au chapitre 2 du présent titre. 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 du ou des États membres dans lesquels le système d'IA à haut risque est mis à disposition.

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 aux systèmes 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 au chapitre 2 du présent titre. 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 73 pour mettre à jour le contenu de la déclaration UE de conformité prévu à l'annexe V afin d'y introduire les éléments devenus nécessaires compte tenu des progrès techniques.

Article 49

Marquage de conformité CE

1. Le marquage de conformité CE est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) nº 765/2008.

2. 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.

3. 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 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.

Article 50

[supprimé]

Article 51

Enregistrement des opérateurs concernés et des systèmes d'IA à haut risque énumérés à l'annexe III

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, points 1, 6 et 7 dans les domaines des activités répressives et de la gestion de la migration, de l'asile et des contrôles aux frontières, et des systèmes d'IA visés à l'annexe III, point 2, le fournisseur et, selon le cas, le mandataire s'enregistrent dans la base de données de l'UE visée à l'article 60. Le fournisseur ou, selon le cas, le mandataire, enregistre également leurs systèmes dans cette base de données.

2. Avant d'utiliser un système d'IA à haut risque énuméré à l'annexe III, les utilisateurs de systèmes d'IA à haut risque qui sont des autorités, des agences ou des organismes publics, ou les entités agissant pour leur compte, s'enregistrent dans la base de données de l'UE visée à l'article 60 et sélectionnent le système qu'ils envisagent d'utiliser.

   Les obligations énoncées à l'alinéa précédent ne s'appliquent pas aux autorités, agences ou organismes œuvrant dans les domaines des activités répressives, des contrôles aux frontières, de l'immigration ou de l'asile ni aux autorités, agences ou organismes utilisant les systèmes d'IA à haut risque visés à l'annexe III, point 2, ou aux entités agissant en leur nom.

TITRE IV

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

Article 52

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

1. Les fournisseurs veillent à ce que les systèmes d'IA destinés à interagir avec des personnes physiques soient conçus et développés de manière à ce que les personnes physiques 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 et de détection des infractions pénales, d'enquêtes et 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.

2. Les utilisateurs d'un système de reconnaissance biométrique informent du fonctionnement du système les personnes physiques qui y sont exposées. Cette obligation ne s'applique pas aux systèmes d'IA de catégorisation biométrique dont la loi autorise l'utilisation à des fins de prévention et de détection des infractions pénales et d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers.

2 *bis*. Les utilisateurs d'un système de reconnaissance des émotions informent du fonctionnement du système les personnes physiques qui y sont exposées. Cette obligation ne s'applique pas aux systèmes d'IA utilisés pour la reconnaissance des émotions de catégorisation biométrique dont la loi autorise l'utilisation à des fins de prévention et de détection des infractions pénales et d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers.

3. Les utilisateurs d'un système d'IA qui génère ou manipule des images ou des contenus audio ou vidéo présentant une ressemblance avec des personnes, des objets, des lieux ou d'autres entités ou événements existants et pouvant être perçus à tort comme authentiques ou véridiques ("hypertrucage") précisent que les contenus ont été générés ou manipulés artificiellement.

Toutefois, le premier alinéa ne s'applique pas lorsque l'utilisation est autorisée par la loi à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou lorsque le contenu fait partie d'un travail ou d'un programme manifestement créatif, satirique, artistique ou de fiction, sous réserve de garanties appropriées pour les droits et libertés de tiers.

3 *bis*. Les informations visées aux paragraphes 1 à 3 sont fournies aux personnes physiques de manière claire et reconnaissable au plus tard au moment de la première interaction ou de la première exposition.

4. Les paragraphes 1, 2, 2 *bis*, 3 et 3 *bis* n'ont pas d'incidence sur les exigences et obligations énoncées au titre III du présent règlement et sont sans préjudice d'autres obligations de transparence pour les utilisateurs de systèmes d'IA prévues par le droit de l'Union ou le droit national.

TITRE V

MESURES DE SOUTIEN À L'INNOVATION

Article 53
Bacs à sable réglementaires de l'IA

1 *bis*. Les autorités nationales compétentes peuvent mettre en place des bacs à sable réglementaires de l'IA pour le développement, l'entraînement, la mise à l'essai et la validation de systèmes d'IA innovants sous la surveillance, le contrôle et le soutien directs des autorités nationales compétentes, avant que ces systèmes ne soient mis sur le marché ou mis en service. Ces bacs à sable réglementaires peuvent comprendre des essais en conditions réelles supervisés par les autorités nationales compétentes.

1 *ter*. [supprimé]

1 *quater*. Le cas échéant, les autorités nationales compétentes coopèrent avec d'autres autorités concernées et peuvent permettre la participation d'autres acteurs de l'écosystème de l'IA.

1 *quinquies*. Le présent article n'a pas d'incidence sur d'autres bacs à sable réglementaires établis en vertu du droit national ou du droit de l'Union, y compris dans les cas où les produits ou services qui y sont testés sont liés à l'utilisation de systèmes d'IA innovants. 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.

1. [supprimé]

1 *bis*. [supprimé]

1 *ter*. La mise en place de bacs à sable réglementaires de l'IA au titre du présent règlement vise à contribuer à un ou plusieurs des objectifs suivants:

a) favoriser l'innovation et la compétitivité et faciliter la mise en place d'un écosystème d'IA;
b) faciliter et accélérer l'accès au marché de l'Union pour les systèmes d'IA, en particulier lorsqu'ils sont fournis par des petites et moyennes entreprises (PME), y compris des jeunes entreprises;
c) améliorer la sécurité juridique et contribuer au partage des bonnes pratiques par la coopération avec les autorités participant au bac à sable réglementaire de l'IA en vue d'assurer à l'avenir la conformité avec le présent règlement et, le cas échéant, avec d'autres législations applicables de l'Union et des États membres;
d) contribuer à l'apprentissage réglementaire fondé sur des données probantes.

2. [supprimé]

2 *bis*. L'accès aux bacs à sable réglementaires de l'IA est ouvert à tout fournisseur ou fournisseur potentiel d'un système d'IA qui remplit les critères d'admissibilité et de sélection visés au paragraphe 6, point a), et qui a été sélectionné par les autorités nationales compétentes à l'issue de la procédure de sélection visée au paragraphe 6, point b). Les fournisseurs ou fournisseurs potentiels peuvent également soumettre des demandes en partenariat avec les utilisateurs ou tout autre tiers concerné.

La participation au bac à sable réglementaire de l'IA est limitée à une période adaptée à la complexité et à l'ampleur du projet. Cette période peut être prolongée par l'autorité nationale compétente.

La participation au bac à sable réglementaire de l'IA repose sur un plan spécifique visé au paragraphe 6 du présent article, qui est convenu entre le ou les participants et la ou les autorités nationales compétentes, selon le cas.

3. La participation aux bacs à sable réglementaires de l'IA n'a pas d'incidence sur les pouvoirs des autorités chargées de la surveillance du bac à sable en matière de contrôle et de mesures correctives. Ces autorités exercent leurs pouvoirs de surveillance de manière flexible, 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 de l'IA, dans le but de soutenir l'innovation dans le domaine de l'IA au sein de l'Union.

Sous réserve du respect, par le ou les participants, du plan du bac à sable ainsi que des conditions applicables à leur participation visées au paragraphe 6, point c), et de leur disposition à suivre de bonne foi les orientations fournies par les autorités, aucune amende administrative n'est imposée par les autorités pour violation de la législation applicable de l'Union ou des États membres relative au système d'IA surveillé dans le bac à sable, y compris les dispositions du présent règlement.

4. Les participants demeurent responsables, en vertu de la législation applicable de l'Union et des États membres en matière de responsabilité, de tout préjudice causé durant leur participation à un bac à sable réglementaire.

4 *bis*. À la demande du fournisseur ou du fournisseur potentiel du système d'IA, l'autorité nationale compétente fournit, le cas échéant, une preuve écrite des activités menées avec succès dans le bac à sable. L'autorité nationale 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. La preuve écrite et le rapport de sortie précités pourraient être pris en compte par les autorités de surveillance du marché ou les organismes notifiés, selon le cas, dans le cadre des procédures d'évaluation de la conformité ou des vérifications dans le cadre de la surveillance du marché.

Sous réserve des dispositions relatives à la confidentialité énoncées à l'article 70 et avec l'accord des participants au bac à sable, la Commission européenne et le Comité de l'IA sont autorisés à accéder aux rapports de sortie et en tiennent compte, le cas échéant, dans l'exercice de leurs tâches au titre du présent règlement. Si le participant 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 à l'article 55, paragraphe 3, point b).

