COM(2021) 206 final

ASSEMBLÉE NATIONALE

QUINZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2020/2021

Reçu à la Présidence de l'Assemblée nationale
le 08 juin 2021

Enregistré à la Présidence du Sénat
le 08 juin 2021

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT

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

E 15817

COMMISSION
EUROPÉENNE

Bruxelles, le 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

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

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPOSÉ DES MOTIFS

1. CONTEXTE DE LA PROPOSITION

1.1. Justification et objectifs de la proposition

Le présent exposé des motifs accompagne la proposition de règlement établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle). L'intelligence artificielle (IA) recouvre un large champ de technologies en évolution rapide et peut procurer de nombreux avantages économiques et sociétaux dans 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 permettant la prestation de services personnalisés, le recours à l'intelligence artificielle peut produire des résultats bénéfiques sur les plans sociaux et environnementaux et donner des avantages concurrentiels aux entreprises et à l'économie européenne. Une action s'impose tout spécialement dans les secteurs à fort impact, notamment dans la lutte contre le changement climatique, l'environnement et la santé, le secteur public, la finance, la mobilité, les affaires intérieures et l'agriculture. Cela étant, les éléments et techniques qui rendent possibles les bénéfices socio-économiques de l'IA peuvent aussi être à l'origine de nouveaux risques ou de conséquences négatives pour les personnes ou la société. Au vu de la rapidité des évolutions technologiques et des éventuels défis à relever à cet égard, l'UE est déterminée à faire tout son possible pour adopter une approche équilibrée. Il est dans l'intérêt de l'UE de préserver son avance technologique et de faire en sorte que les Européens puissent bénéficier de nouvelles technologies dont le développement et le fonctionnement respectent les valeurs de l'Union et les droits et principes fondamentaux.

La présente proposition met en œuvre l'engagement politique pris par la présidente von der Leyen, qui avait annoncé, dans ses orientations politiques pour la Commission 2019-2024 intitulées «Une Union plus ambitieuse»[1], que la Commission présenterait une proposition législative en vue de l'adoption d'une approche européenne coordonnée relative aux implications humaines et éthiques de l'IA. À la suite de cette annonce, le 19 février 2020, la Commission a publié son livre blanc intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance»[2]. Ce livre blanc définit des options stratégiques poursuivant le double objectif de promouvoir l'adoption de l'IA et de tenir compte des risques associés à certaines utilisations de cette technologie. La présente proposition vise à mettre en œuvre le deuxième objectif, relatif à la mise en place d'un écosystème de confiance, en proposant un cadre juridique pour une IA digne de confiance. La proposition se fonde sur les valeurs de l'UE et les droits fondamentaux, et vise à donner aux personnes et aux autres utilisateurs la confiance d'adopter des solutions fondées sur l'IA, tout en encourageant les entreprises à développer ces solutions. L'IA est un outil qui devrait se mettre au service des personnes et constituer une force positive pour la société afin d'accroître, en définitive, le bien-être de l'être humain. Les règles en matière d'IA qui s'appliquent au marché de l'Union ou qui touchent d'une autre façon les personnes de l'Union devraient par conséquent être axées sur le facteur humain, de manière à ce que les personnes puissent avoir confiance dans le fait que la technologie est utilisée d'une façon sûre et conforme à la loi, notamment en ce qui concerne le respect des droits fondamentaux. À la suite de la publication du livre blanc, la Commission a lancé une large consultation des parties intéressées, qui a suscité un vif intérêt de la part de nombreuses parties prenantes, dont la

[1] https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_fr.pdf

[2] Livre blanc de la Commission intitulé «Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance», COM(2020) 65 final, 2020.

plupart étaient en faveur d'une intervention réglementaire visant à répondre aux défis et préoccupations liés à l'utilisation croissante de l'IA.

La présente proposition répond à des demandes explicites du Parlement européen et du Conseil européen, qui ont lancé plusieurs appels en faveur de l'adoption de mesures législatives visant à assurer le bon fonctionnement du marché intérieur des systèmes d'intelligence artificielle (ci-après les «systèmes d'IA») en mettant en balance les bénéfices et les risques de l'IA à l'échelle de l'Union. Elle vise à contribuer à la réalisation de l'objectif formulé par le Conseil européen[3] de faire de l'Union un acteur mondial de premier plan dans le développement d'une intelligence artificielle sûre, fiable et éthique, et elle garantit la protection de principes éthiques expressément demandée par le Parlement européen[4].