4 *ter*. 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.

5. Les autorités nationales compétentes rendent publics des rapports annuels sur la mise en œuvre des bacs à sable réglementaires de l'IA, y compris les bonnes pratiques, les enseignements et les recommandations à suivre sur leur mise en place et, le cas échéant, sur l'application du présent règlement et d'autres actes législatifs de l'Union contrôlés dans le bac à sable. Ces rapports annuels sont soumis au Comité de l'IA, qui met à la disposition du public un résumé de l'ensemble des bonnes pratiques, des enseignements tirés et des recommandations. Cette obligation de rendre publics les rapports annuels 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. La Commission et le Comité de l'IA tiennent compte, le cas échéant, des rapports annuels dans l'exercice de leurs tâches au titre du présent règlement.

5 *ter*. La Commission veille à ce que les informations relatives aux bacs à sable réglementaires de l'IA, y compris celles établies en vertu du présent article, soient disponibles sur la plateforme d'information unique visée à l'article 55, paragraphe 3, point b).

6. Les modalités et les conditions de mise en place et de fonctionnement des bacs à sable réglementaires de l'IA au titre du présent règlement sont adoptées au moyen d'actes d'exécution en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.

Les modalités et les conditions 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, encouragent l'innovation et l'apprentissage réglementaire et tiennent particulièrement compte des circonstances et des capacités particulières des PME participantes, y compris les jeunes entreprises.

Ces actes d'exécution contiennent des principes généraux communs sur les questions suivantes:

a) admissibilité et sélection pour la participation au bac à sable réglementaire de l'IA;
b) procédure 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) conditions applicables aux participants.

7. Lorsque les autorités nationales compétentes envisagent d'autoriser des essais en conditions réelles supervisées dans le cadre d'un bac à sable réglementaire de l'IA établi en vertu du présent article, elles conviennent spécifiquement avec les participants des conditions de ces essais et, en particulier, des garanties appropriées 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.

Article 54

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 cadre du bac à sable réglementaire de l'IA, des données à caractère personnel collectées légalement à d'autres fins peuvent être traitées aux fins du développement, de la mise à l'essai et de l'entraînement de systèmes d'IA innovants dans le bac à sable, sous réserve du respect de l'ensemble des conditions ci-après:

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

      i) [supprimé]

      ii) la sécurité et la santé publiques, y compris la prévention, le contrôle et le traitement des maladies et l'amélioration des systèmes de soins de santé,

      iii) la protection et l'amélioration de la qualité de l'environnement, y compris la transition écologique, l'atténuation du changement climatique et l'adaptation à celui-ci,

      iv) la durabilité énergétique, les transports et la mobilité,

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

      vi) la cybersécurité et la résilience des infrastructures critiques;

   b) les données traitées sont nécessaires pour satisfaire à une ou plusieurs des exigences visées au titre III, chapitre 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 qu'un mécanisme de réponse permettant d'atténuer rapidement ces risques et, le cas échéant, 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 des participants, et seules les personnes autorisées ont accès à ces données;

e) aucune donnée à caractère personnel traitée ne doit être transmise, transférée ou consultée d'une autre manière par d'autres parties ne participant pas au bac à sable, à moins que cette divulgation n'ait lieu conformément au règlement (UE) 2016/679 ou, le cas échéant, au règlement (UE) 2018/1725, et que tous les participants y aient consenti;

f) aucun traitement de données à caractère personnel effectué dans le cadre du bac à sable n'affecte l'application des droits des personnes concernées prévus par le droit de l'Union relatif à la protection des données à caractère personnel, en particulier l'article 22 du règlement (UE) 2016/679 et l'article 24 du règlement (UE) 2018/1725;

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 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.

1 *bis*. À des fins de prévention et de détection d'infractions pénales, ainsi que d'enquêtes et de 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 le droit d'un État membre spécifique ou de l'Union et soumis aux mêmes conditions cumulatives que celles visées au paragraphe 1.

2. Le paragraphe 1 est sans préjudice de la législation de l'Union ou des États membres établissant la base 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 54 bis

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 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 aux dispositions du présent article et au plan d'essais en conditions réelles visé au présent article.

Les éléments détaillés du plan d'essais en conditions réelles sont précisés dans des actes d'exécution adoptés par la Commission conformément à la procédure d'examen visée à l'article 74, paragraphe 2.

La présente disposition est sans préjudice de la législation de l'Union ou des États membres relative aux essais en conditions réelles de systèmes d'IA à haut risque liés aux produits couverts par la législation énumérée à l'annexe II.

2. Les fournisseurs ou fournisseurs potentiels peuvent effectuer, seuls ou en partenariat avec un ou plusieurs utilisateurs 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 l'examen éthique qui peut être exigé par le droit national ou le droit de l'Union.

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 ou les États membres où les essais en conditions réelles doivent être réalisés;

b) l'autorité de surveillance du marché de l'État membre ou des États membres où les essais en conditions réelles doivent être réalisés n'a pas formulé d'objection aux essais dans les 30 jours suivant leur présentation;

c) le fournisseur ou fournisseur potentiel de systèmes d'IA, à l'exception des systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 7, dans les domaines des activités répressives et de la gestion de la migration, de l'asile et 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 base de données de l'Union visée à l'article 60, paragraphe 5 *bis*, avec un numéro d'identification unique à l'échelle de l'Union et les informations indiquées à l'annexe VIII *bis*;

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

e) les données collectées et traitées aux fins des essais en conditions réelles ne sont pas transférées vers des pays situés en dehors de l'Union, à moins que le transfert et le traitement des données n'offrent des garanties équivalentes à celles prévues par le droit de l'Union;

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 12 mois;

g) les personnes appartenant à des groupes vulnérables en raison de leur âge ou de leur handicap physique ou mental sont dûment protégées;

h) [supprimé]

i) lorsqu'un fournisseur ou un fournisseur potentiel organise les essais en conditions réelles en coopération avec un ou plusieurs utilisateurs 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 pertinentes sur la manière d'utiliser le système d'IA visé à l'article 13; le fournisseur ou fournisseur potentiel et le ou les utilisateurs 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 par d'autres législations applicables de l'Union et des États membres;

j) les participants aux essais en conditions réelles ont donné leur consentement éclairé conformément à l'article 54 *ter* 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 le participant;

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

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

5. Tout participant aux essais en conditions réelles, ou son représentant légal, peut, selon le cas, sans encourir de préjudice et sans devoir se justifier, se retirer de l'essai à tout moment, en révoquant son consentement éclairé. Le retrait du consentement éclairé n'affecte pas les activités déjà menées ni l'utilisation des données obtenues sur la base du consentement éclairé du participant avant ce retrait.

6. 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 62 du présent règlement. 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 autrement. 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.

7. Les fournisseurs ou fournisseurs potentiels informent l'autorité nationale de surveillance du marché de l'État membre ou des États membres 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.

8. Le fournisseur et le fournisseur potentiel sont responsables, en vertu de la législation applicable de l'Union et des États membres en matière de responsabilité, de tout préjudice causé durant leur participation à l'essai en conditions réelles.

Article 54 ter

Consentement éclairé à participer aux essais de systèmes d'IA à haut risque 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 54 *bis*, le consentement éclairé est donné librement par le participant avant de prendre part à ces essais et après avoir été dûment informé au moyen d'informations concises, claires, pertinentes et compréhensibles concernant:

i) la nature et les objectifs de l'essai en conditions réelles ainsi que les inconvénients éventuels pouvant être liés à sa participation;

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

iii) les droits et garanties du participant concernant sa participation, en particulier son droit de refuser de participer à l'essai en conditions réelles et son droit de s'en retirer à tout moment sans encourir de préjudice et sans devoir se justifier;

iv) les modalités de demande d'annulation ou de méconnaissance des prévisions, recommandations ou décisions du système d'IA;

v) le numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles conformément à l'article 54 *bis*, 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 au participant ou à son représentant légal.

Article 55

Mesures de soutien pour les opérateurs, en particulier les PME, y compris les jeunes entreprises

1. Les États membres:

a) accordent aux PME, y compris les jeunes entreprises, un accès prioritaire aux bacs à sable réglementaires de l'IA dans la mesure où elles remplissent les critères d'admissibilité et de sélection;

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 entreprises et, le cas échéant, des pouvoirs publics locaux;

c) le cas échéant, établissent un canal de communication spécifique avec les PME, y compris les jeunes entreprises 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.