En 2017, le Conseil européen a fait valoir la nécessité de faire preuve d'«un sens de l'urgence face aux tendances émergentes, notamment en ce qui concerne des questions telles que l'intelligence artificielle», tout en veillant à assurer «une protection des données, des droits numériques et des normes éthiques d'un niveau élevé»[5]. Dans ses conclusions de 2019 concernant le plan coordonné pour le développement et l'utilisation de l'intelligence artificielle «made in Europe»[6], le Conseil a en outre souligné l'importance d'assurer le respect intégral des droits des citoyens européens, et il a demandé que la législation pertinente en vigueur fasse l'objet d'un réexamen en vue de s'assurer qu'elle est adaptée aux nouvelles possibilités qu'offre l'intelligence artificielle et aux nouveaux défis qui en découlent. Le Conseil européen a aussi demandé à ce que soit présentée une définition claire des applications d'IA à haut risque[7].

Les dernières conclusions, publiées le 21 octobre 2020, préconisent en outre l'adoption de mesures visant à remédier aux difficultés posées par l'opacité, la complexité, les biais, le degré relatif d'imprévisibilité et le comportement partiellement autonome de certains systèmes d'IA, afin de faire en sorte que ceux-ci soient compatibles avec les droits fondamentaux et de faciliter l'application des règles juridiques[8].

Le Parlement européen a aussi accompli un travail considérable dans le domaine de l'IA. En octobre 2020, il a adopté un certain nombre de résolutions relatives à l'IA, notamment en ce qui concerne les aspects éthiques[9], le régime de responsabilité[10] et les droits de propriété intellectuelle[11]. En 2021, celles-ci ont été suivies par des résolutions relatives à l'utilisation de

---

3 Conseil européen, Réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

4 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 Conseil européen, *Réunion du Conseil européen (19 octobre 2017) – Conclusions*, EUCO 14/17, 2017, p. 8.

6 Conseil de l'Union européenne, *Intelligence artificielle b) Conclusions sur le plan coordonné dans le domaine de l'intelligence artificielle – Adoption*, 6177/19, 2019.

7 Conseil européen, *Réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) – Conclusions*, EUCO 13/20, 2020.

8 Conseil de l'Union européenne, *Conclusions de la présidence – La charte des droits fondamentaux dans le contexte de l'intelligence artificielle et du changement numérique*, 11481/20, 2020.

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

10 Résolution du Parlement européen du 20 octobre 2020 sur un régime de responsabilité civile pour l'intelligence artificielle, 2020/2014(INL).

11 Résolution du Parlement européen du 20 octobre 2020 sur les droits de propriété intellectuelle pour le développement des technologies liées à l'intelligence artificielle, 2020/2015(INI).

l'IA dans les affaires pénales[12] et dans les domaines de l'éducation, de la culture et de l'audiovisuel[13]. Dans sa résolution concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, le Parlement européen recommande expressément à la Commission de proposer des mesures législatives visant à exploiter les possibilités et les avantages offerts par l'IA, mais aussi à garantir la protection des principes éthiques. La résolution comprend un texte de la proposition législative pour un règlement sur les principes éthiques relatifs au développement, au déploiement et à l'utilisation de l'IA, de la robotique et des technologies connexes. Conformément à l'engagement politique pris par la présidente von der Leyen dans ses orientations politiques en ce qui concerne les résolutions adoptées par le Parlement européen au titre de l'article 225 du traité sur le fonctionnement de l'Union européenne (TFUE), la présente proposition tient compte de la résolution du Parlement européen susmentionnée dans le plein respect des principes de proportionnalité et de subsidiarité ainsi que de l'accord «Mieux légiférer».

Dans ce contexte politique, la Commission présente la proposition de cadre réglementaire relatif à l'IA dont les **objectifs spécifiques** sont les suivants:

- veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés 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 des exigences de sécurité applicables aux systèmes d'IA;
- faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et dignes de confiance, et empêcher la fragmentation du marché.