2. Les intérêts et les besoins spécifiques des PME fournisseuses, y compris les jeunes entreprises, 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. La Commission engage les actions suivantes:

(a) fournir, à la demande du Comité de l'IA, des modèles normalisés pour les domaines couverts par le présent règlement;

(b) mettre au point et tenir 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) organiser des campagnes de communication appropriées pour sensibiliser aux obligations découlant du présent règlement;

(d) évaluer et promouvoir la convergence des meilleures pratiques en matière de procédures de passation de marchés publics en ce qui concerne les systèmes d'IA.

Article 54 bis

Dérogations pour des situations particulières

1. Les obligations prévues à l'article 17 du présent règlement ne s'appliquent pas aux microentreprises telles que définies à l'article 2, paragraphe 3, de l'annexe de la recommandation 2003/361/CE de la Commission concernant la définition des micro, petites et moyennes entreprises, pour autant que ces entreprises n'aient pas d'entreprises partenaires ou d'entreprises liées telles que définies à l'article 3 de la même annexe.

2. Le paragraphe 1 ne peut être interprété comme dispensant ces opérateurs de satisfaire à d'autres exigences et obligations prévues par le présent règlement, y compris celles établies aux articles 9, 61 et 62.

3. Les exigences et obligations applicables aux systèmes d'IA à usage général énoncées à l'article 4 *ter* ne s'appliquent pas aux micro, petites et moyennes entreprises, pour autant que ces entreprises n'aient pas d'entreprises partenaires ou d'entreprises liées telles que définies à l'article 3 de l'annexe de la recommandation 2003/361/CE de la Commission concernant la définition des micro, petites et moyennes entreprises.

TITRE VI

GOUVERNANCE

CHAPITRE 1

COMITE EUROPEEN DE L'INTELLIGENCE ARTIFICIELLE

Article 56

Création et structure du Comité européen de l'intelligence artificielle

1. Un "Comité européen de l'intelligence artificielle" (ci-après le "Comité") est créé.

2. Le Comité est composé d'un représentant par État membre. Le Contrôleur européen de la protection des données participe en qualité d'observateur. La Commission assiste également aux réunions du Comité 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 au cas par cas, lorsque les questions examinées relèvent de leurs compétences.

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

2 *bis bis*. Les États membres veillent à ce que leurs représentants au sein du Comité:

   i) disposent des compétences et pouvoirs pertinents dans leur État membre afin de contribuer activement à l'accomplissement des tâches du Comité visées à l'article 58;

   ii) soient désignés comme point de contact unique vis-à-vis du Comité et, le cas échéant, compte tenu des besoins des États membres, comme point de contact unique pour les parties prenantes;

iii) 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.

3. Les représentants désignés des États membres adoptent le règlement intérieur du Comité 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 et l'organisation des activités du Comité et de ses sous-groupes.

Le Comité établit un sous-groupe permanent servant de plateforme aux parties prenantes pour le conseiller sur toutes les questions liées à la mise en œuvre du présent règlement, y compris sur la préparation des actes d'exécution et des actes délégués. À cette fin, les organisations représentant les intérêts des fournisseurs et des utilisateurs des systèmes d'IA, y compris les PME et les jeunes entreprises, ainsi que les organisations de la société civile, les représentants des personnes concernées, les chercheurs, les organismes de normalisation, les organismes notifiés, les laboratoires et les installations d'expérimentation et d'essai sont invités à participer à ce sous-groupe. Le Comité 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 sur des questions liées respectivement à la surveillance du marché et aux organismes notifiés.

Le Comité peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le cas échéant, les parties prenantes visées à l'alinéa précédent peuvent être invitées à ces sous-groupes ou à des réunions spécifiques de ces sous-groupes en qualité d'observatrices.

3 *bis*. Le Comité est organisé et fonctionne de façon à garantir l'objectivité et l'impartialité de ses activités.

4. Le Comité est présidé par l'un des représentants des États membres. À la demande du président, la Commission convoque les réunions et prépare l'ordre du jour conformément aux tâches du Comité au titre du présent règlement et à son règlement intérieur. La Commission apporte un appui administratif et analytique aux activités du Comité au titre du présent règlement.

Article 57

[supprimé]

Article 58

Tâches du Comité

Le Comité 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 peut notamment:

a) recueillir l'expertise et les bonnes pratiques sur les plans technique et réglementaire et les partager entre les États membres;

b) 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 47, le fonctionnement des bacs à sable réglementaires et les essais en conditions réelles visés aux articles 53, 54 et 54 *bis*;

c) 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 les spécifications techniques ou les normes existantes se rapportant aux exigences énoncées au titre III, chapitre 2,

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

iii) sur l'élaboration de documents d'orientation, y compris les lignes directrices relatives à la fixation des amendes administratives visées à l'article 71;

d) conseiller la Commission sur la nécessité éventuelle de modifier l'annexe III conformément aux articles 4 et 7, en tenant compte des éléments de preuve pertinents disponibles et des dernières évolutions technologiques;

e) conseiller la Commission lors de la préparation des actes délégués ou des actes d'exécution en vertu du présent règlement;

f) coopérer, le cas échéant, avec les organes, groupes d'experts et réseaux compétents de l'UE, 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, des cryptomonnaies, de la protection des consommateurs, de la protection des données et des droits fondamentaux;

g) contribuer et fournir des conseils pertinents à la Commission dans l'élaboration des orientations visées à l'article 58 *bis* ou demander l'élaboration de telles orientations;

h) soutenir les autorités de surveillance du marché dans leur travail et, en coopération et sous réserve de l'accord des autorités de surveillance du marché concernées, promouvoir et soutenir les enquêtes transfrontières de surveillance du marché, y compris en ce qui concerne l'émergence de risques de nature systémique pouvant découler des systèmes d'IA;

i) contribuer à l'évaluation des besoins de formation du personnel des États membres participant à la mise en œuvre du présent règlement;

j) conseiller la Commission sur les questions internationales en matière d'intelligence artificielle.

CHAPITRE 1 *BIS*

LIGNES DIRECTRICES DE LA COMMISSION

Article 58 bis

Lignes directrices de la Commission sur la mise en œuvre du présent règlement

1. À la demande des États membres ou du Comité, ou de sa propre initiative, la Commission émet des lignes directrices sur la mise en œuvre pratique du présent règlement, et notamment sur:

   i) l'application des exigences visées aux articles 8 à 15;

   ii) les pratiques interdites visées à l'article 5;

   iii) la mise en œuvre pratique des dispositions relatives aux modifications substantielles;

   iv) la mise en œuvre pratique des conditions uniformes visées à l'article 6, paragraphe 3, y compris des exemples relatifs aux systèmes d'IA à haut risque visés à l'annexe III;

   v) la mise en œuvre pratique des obligations de transparence prévues à l'article 52;

   vi) la relation entre le présent règlement et d'autres actes législatifs pertinents de l'Union, y compris en ce qui concerne la cohérence de leur application.

Lorsqu'elle publie ces lignes directrices, la Commission accorde une attention particulière aux besoins des PME, y compris les jeunes entreprises, les pouvoirs publics locaux et les secteurs les plus susceptibles d'être affectés par le présent règlement.

CHAPITRE 2

AUTORITES NATIONALES COMPETENTES

Article 59

Désignation des autorités nationales compétentes

1. [supprimé]

2. Chaque État membre établit ou désigne au moins une autorité notifiante et au moins une autorité de surveillance du marché aux fins du présent règlement en tant qu'autorités nationales compétentes. Ces autorités nationales compétentes sont organisées de manière à garantir les principes d'objectivité et d'impartialité de leurs activités et de leurs tâches. 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.

3. Les États membres font connaître à la Commission le nom de la ou des autorités désignées.

4. Les États membres veillent à ce que les autorités nationales compétentes disposent de ressources financières suffisantes, d'équipements techniques adéquats et de ressources humaines dûment qualifiées, pour s'acquitter efficacement des tâches qui leur sont confiées en vertu du présent règlement.

5. Au plus tard le *[un an après l'entrée en vigueur du présent règlement]* et par la suite six mois avant la date limite visée à l'article 84, paragraphe 2, les États membres informent la Commission de l'état des ressources financières, de l'équipement technique et des ressources humaines des autorités nationales compétentes et lui présentent une évaluation de l'adéquation de ces ressources. La Commission transmet ces informations au Comité pour discussion et recommandations éventuelles.

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

7. Les autorités nationales compétentes peuvent fournir des conseils sur la mise en œuvre du présent règlement, notamment adaptés aux PME fournisseuses, y compris les jeunes entreprises. Chaque fois que les autorités nationales compétentes ont l'intention 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 nationales compétentes en vertu de ces actes législatifs de l'Union sont consultées, le cas échéant. Les États membres peuvent également établir un point de contact central pour la communication avec les opérateurs.

8. Lorsque les institutions, agences et organes 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.

TITRE VII

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

Article 60

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 au paragraphe 2 en ce qui concerne les opérateurs pertinents et les systèmes d'IA à haut risque énumérés à l'annexe III, qui sont enregistrés conformément aux articles 51 et 54 *bis*. Lorsqu'elle définit les spécifications fonctionnelles de cette base de données, la Commission consulte le Comité de l'IA.

2. Les données énumérées à l'annexe VIII, partie I, sont introduites dans la base de données de l'Union par les fournisseurs, les représentants autorisés et les utilisateurs concernés, selon le cas, lors de leur enregistrement. Les données énumérées à l'annexe VIII, partie II, points 1 à 11, sont introduites dans la base de données de l'Union par les fournisseurs ou, le cas échéant, par le mandataire, conformément à l'article 51. Les données visées à l'annexe VIII, partie II, point 12, sont générées automatiquement par la base de données en fonction des informations fournies par les utilisateurs concernés conformément à l'article 51, paragraphe 2. Les données énumérées à l'annexe VIII *bis* sont introduites dans la base de données par les fournisseurs ou fournisseurs potentiels conformément à l'article 54 *bis*.

3. [supprimé]

4. La base de données de l'Union ne contient aucune donnée à caractère personnel, à l'exception des informations énumérées à l'annexe VIII, et est sans préjudice de l'article 70.

5. 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 utilisateurs un soutien technique et administratif approprié.

5 *bis*. Les informations contenues dans la base de données de l'UE, enregistrées conformément à l'article 51, sont accessibles au public. Les informations enregistrées conformément à l'article 54 *bis* 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.

TITRE VIII

SURVEILLANCE APRÈS COMMERCIALISATION, PARTAGE D'INFORMATIONS ET SURVEILLANCE DU MARCHÉ

CHAPITRE 1

SURVEILLANCE APRES COMMERCIALISATION

Article 61

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 aux risques du système d'IA à haut risque.

2. Afin de permettre au fournisseur d'évaluer si les systèmes d'IA respectent les exigences énoncées au titre III, chapitre 2, tout au long de leur cycle de vie, le système de surveillance après commercialisation collecte, documente et analyse les données pertinentes, qui peuvent être fournies par les utilisateurs ou collectées via d'autres sources sur les performances des systèmes d'IA à haut risque. Cette obligation ne couvre pas les données opérationnelles sensibles des utilisateurs de systèmes d'IA 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.

4. Pour les systèmes d'IA à haut risque relevant des actes juridiques visés à l'annexe II, section A, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de cette législation, la documentation relative à la surveillance après commercialisation élaborée en vertu de ladite législation est jugée suffisante si le modèle visé au paragraphe 3 est utilisé.

Le premier alinéa 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 concernant leur gouvernance, leurs dispositifs ou leurs processus internes en vertu de la législation de l'Union sur les services financiers.

CHAPITRE 2

PARTAGE D'INFORMATIONS SUR LES INCIDENTS GRAVES

Article 62

Notifications de violations graves

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union notifient tout incident grave aux autorités de surveillance du marché des États membres où a eu lieu cet incident.

Cette notification est effectuée 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 a eu connaissance de l'incident grave.

2. Dès réception d'une notification relative à un incident grave visé à l'article 3, point 44) c), l'autorité de surveillance du marché compétente informe les autorités ou organismes publics nationaux visés à l'article 64, paragraphe 3. La Commission élabore des orientations spécifiques pour faciliter le respect des obligations énoncées au paragraphe 1. Ces orientations sont publiées au plus tard 12 mois après l'entrée en vigueur du présent règlement.

3. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 5, qui sont mis sur le marché ou mis en service par des fournisseurs qui sont des établissements financiers soumis à des exigences concernant leur gouvernance, leurs dispositifs ou leurs processus internes en vertu de la législation de l'Union sur les services financiers, la notification des incidents graves est limitée à ceux qui sont visés à l'article 3, point 44) c).

4. Pour les systèmes d'IA à haut risque qui sont des composants de sécurité de dispositifs, ou qui sont eux-mêmes des dispositifs, relevant du règlement (UE) 2017/745 et du règlement (UE) 2017/746, la notification des incidents graves est limitée à ceux qui sont visés à l'article 3, point 44) c), et est adressée à l'autorité nationale compétente choisie à cette fin par les États membres dans lesquels cet incident s'est produit.

CHAPITRE 3

CONTROLE DE L'APPLICATION

Article 63

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. Toutefois, 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 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 de communication d'informations qui leur incombent en vertu de l'article 34, paragraphe 4, du règlement (UE) 2019/1020, les autorités de surveillance du marché communiquent à la Commission les résultats des activités de surveillance du marché pertinentes au titre du présent règlement.

3. Pour les systèmes d'IA à haut risque, en ce qui concerne les produits auxquels s'appliquent les actes juridiques énumérés à l'annexe II, section A, 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 ou, lorsque les circonstances le justifient et pour autant que la coordination soit assurée, une autre autorité compétente désignée par l'État membre.

Les procédures visées aux articles 65, 66, 67 et 68 du présent règlement ne s'appliquent pas aux systèmes d'IA liés à des produits auxquels s'appliquent les actes juridiques énumérés à l'annexe II, section A, lorsque ces actes juridiques prévoient déjà des procédures ayant le même objectif. En pareils cas, ce sont ces procédures sectorielles qui s'appliquent.

4. 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.

Par dérogation à l'alinéa précédent, lorsque les circonstances le justifient 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 (MSU) institué par le règlement (UE) n° 1024/2013 du Conseil, devraient communiquer sans délai à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt pour les missions de surveillance prudentielle de la Banque centrale européenne telles qu'elles sont définies dans ledit règlement.

5. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1 a), dans la mesure où ils sont utilisés à des fins répressives, et points 6, 7 et 8, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités nationales compétentes pour surveiller les activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration, des autorités compétentes en matière d'asile ou des autorités judiciaires, soit les autorités compétentes en matière de contrôle de la protection des données en vertu de la directive (UE) 2016/680 ou du règlement (UE) 2016/679.. 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 lorsqu'elles agissent dans l'exercice de leurs fonctions judiciaires.

6. Lorsque les institutions, agences et organes 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.

7. 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 des législations d'harmonisation de l'Union énumérées à l'annexe II ou d'autres législations de l'Union susceptibles d'être pertinentes pour les systèmes d'IA à haut risque visés à l'annexe III.

8. 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, le fournisseur accorde 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 du système d'IA à haut risque, y compris, lorsque c'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 d'octroyer un accès à distance.

9. 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 toutes les 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 titre III, chapitre 2, et

b) les procédures d'essai/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.

10. Toute information et documentation obtenue par les autorités de surveillance du marché est traitée dans le respect des obligations de confidentialité énoncées à l'article 70.

11. Toute personne physique ou morale ayant des raisons de penser que des infractions aux dispositions du présent règlement ont été commises peut déposer une réclamation auprès de l'autorité de surveillance du marché compétente.

Conformément à l'article 11, paragraphe 3, point e), et paragraphe 7), point a), du règlement (UE) 2019/1020, les 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 63 bis

Supervision des essais en conditions réelles par les autorités de surveillance du marché

1. Les autorités de surveillance du marché ont la compétence et les pouvoirs nécessaires pour garantir que les essais en conditions réelles sont 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 54, les autorités de surveillance du marché vérifient le respect des dispositions de l'article 54 *bis* 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 54 *bis*, 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 54 *bis* et 54 *ter* ne sont pas remplies, elle peut prendre l'une 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 ou des utilisateurs qu'ils modifient tout aspect des essais en conditions réelles.

4. Lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3 du présent article ou a émis une objection au sens de l'article 54 *bis*, paragraphe 4, point b), la décision ou l'objection est motivée et indique les modalités et conditions 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 du présent article, 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'essai.

Article 64

Pouvoirs des autorités chargées de la protection des droits fondamentaux

1. [supprimé]

2. [supprimé]

3. 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 et à avoir accès à toute documentation créée ou conservée en vertu du présent règlement lorsque l'accès à cette documentation est nécessaire à l'exercice des attributions prévues par 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.

4. Au plus tard 3 mois après l'entrée en vigueur du présent règlement, chaque État membre identifie les autorités ou organismes publics visés au paragraphe 3 et met la liste à la disposition du public. Les États membres notifient la liste à la Commission et à tous les autres États membres et tiennent cette liste à jour.