Afin d'atteindre ces objectifs, la présente proposition présente une approche réglementaire horizontale équilibrée et proportionnée de l'IA qui se limite aux exigences minimales nécessaires pour répondre aux risques et aux problèmes liés à l'IA, sans restreindre ou freiner indûment le développement technologique ni augmenter de manière disproportionnée les coûts de mise sur le marché de solutions d'IA. La proposition établit un cadre juridique solide et souple. D'une part, le cadre est complet et conçu pour résister à l'épreuve du temps dans ses choix réglementaires fondamentaux, y compris dans les exigences fondées sur des principes auxquelles les systèmes d'IA devraient se conformer. D'autre part, il met en place un système réglementaire proportionné centré sur une approche réglementaire bien définie fondée sur le risque qui ne crée pas de restrictions commerciales injustifiées, et en vertu duquel l'intervention juridique est adaptée aux situations concrètes dans lesquelles des préoccupations légitimes existent ou sont raisonnablement prévisibles dans un avenir proche. Par ailleurs, le cadre juridique prévoit des mécanismes souples qui permettent de l'adapter de manière dynamique à l'évolution de la technologie et aux nouvelles situations préoccupantes.

---

[12] Projet de rapport du Parlement européen intitulé «L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires dans les affaires pénales», 2020/2016(INI).

[13] Projet de rapport du Parlement européen intitulé «L'intelligence artificielle dans les domaines de l'éducation, de la culture et de l'audiovisuel», 2020/2017(INI). À cet égard, dans sa communication intitulée «Plan d'action en matière d'éducation numérique 2021-2027: Réinitialiser l'éducation et la formation à l'ère du numérique» [COM(2020) 624 final], la Commission prévoit l'élaboration de lignes directrices éthiques sur l'IA et l'utilisation des données dans l'enseignement.

La proposition établit des règles harmonisées pour le développement, la mise sur le marché et l'utilisation de systèmes d'IA dans l'Union suivant une approche proportionnée fondée sur le risque. Elle contient une définition de l'IA unique et à l'épreuve du temps. Certaines pratiques d'IA particulièrement néfastes sont interdites en raison de leur caractère contraire aux valeurs de l'Union, tandis que des restrictions et des garanties spécifiques sont proposées en ce qui concerne certaines utilisations de systèmes d'identification biométrique à distance à des fins répressives. La proposition établit une méthode solide d'évaluation du risque permettant de recenser les systèmes d'IA dits «à haut risque» qui présentent des risques importants pour la santé, la sécurité ou les droits fondamentaux des personnes. Les systèmes d'IA en question devront satisfaire à un ensemble d'exigences obligatoires horizontales garantissant une IA digne de confiance et faire l'objet de procédures d'évaluation de la conformité avant de pouvoir être mis sur le marché de l'Union. Des obligations prévisibles, proportionnées et claires sont aussi imposées aux fournisseurs et aux utilisateurs de ces systèmes afin de garantir la sécurité et le respect de la législation existante en matière de protection des droits fondamentaux tout au long du cycle de vie des systèmes d'IA. Pour certains systèmes d'IA spécifiques, seules des obligations minimales en matière de transparence sont proposées, en particulier lorsque des dialogueurs ou des trucages vidéo ultra-réalistes sont utilisés.

Le contrôle de l'application des règles proposées sera assuré au moyen d'un système de gouvernance au niveau des États membres reposant sur des structures déjà existantes ainsi que d'un mécanisme de coopération au niveau de l'Union accompagnant la création d'un Comité européen de l'intelligence artificielle. Des mesures supplémentaires sont aussi proposées dans le but de soutenir l'innovation, notamment par l'établissement de bacs à sable réglementaires sur l'IA et d'autres mesures visant à réduire la charge réglementaire et à soutenir les petites et moyennes entreprises (PME) et les start-up.

1.2. Cohérence avec les dispositions existantes dans le domaine d'action

Le caractère horizontal de la proposition requiert une cohérence parfaite avec la législation de l'Union existante applicable aux secteurs dans lesquels des systèmes d'IA à haut risque sont déjà utilisés ou sont susceptibles de l'être dans un avenir proche.