5. Lorsque la documentation visée au paragraphe 3 ne suffit pas pour établir l'existence d'une violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux, l'autorité ou l'organisme public visé au paragraphe 3 peut présenter à l'autorité de surveillance du marché une demande motivée d'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.

6. Toute information et documentation obtenue par les autorités ou organismes publics nationaux visés au paragraphe 3 en application des dispositions du présent article est traitée dans le respect des obligations de confidentialité énoncées à l'article 70.

Article 65

Procédure applicable aux systèmes d'IA qui présentent un risque au niveau national

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 les risques concernent la santé ou la sécurité ou 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, 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. Lorsque des risques pour les droits fondamentaux sont détectés, l'autorité de surveillance du marché informe également les autorités ou organismes publics nationaux concernés visés à l'article 64, paragraphe 3. Les opérateurs concernés coopèrent, en tant que de besoin, avec les autorités de surveillance du marché et les autres autorités ou organismes publics nationaux visés à l'article 64, paragraphe 3.

   Si, au cours de cette évaluation, l'autorité de surveillance du marché 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.

   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.

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 dans toute l'Union.

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 adopte toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du système d'IA sur son marché national, pour le retirer de ce marché ou pour le rappeler. L'autorité notifie ces mesures à la Commission et aux autres États membres sans retard injustifié.

6. La notification visée au paragraphe 5 contient toutes les précisions disponibles, notamment en ce qui concerne les informations nécessaires pour identifier le système d'IA non conforme, son origine, la nature de la non-conformité alléguée et du risque encouru, ainsi que la nature et la durée des mesures nationales adoptées 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 frappant les pratiques en matière d'intelligence artificielle visées à l'article 5;

a) le non-respect, par le système d'IA à haut risque, des exigences énoncées au titre III, chapitre 2;

b) des lacunes dans les normes harmonisées ou dans les spécifications communes visées aux articles 40 et 41 qui confèrent une présomption de conformité.

c) le non-respect des dispositions énoncées à l'article 52;

d) la non-conformité des systèmes d'IA à usage général avec les exigences et obligations visées à l'article 4 *bis*;

7. Les autorités de surveillance du marché des États membres 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 notification des informations visées au paragraphe 5, aucune objection n'a été émise par un État membre ou par la Commission à l'encontre d'une mesure provisoire prise par un 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 visé à la première phrase du présent paragraphe est ramené à 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'intelligence artificielle visées à l'article 5.

9. Les autorités de surveillance du marché de tous les États membres veillent alors à ce que les mesures restrictives appropriées soient prises sans retard injustifié à l'égard du système d'IA concerné, par exemple son retrait de leur marché.

Article 66

Procédure de sauvegarde de l'Union

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 65, paragraphe 5, ou de 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'intelligence artificielle visées à l'article 5, un État membre soulève des objections à l'encontre d'une mesure prise par un autre État membre ou que la Commission estime que cette mesure est contraire au droit de l'Union, la Commission entame sans tarder des consultations avec l'État membre et le ou les opérateurs concernés et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission décide si la mesure nationale est justifiée ou non dans un délai de 9 mois, ou de 60 jours en cas de non-respect de l'interdiction des pratiques en matière d'intelligence artificielle visées à l'article 5, à compter de la notification visée à l'article 65, paragraphe 5. Elle notifie cette décision à l'État membre concerné. La Commission informe également tous les autres États membres de cette décision.

2. Si la Commission estime que la mesure prise par l'autorité de surveillance du marché de l'État membre concerné est justifiée, les autorités de surveillance du marché de tous les États membres veillent à ce que des mesures restrictives appropriées soient prises à l'égard du système d'IA concerné, telles que le retrait du système d'IA de leur marché, sans retard injustifié, et en informent la Commission. Si la mesure nationale est jugée injustifiée par la Commission, l'autorité de surveillance du marché de 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 dans 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) nº 1025/2012.

Article 67

Systèmes d'IA à haut risque ou systèmes d'IA à usage général conformes qui présentent un risque

1. Lorsque l'autorité de surveillance du marché d'un État membre constate, après avoir réalisé une évaluation au titre de l'article 65, qu'un système d'IA à haut risque ou à usage général conforme au présent règlement comporte néanmoins un risque pour la santé ou la sécurité des personnes ou les droits fondamentaux, elle invite l'opérateur concerné à 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, ou pour le retirer du marché ou le rappeler sans retard injustifié, dans un délai qu'elle peut prescrire.

2. Le fournisseur ou les autres opérateurs concernés s'assurent que des mesures correctives sont prises pour tous les systèmes d'IA concernés qu'ils ont mis à disposition sur le marché dans toute l'Union dans le délai prescrit par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

3. L'État membre informe immédiatement la Commission et les autres États membres. 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 adoptées.

4. La Commission entame sans retard injustifié des consultations avec les États membres et l'opérateur 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 des mesures appropriées.

5. La Commission adresse sa décision aux États membres concernés et en informe tous les autres États membres.

Article 68

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 de conformité a été apposé en violation de l'article 49;

   b) le marquage de conformité n'a pas été apposé;

   c) la déclaration UE de conformité n'a pas été établie;

   d) la déclaration UE de conformité n'a pas été établie correctement;

   e) le numéro d'identification de l'organisme notifié, qui participe à la procédure d'évaluation de la conformité, le cas échéant, n'a pas été apposé.

2. Si le cas de non-conformité visé au paragraphe 1 persiste, l'État membre concerné prend toutes les mesures appropriées 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 du marché.

Article 68 bis

Installations d'essai de l'Union dans le domaine de l'intelligence artificielle

1. La Commission désigne une ou plusieurs installations d'essai de l'Union conformément à l'article 21 du règlement (UE) 2019/1020 dans le domaine de l'intelligence artificielle.

2. Sans préjudice des activités des installations d'essai de l'Union visées à l'article 21, paragraphe 6, du règlement (UE) 2019/1020, les installations d'essai de l'Union visées au paragraphe 1 fournissent également des avis techniques ou scientifiques indépendants à la demande du Comité ou des autorités de surveillance du marché.

Article 68 ter

Réserve centrale d'experts indépendants

1. À la demande du Comité, la Commission arrête, au moyen d'un acte d'exécution, des dispositions relatives à la création, au fonctionnement et au financement d'une réserve centrale d'experts indépendants pour soutenir les activités de contrôle de l'application du présent règlement.

2. Les experts sont sélectionnés par la Commission et inclus dans la réserve centrale sur la base d'une expertise à la pointe des connaissances scientifiques ou techniques en matière d'intelligence artificielle, en tenant dûment compte des domaines techniques couverts par les exigences et obligations prévues par le présent règlement et des activités des autorités de surveillance du marché conformément à l'article 11 du règlement (UE) 2019/1020. La Commission fixe le nombre d'experts de la réserve en fonction des besoins.

3. Les experts peuvent être chargés des tâches suivantes:

a) fournir des conseils aux autorités de surveillance du marché et les soutenir dans leur travail, à leur demande;

b) soutenir les enquêtes transfrontières de surveillance du marché visées à l'article 58, point h), sans préjudice des pouvoirs des autorités de surveillance du marché;

c) conseiller et soutenir la Commission dans l'exercice de ses fonctions dans le cadre de la clause de sauvegarde prévue à l'article 66.

4. Les experts 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. Chaque expert établit une déclaration d'intérêts qui est rendue publique. La Commission met en place des systèmes et des procédures visant à prévenir et gérer efficacement les conflits d'intérêts potentiels.

5. 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 adoptés par la Commission au moyen de l'acte d'exécution visé au paragraphe 1, en tenant compte des objectifs consistant à mettre en œuvre le présent règlement de façon adéquate, d'assurer un bon rapport coût-efficacité et de garantir que tous les États membres aient un accès effectif aux experts.

6. 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 installations d'essai de l'Union conformément à l'article 68 *bis* et par les experts au titre du présent article soit organisée de manière efficace et apporte la meilleure valeur ajoutée possible.

TITRE IX

CODES DE CONDUITE

Article 69

Codes de conduite pour l'application volontaire de certaines exigences

1. La Commission et les États membres facilitent l'élaboration de codes de conduite destinés à encourager l'application volontaire, aux systèmes d'IA autres que les systèmes d'IA à haut risque, d'une ou de plusieurs des exigences énoncées au titre III, chapitre 2, du présent règlement, dans toute la mesure du possible, en tenant compte des solutions techniques disponibles permettant l'application de ces exigences.

2. La Commission et les États membres facilitent l'élaboration de codes de conduite destinés à encourager l'application volontaire à tous les systèmes d'IA d'exigences spécifiques liées, par exemple, à la viabilité environnementale, y compris en ce qui concerne la programmation économe en énergie, à l'accessibilité pour les personnes handicapées, à la participation des parties prenantes à la conception et au développement des systèmes d'IA et à la diversité des équipes de développement sur la base d'objectifs clairs et d'indicateurs de performance clés pour mesurer la réalisation de ces objectifs. La Commission et les États membres facilitent également, lorsqu'il y a lieu, l'élaboration de codes de conduite applicables sur une base volontaire pour les obligations des utilisateurs en ce qui concerne les systèmes d'IA.

3. Les codes de conduite applicables sur une base volontaire peuvent être élaborés par des fournisseurs individuels de systèmes d'IA ou par des organisations les représentant ou par les deux, y compris avec la participation d'utilisateurs et de toute partie intéressée et de leurs organisations représentatives, ou encore, lorsque c'est approprié, par des utilisateurs, en ce qui concerne leurs obligations. 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. La Commission et les États membres prennent en considération les intérêts et les besoins spécifiques des PME fournisseuses, y compris les jeunes entreprises, lorsqu'ils encouragent et facilitent l'élaboration des codes de conduite visés au présent article.

TITRE X

CONFIDENTIALITÉ ET SANCTIONS

Article 70

Confidentialité

1. Les autorités nationales compétentes, les organismes notifiés, la Commission, le Comité et toute autre personne physique ou morale associés à l'application du présent règlement mettent en place, conformément au droit de l'Union ou au droit national, les mesures techniques et organisationnelles appropriées pour garantir la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités, de manière à protéger, en particulier:

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 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre leur obtention, utilisation et divulgation illicites;

b) l'application 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) l'intégrité des procédures pénales ou administratives;

e) l'intégrité des informations classifiées conformément au droit de l'Union ou au droit national.

2. Sans préjudice du paragraphe 1, les informations échangées à titre confidentiel entre les autorités nationales compétentes et entre celles-ci et la Commission ne sont pas divulguées sans consultation préalable de l'autorité nationale compétente dont elles émanent et de l'utilisateur lorsque les systèmes d'IA à haut risque visés à l'annexe III, points 1, 6 et 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, lorsque cette divulgation risquerait de porter atteinte aux intérêts en matière de sécurité nationale et publique. Cette obligation d'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, points 1, 6 et 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 63, paragraphes 5 et 6, 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.

3. Les paragraphes 1 et 2 sont sans effet sur les droits et obligations de la Commission, des États membres et de leurs autorités compétentes ainsi que des organismes notifiés, en matière d'échange d'informations et de diffusion de mises en garde, y compris dans le contexte de la coopération transfrontières, et sur les obligations d'information incombant aux parties concernées en vertu du droit pénal des États membres.

Article 71

Sanctions

1. Dans le respect des conditions établies dans le présent règlement, les États membres déterminent le régime des sanctions, y compris les amendes administratives, applicables aux violations des dispositions du présent règlement et prennent toute mesure nécessaire pour assurer la mise en œuvre correcte et effective de ces sanctions. Ces sanctions doivent être effectives, proportionnées et dissuasives. Elles tiennent compte en particulier de la taille et des intérêts des PME fournisseuses, y compris des jeunes entreprises, ainsi que de leur viabilité économique. Elles tiennent également compte de la question de savoir si l'IA est utilisée dans le cadre d'une activité non professionnelle personnelle.

2. Les États membres informent la Commission sans retard du régime ainsi déterminé et des mesures ainsi prises, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Le non-respect de l'une des interdictions visées à l'article 5 en ce qui concerne les pratiques en matière d'intelligence artificielle fait l'objet d'une amende administrative pouvant aller jusqu'à 30 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 6 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu. Dans le cas des PME, y compris les jeunes entreprises, ces amendes peuvent atteindre 3 % de leur chiffre d'affaires annuel mondial réalisé au cours de l'exercice précédent.

4. Les infractions aux dispositions suivantes liées aux opérateurs et aux organismes notifiés font l'objet d'amendes administratives pouvant aller jusqu'à 20 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 4 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu:

-a) les obligations incombant aux fournisseurs en vertu des articles 4 *ter* et 4 *quater*;

a) les obligations incombant aux fournisseurs en vertu de l'article 16;

b) les obligations incombant à certaines autres personnes en vertu de l'article 23 *bis*;

c) les obligations incombant aux mandataires conformément à l'article 25;

d) les obligations incombant aux importateurs en vertu de l'article 26;

e) les obligations incombant aux distributeurs en vertu de l'article 27;

f) les obligations incombant aux utilisateurs en vertu de l'article 29, paragraphes 1 à 6 *bis*;

g) les exigences et obligations applicables aux organismes notifiés en vertu de l'article 33, de l'article 34, paragraphes 1, 3 et 4, et de l'article 34 *bis*;

h) les obligations de transparence pour les fournisseurs et les utilisateurs conformément à l'article 52.

Dans le cas des PME, y compris les jeunes entreprises, ces amendes peuvent atteindre 2 % de leur chiffre d'affaires annuel mondial réalisé au cours de l'exercice précédent.

5. La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés et aux autorités nationales compétentes en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 10 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu. Dans le cas des PME, y compris les jeunes entreprises, ces amendes peuvent atteindre 1 % de leur chiffre d'affaires annuel mondial réalisé au cours de l'exercice précédent.

6. 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 l'infraction et de ses conséquences;

a *bis*) le fait que la violation a été commise délibérément ou par négligence;

a *ter*) toute mesure prise par l'opérateur pour remédier à l'infraction et en atténuer les éventuels effets négatifs;

b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché dans d'autres États membres au même opérateur pour la même infraction;

b *bis*) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités au même opérateur pour des infractions à d'autres dispositions du droit de l'Union ou du droit national, lorsque ces infractions résultent de la même activité ou omission constituant une infraction pertinente au sens du présent acte;

c) la taille, le chiffre d'affaires annuel et la part de marché de l'opérateur qui commet l'infraction;

d) 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.

7. Chaque État membre établit les règles déterminant si et dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics établis sur son territoire.

8. 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 d'autres organismes, selon le cas prévu dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

9. L'exercice, par l'autorité de surveillance du marché, des pouvoirs que lui confère le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit des États membres, y compris un recours juridictionnel effectif et une procédure régulière.

Article 72

Amendes administratives imposées aux institutions, agences et organes de l'Union

1. Le Contrôleur européen de la protection des données peut imposer des amendes administratives aux institutions, agences et organes 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 l'infraction et de ses conséquences;

   b) la coopération établie avec le Contrôleur européen de la protection des données en vue de remédier à l'infraction 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 ou de l'agence ou de l'organe de l'Union concerné pour le même objet;

   c) toute infraction similaire commise précédemment par l'institution, l'agence ou l'organe de l'Union.

2. Le non-respect de l'une des interdictions visées à l'article 5 en ce qui concerne les pratiques en matière d'intelligence artificielle fait l'objet d'une amende administrative pouvant aller jusqu'à 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 aux articles 5 et 10, fait l'objet d'une amende administrative pouvant aller jusqu'à 250 000 EUR.

4. Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution, à l'agence ou à l'organe 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 font partie des recettes du budget général de l'Union.

TITRE XI

DÉLÉGATION DE POUVOIR ET PROCÉDURE DE COMITÉ

Article 73

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. La délégation de pouvoir visée à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, et à l'article 48, paragraphe 5, est conférée à la Commission pour une durée de cinq ans à partir du [*date d'entrée en vigueur du présent règlement*].

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 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, et à l'article 48, paragraphe 5, 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 n'affecte pas la validité des actes délégués déjà en vigueur.

4. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

5. Tout acte délégué adopté en vertu de l'article 7, paragraphes 1 et 3, de l'article 11, paragraphe 3, de l'article 43, paragraphes 5 et 6, et de l'article 48, paragraphe 5, 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 74

Procédure de 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.

TITRE XII

DISPOSITIONS FINALES

Article 75

Modification du règlement (CE) n° 300/2008

À l'article 4, paragraphe 3, du règlement (CE) nº 300/2008, l'alinéa suivant est ajouté:

"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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...).".

Article 76

Modification du règlement (UE) nº 167/2013

À l'article 17, paragraphe 5, du règlement (UE) nº 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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...)."

Article 77

Modification du règlement (UE) nº 168/2013

À l'article 22, paragraphe 5, du règlement (UE) nº 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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...).".