La cohérence est aussi assurée avec la charte des droits fondamentaux de l'UE et le droit dérivé de l'Union existant en matière de protection des données, de protection des consommateurs, de non-discrimination et d'égalité entre les femmes et les hommes. La proposition est sans préjudice du règlement général sur la protection des données [règlement (UE) 2016/679] et de la directive en matière de protection des données dans le domaine répressif [directive (UE) 2016/680], et elle complète ces actes avec un ensemble de règles harmonisées concernant la conception, le développement et l'utilisation de certains systèmes d'IA à haut risque ainsi que des restrictions portant sur certaines utilisations de systèmes d'identification biométrique à distance. En outre, la proposition complète le droit de l'Union existant en matière de non-discrimination en prévoyant des exigences spécifiques qui visent à réduire au maximum le risque de discrimination algorithmique, en particulier s'agissant de la conception et de la qualité des jeux de données utilisés pour le développement de systèmes d'IA, assorties d'obligations en ce qui concerne les essais, la gestion des risques, la documentation et le contrôle humain tout au long du cycle de vie des systèmes d'IA. La proposition est sans préjudice de l'application du droit de la concurrence de l'Union.

En ce qui concerne les systèmes d'IA à haut risque constituant des composants de sécurité de produits, la présente proposition sera intégrée dans la législation sectorielle existante en matière de sécurité pour assurer la cohérence, empêcher les doubles emplois et réduire au minimum les charges supplémentaires. S'agissant en particulier des systèmes d'IA à haut risque liés aux produits couverts par les actes du nouveau cadre législatif (les machines, les

dispositifs médicaux et les jouets, par exemple), les exigences applicables aux systèmes d'IA définies dans la présente proposition feront l'objet d'une vérification dans le cadre des procédures existantes d'évaluation de la conformité prévues dans les actes appropriés du nouveau cadre législatif. En ce qui concerne l'interaction entre les exigences, la présente proposition définit des exigences destinées à couvrir les risques en matière de sécurité spécifiques aux systèmes d'IA, tandis que les actes du nouveau cadre législatif visent à garantir la sécurité globale du produit final et peuvent par conséquent contenir des exigences spécifiques relatives à l'intégration sûre d'un système d'IA dans le produit final. La proposition de règlement relatif aux machines et équipements, dont l'adoption est prévue le même jour que la présente proposition, cadre parfaitement avec cette approche. Pour ce qui est des systèmes d'IA à haut risque liés aux produits couverts par des législations spécifiques relevant de l'ancienne approche (l'aviation et les voitures, par exemple), la présente proposition ne devrait pas s'appliquer directement. Cela étant, les exigences ex ante essentielles applicables aux systèmes d'IA à haut risque définies dans la présente proposition devront être prises en considération lors de l'adoption d'actes d'exécution ou d'actes délégués pertinents en vertu des actes correspondants.

En ce qui concerne les systèmes d'IA fournis ou utilisés par des établissements de crédit réglementés, les autorités de surveillance dans le cadre de la législation de l'Union relative aux services financiers devraient être désignées comme les autorités compétentes pour la surveillance des exigences de la présente proposition afin d'assurer un contrôle cohérent du respect des obligations au titre de la présente proposition et de la législation de l'Union relative aux services financiers lorsque les systèmes d'IA sont, dans une certaine mesure, implicitement réglementés par rapport au système de gouvernance interne des établissements de crédit. Pour renforcer davantage la cohérence, la procédure d'évaluation de la conformité et certaines des obligations procédurales des fournisseurs au titre de la présente proposition sont intégrées dans les procédures de la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle[14].

La présente proposition concorde également avec la législation applicable de l'Union en matière de services, notamment s'agissant des services intermédiaires réglementés par la directive 2000/31/CE sur le commerce électronique[15], et avec la récente proposition de la Commission concernant une législation sur les services numériques[16].

En ce qui concerne les systèmes d'IA constituant des composants de systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice géré par l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice (eu-LISA), la proposition ne s'appliquera pas aux systèmes d'IA mis sur le marché ou en service avant qu'une année se soit écoulée à partir de la date d'application du présent règlement, à moins que le remplacement ou la modification des actes législatifs correspondants entraîne un changement important de la conception ou de la destination du ou des systèmes d'IA concernés.

---

14 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 (Texte présentant de l'intérêt pour l'EEE) (JO L 176 du 27.6.2013, p. 338).

15 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).