Article 78

Modification de la directive 2014/90/UE

À l'article 8 de la directive 2014/90/UE, le paragraphe suivant est ajouté:

"4. "4. Pour les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, lorsqu'elle exerce ses activités conformément au paragraphe 1 et lorsqu'elle adopte des spécifications techniques et des normes d'essai conformément aux paragraphes 2 et 3, la Commission tient compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...).".

Article 79

Modification de la directive (UE) 2016/797

À l'article 5 de la directive (UE) 2016/797, le paragraphe suivant est ajouté:

"12. "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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...).".

Article 80

Modification du règlement (UE) 2018/858

À l'article 5 du règlement (UE) 2018/858, le paragraphe suivant est ajouté:

"4. "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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...).".

Article 81

Modification 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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...)."

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) YYY/XX [sur l'intelligence artificielle], il est tenu compte des exigences énoncées au titre III, chapitre 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) YYY/XX [sur l'intelligence artificielle], il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement."

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) YYY/XX [sur l'intelligence artificielle], il est tenu compte des exigences énoncées au titre III, chapitre 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) YYY/XX [sur l'intelligence artificielle], il est tenu compte des exigences énoncées au titre III, chapitre 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) YYY/XX [sur l'intelligence artificielle], il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.".

Article 82

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) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, il est tenu compte des exigences énoncées au titre III, chapitre 2, dudit règlement.

_____

* Règlement (UE) YYY/XX [sur l'intelligence artificielle] (JO ...).".

Article 83

Systèmes d'IA déjà mis sur le marché ou mis en service

1. Le présent règlement ne s'applique pas aux systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe IX qui ont été mis sur le marché ou mis en service avant le [12 mois après la date d'application du présent règlement visée à l'article 85, paragraphe 2], sauf si le remplacement ou la modification de ces actes juridiques entraîne une modification importante de la conception ou de la destination du ou des systèmes d'IA concernés.

   Il est tenu compte des exigences énoncées dans le présent règlement, le cas échéant, lors de l'évaluation de chacun des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe IX devant être effectuée conformément à ces actes respectifs.

2. Le présent règlement s'applique aux systèmes d'IA à haut risque, autres que ceux visés au paragraphe 1, qui ont été mis sur le marché ou mis en service avant le [*date d'application du présent règlement visée à l'article 85, paragraphe 2*], uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leur conception ou de leur destination.

Article 84

Évaluation et réexamen

1. [supprimé]

1 *ter*. La Commission évalue la nécessité de modifier la liste figurant à l'annexe III tous les 24 mois après l'entrée en vigueur du présent règlement et jusqu'à la fin de la période de délégation de pouvoir. Les conclusions de cette évaluation sont présentées au Parlement européen et au Conseil.

2. Au plus tard le [*trois ans après la date d'application du présent règlement visée à l'article 85, paragraphe 2*] 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. Les rapports sont publiés.

3. Les rapports visés au paragraphe 2 accordent une attention particulière aux éléments suivants:

   a) l'état des ressources financières, des équipements techniques et des ressources humaines dont les autorités nationales compétentes ont besoin pour pouvoir mener efficacement à bien les missions qui leur sont dévolues par le présent règlement;

   b) l'état des sanctions, et notamment des amendes administratives visées à l'article 71, paragraphe 1, appliquées par les États membres en cas de violation des dispositions du présent règlement.

4. Au plus tard le [*trois ans après la date d'application du présent règlement visée à l'article 85, paragraphe 2*] et tous les quatre ans par la suite, lorsqu'il y a lieu, la Commission évalue l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées au titre III, chapitre 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, y compris en ce qui concerne la durabilité environnementale.

5. Aux fins des paragraphes 1 *bis* à 4, le Comité, les États membres et les autorités nationales compétentes fournissent des informations à la Commission à la demande de cette dernière.

6. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 *bis* à 4, la Commission tient compte des positions et des conclusions du Comité, du Parlement européen, du Conseil, et d'autres organismes ou sources pertinents.

7. La Commission soumet, si nécessaire, des propositions appropriées visant à modifier le présent règlement, notamment en tenant compte de l'évolution des technologies et à la lumière de l'état d'avancement de la société de l'information.

Article 85

Entrée en vigueur et application

1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Le présent règlement est applicable à partir du [36 mois après l'entrée en vigueur du présent règlement].

3. Par dérogation au paragraphe 2:

   a) le titre III, chapitre 4, et le titre VI sont applicables à partir du [douze mois après l'entrée en vigueur du présent règlement];

   b) l'article 71 est applicable à partir du [douze mois après l'entrée en vigueur du présent règlement].

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le président / La présidente	*Le président / La présidente*

ANNEXE I

[supprimée]

ANNEXE II

LISTE D'ACTES LÉGISLATIFS D'HARMONISATION DE L'UNION

Section A – Liste d'actes législatifs 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) [abrogée par le règlement relatif aux machines et équipements]

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) nº 178/2002 et le règlement (CE) nº 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 actes législatifs d'harmonisation de l'Union

1. Règlement (CE) nº 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) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72).

2. Règlement (UE) nº 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)

3. Règlement (UE) nº 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)

4. 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)

5. 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).

6. 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) nº 715/2007 et (CE) nº 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1) 3.

7. 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) nº 78/2009, (CE) nº 79/2009 et (CE) nº 661/2009 du Parlement européen et du Conseil et les règlements (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010, (UE) nº 1008/2010, (UE) nº 1009/2010, (UE) nº 19/2011, (UE) nº 109/2011, (UE) nº 458/2011, (UE) nº 65/2012, (UE) nº 130/2012, (UE) nº 347/2012, (UE) nº 351/2012, (UE) nº 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

8. 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) nº 2111/2005, (CE) nº 1008/2008, (UE) nº 996/2010, (UE) nº 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) nº 552/2004 et (CE) nº 216/2008 du Parlement européen et du Conseil et le règlement (CEE) nº 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, et de leurs moteurs, hélices, pièces et équipements de contrôle à distance.

ANNEXE III

SYSTÈMES D'IA À HAUT RISQUE VISÉS À L'ARTICLE 6, PARAGRAPHE 3

Dans chacun des domaines énumérés aux points 1 à 8, les systèmes d'IA mentionnés sous chaque lettre sont considérés comme des systèmes d'IA à haut risque au sens de l'article 6, paragraphe 3:

1. Biométrie:

   a) systèmes d'identification biométrique à distance.

2. Infrastructures critiques:

   (a) les 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 et de la fourniture d'eau, de gaz, de chauffage et d'électricité.

3. Éducation et formation professionnelle:

   (a) les systèmes d'IA destinés à être utilisés pour déterminer l'accès, l'admission ou l'affectation de personnes physiques aux établissements ou programmes d'enseignement et de formation professionnelle, à tous les niveaux;

   (b) les 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 ou programmes d'enseignement et de formation professionnelle, à tous les niveaux.

4. Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant:

   (a) les systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, notamment pour le placement d'offres d'emploi ciblées, pour analyser et filtrer les candidatures et pour évaluer les candidats;

(b) l'IA destinée à être utilisée pour prendre des décisions de promotion et de licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalités ou de caractéristiques personnelles et 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:

(a) les 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, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services;

(b) les 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 mis en service par des fournisseurs qui sont des micro ou petites entreprises au sens de l'annexe de la recommandation 20030/361/CE de la Commission, et utilisés exclusivement par ces derniers;

(c) les systèmes d'IA destinés à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par les pompiers et les secours;

(d) les systèmes d'IA destinés à être utilisés à des fins d'évaluation et de tarification en ce qui concerne des personnes physiques en matière d'assurance-vie et d'assurance maladie, à l'exception des systèmes d'IA mis en service par des fournisseurs qui sont des micro ou petites entreprises au sens de l'annexe de la recommandation 2030/361/CE de la Commission, et utilisés exclusivement par ces derniers.

6. Autorités répressives:

(e) les systèmes d'IA destinés à être utilisés par les autorités répressives ou en leur nom pour déterminer la probabilité qu'une personne physique commette une infraction ou récidive, ou le risque qu'une personne physique devienne une victime potentielle d'infractions pénales;

(f) les systèmes d'IA destinés à être utilisés par les autorités répressives ou en leur nom en tant que polygraphes et outils similaires, ou pour analyser l'état émotionnel d'une personne physique;

(g) [supprimé]

(h) les systèmes d'IA destinés à être utilisés par les autorités répressives ou en leur nom pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales;

(i) les systèmes d'IA destinés à être utilisés par les autorités répressives ou en leur nom pour prédire la survenance ou la réitération d'une infraction pénale réelle ou potentielle sur la base du profilage de personnes physiques tel que 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;

(j) les systèmes d'IA destinés à être utilisés par les autorités répressives ou en leur nom pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre d'activités de détection, d'enquête ou de poursuite relatives à des infractions pénales.

(k) [supprimé]

7. Gestion de la migration, de l'asile et des contrôles aux frontières:

(a) les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou en leur nom en tant que polygraphes et outils similaires, ou pour analyser l'état émotionnel d'une personne physique;

(b) les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou en leur nom pour évaluer des risques, y compris des risques pour la sécurité, des risques de migration irrégulière ou des risques pour la santé, posés par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre;

(c) [supprimé]

(d) les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou en leur nom pour examiner les demandes d'asile, de visa et de permis de séjour ainsi que les réclamations connexes, dans le but de vérifier l'éligibilité des personnes physiques qui demandent un statut.

8. Administration de la justice et processus démocratiques:

(a) les systèmes d'IA destinés à être utilisés par les autorités judiciaires ou en leur nom pour interpréter les faits ou la loi et pour appliquer la loi à un ensemble concret de faits.

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, notamment:

   (a) la destination du système, la ou les personnes ayant développé le système, la date et la version du système;

   (b) la manière dont le système d'IA interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels 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 à la mise 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 (logiciel intégré dans du matériel informatique, téléchargeable ou API, par exemple);

   (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 notice d'utilisation pour l'utilisateur et, le cas échéant, des instructions d'installation;

2. une description détaillée des éléments du système d'IA et du processus de développement, notamment:

   (h) 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;

(i) 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 et la pertinence des différents paramètres; la description des résultats attendus du système; les décisions relatives aux compromis éventuels en ce qui concerne les solutions techniques adoptées pour se conformer aux exigences énoncées au titre III, chapitre 2;

(j) 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;

(k) 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);

(l) 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 utilisateurs des résultats produits par les systèmes d'IA, conformément à l'article 13, paragraphe 3, point d);

(m) 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 les fournisseurs continuent à assurer la conformité du système d'IA avec les exigences pertinentes énoncées au titre III, chapitre 2;

(n) les procédures de validation et de test utilisées, y compris les informations sur les données de validation et de test utilisées et leurs principales caractéristiques; les paramètres utilisés pour mesurer l'exactitude, la robustesse, la cybersécurité et le respect des autres exigences pertinentes énoncées au titre III, chapitre 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);

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 des performances, 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 la destination du système; les résultats non intentionnels et les sources de risques prévisibles pour la santé et la sécurité, les droits fondamentaux et la 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 utilisateurs des résultats produits par les systèmes d'IA; les spécifications concernant les données d'entrée, le cas échéant;

4. une description détaillée du système de gestion des risques conformément à l'article 9;

5. une description des modifications pertinentes apportées par le fournisseur au système tout au long de son cycle de vie;

6. 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 titre III, chapitre 2, y compris une liste des autres normes pertinentes et spécifications techniques appliquées;

7. une copie de la déclaration "UE" de conformité;

8. une description détaillée du système en place pour évaluer les performances du système d'IA après la commercialisation conformément à l'article 61, y compris le plan de surveillance après commercialisation visé à l'article 61, paragraphe 3.

ANNEXE V

DÉCLARATION "UE" DE CONFORMITÉ

La déclaration "UE" de conformité prévue à l'article 48 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 est établie sous la seule responsabilité du fournisseur;

4. une déclaration attestant que le système d'IA en question respecte le présent règlement et, le cas échéant, toute autre législation de l'Union applicable prévoyant l'établissement d'une déclaration "UE" de conformité;

5. des références aux éventuelles normes harmonisées pertinentes utilisées ou aux éventuelles autres spécifications communes par rapport auxquelles la conformité est déclarée;

6. 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;

7. 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 la signature.

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 à 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 avec les exigences essentielles pertinentes énoncées au titre III, chapitre 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 61 sont cohérents avec la documentation technique.

ANNEXE VII

CONFORMITÉ FONDÉE SUR L'ÉVALUATION DU SYSTÈME DE GESTION DE LA QUALITÉ ET L'ÉVALUATION DE LA DOCUMENTATION TECHNIQUE

1. Introduction

La conformité fondée sur l'évaluation du système de gestion de la qualité et l'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 la mise à l'essai 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 du 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.

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 de test utilisés, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'interfaces de programmation (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 tests supplémentaires afin de permettre une évaluation correcte de la conformité du système d'IA avec les exigences énoncées au titre III, chapitre 2. Chaque fois que l'organisme notifié n'est pas satisfait des tests effectués par le fournisseur, l'organisme notifié effectue directement des tests adéquats, le cas échéant.

4.5. Les organismes notifiés se voient accorder l'accès au code source du système d'IA sur demande motivée et uniquement lorsque toutes les conditions suivantes sont réunies:

a) l'accès au code source est nécessaire pour évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au titre III, chapitre 2, et

b) les procédures d'essai/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.

4.6. La décision 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 titre III, chapitre 2, un certificat d'évaluation UE de la documentation technique est délivré par l'organisme notifié. L'attestation 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 titre III, chapitre 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.

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, notamment 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 la destination du système d'IA doivent être approuvées 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 ces modifications 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 remplit dûment les 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 et 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 tests supplémentaires des systèmes d'IA pour lesquels un certificat d'évaluation "UE" de la documentation technique a été délivré.

ANNEXE VIII

INFORMATIONS À FOURNIR LORS DE L'ENREGISTREMENT D'OPÉRATEURS ET DE SYSTÈMES D'IA À HAUT RISQUE CONFORMÉMENT À L'ARTICLE 51

Les fournisseurs, les mandataires et les utilisateurs qui sont des autorités, des agences ou des organismes publics fournissent les informations visées à la partie I. Les fournisseurs ou, le cas échéant, les mandataires veillent à ce que les informations concernant leurs systèmes d'IA à haut risque visées à la partie II, points 1 à 11, soient complètes, correctes et tenues à jour. Les informations visées à la partie II, point 12, sont générées automatiquement par la base de données.

Partie I. Informations relatives aux opérateurs (lors de leur enregistrement)

-1. Le type d'opérateur (fournisseur, mandataire ou utilisateur).

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 de l'opérateur, le nom, l'adresse et les coordonnées de cette personne.

Partie II. Informations relatives au système d'IA à haut risque

1. Le nom, l'adresse et les coordonnées du fournisseur.

2. Le nom, l'adresse et les coordonnées du mandataire, le cas échéant.

3. La dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA.

4. La description de la destination du système d'IA.

5. Le statut du système d'IA (sur le marché ou en service; plus mis sur le marché/en service, rappelé).

6. 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.

7. Une copie numérisée du certificat visé au point 6, le cas échéant.

8. Les États membres dans lesquels le système d'IA est ou a été mis sur le marché, mis en service ou mis à disposition dans l'Union.

9. Une copie de la déclaration "UE" de conformité visée à l'article 48.

10. Une notice d'utilisation en format électronique.

11. Un lien URL vers des informations supplémentaires (facultatif).

12. Le nom, l'adresse et les coordonnées des utilisateurs.

ANNEXE VIII *bis*

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 54 *BIS*

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 54 *bis*:

1. Le 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 utilisateurs participant aux essais en conditions réelles.

3. Une brève description du système d'IA, sa destination et 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.

ANNEXE IX

Législation de l'Union relative 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) nº 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) nº 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) Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (CE) nº 767/2008, le règlement (CE) nº 810/2009, le règlement (UE) 2017/2226, le règlement (UE) 2016/399, le règlement nº XX/2018 [règlement sur l'interopérabilité] et la décision 2004/512/CE et abrogeant la décision 2008/633/JAI du Conseil [COM(2018) 302 final]. À mettre à jour une fois le règlement adopté (avril/mai 2021) par les colégislateurs.

3. Eurodac

(a) Proposition modifiée de règlement du Parlement européen et du Conseil relatif à la création d'"Eurodac" pour la comparaison des données biométriques aux fins de l'application efficace du règlement (UE) XXX/XXX [règlement relatif à la gestion de l'asile et de la migration] et du règlement (UE) XXX/XXX [règlement relatif à la réinstallation], pour l'identification des ressortissants de pays tiers ou 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, et modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 [COM(2020) 614 final].

4. Système d'entrée/de sortie

(a) 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) nº 767/2008 et (UE) nº 1077/2011 (JO L 327 du 9.12.2017, p. 20).

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) nº 1077/2011, (UE) nº 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

(a) 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 (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 (JO L 135 du 22.5.2019, p. 85).