16 Voir la proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE, COM(2020) 825 final.

1.3. Cohérence avec les autres politiques de l'Union

La proposition s'inscrit dans le cadre plus large d'un ensemble complet de mesures visant à résoudre les problèmes liés au développement et à l'utilisation de l'IA examinés dans le livre blanc sur l'IA. Par conséquent, elle assure la cohérence et la complémentarité avec d'autres initiatives en cours ou prévues de la Commission qui visent également à résoudre ces problèmes, parmi lesquelles la révision de la législation sectorielle sur les produits (la directive «Machines» et la directive relative à la sécurité générale des produits, par exemple) et les initiatives qui traitent des questions de responsabilité liées aux nouvelles technologies, y compris aux systèmes d'IA. Ces initiatives s'appuieront sur la présente proposition et la compléteront afin d'apporter une certaine clarté juridique et de favoriser la mise en place d'un écosystème de confiance pour l'IA en Europe.

La présente proposition est aussi cohérente avec la stratégie numérique globale de la Commission en ce qu'elle contribue à promouvoir des technologies au service des personnes, l'un des trois piliers principaux de l'orientation politique et des objectifs annoncés dans la communication «Façonner l'avenir numérique de l'Europe»[17]. Elle établit un cadre cohérent, efficace et proportionné destiné à garantir que l'IA soit développée de manière à respecter les droits des personnes et à gagner la confiance de ceux-ci, à faire en sorte que l'Europe soit adaptée à l'ère du numérique et à faire des dix prochaines années la **décennie numérique**[18].

En outre, la promotion des innovations engendrées par l'IA est étroitement liée à l'**acte sur la gouvernance des données**[19], à la **directive concernant les données ouvertes**[20] et à d'autres initiatives s'inscrivant dans le cadre de la **stratégie de l'UE pour les données**[21], qui établiront des mécanismes et des services de confiance pour la réutilisation, le partage et la mise en commun des données essentielles au développement de modèles d'IA fondés sur les données de haute qualité.

La proposition renforce aussi considérablement la contribution de l'Union à la définition de normes mondiales et à la promotion d'une IA digne de confiance qui soit conforme aux valeurs et aux intérêts de l'Union. Elle fournit à l'Union une base solide pour dialoguer davantage avec ses partenaires extérieurs, y compris avec des pays tiers et dans le cadre d'échanges internationaux sur des questions liées à l'IA.

2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

2.1. Base juridique

La base juridique de la proposition est en premier lieu l'article 114 du TFUE, qui prévoit l'adoption de mesures destinées à assurer l'établissement et le fonctionnement du marché intérieur.

---

17 Communication de la Commission intitulée «Façonner l'avenir numérique de l'Europe», COM(2020) 67 final.

18 Une boussole numérique pour 2030: l'Europe balise la décennie numérique.

19 Proposition de règlement du Parlement européen et du Conseil sur la gouvernance européenne des données (acte sur la gouvernance des données), COM(2020) 767 final.

20 Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (PE/28/2019/REV/1) (JO L 172 du 26.6.2019, p. 56).

21 Communication de la Commission intitulée «Une stratégie européenne pour les données», COM(2020) 66 final.

La présente proposition fait partie intégrante de la stratégie de l'UE pour le marché unique numérique. Elle a pour objectif principal d'assurer le bon fonctionnement du marché intérieur en établissant des règles harmonisées notamment en ce qui concerne le développement, la mise sur le marché de l'Union et l'utilisation de produits et de services exploitant des technologies de l'IA ou commercialisés en tant que systèmes d'IA autonomes. Certains États membres envisagent déjà de mettre en place des règles nationales destinées à faire en sorte que l'IA soit sûre et à ce qu'elle soit développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Cela donnera vraisemblablement lieu à deux problèmes principaux: i) une fragmentation du marché intérieur sur des éléments essentiels concernant notamment les exigences relatives aux produits et services d'IA, leur commercialisation, leur utilisation, la responsabilité et la surveillance par les pouvoirs publics, et ii) la diminution substantielle de la sécurité juridique tant pour les fournisseurs que pour les utilisateurs de systèmes d'IA quant à la manière dont les règles existantes et nouvelles s'appliqueront à ces systèmes dans l'Union. Compte tenu de la large circulation transfrontière des produits et services, la législation d'harmonisation de l'UE est l'outil le plus approprié pour résoudre ces deux problèmes.

En effet, la proposition définit des exigences obligatoires communes applicables à la conception et au développement de certains systèmes d'IA avant leur mise sur le marché, qui seront mises en œuvre concrètement grâce à des normes techniques harmonisées. La proposition traite aussi de la situation après la mise sur le marché des systèmes d'IA en harmonisant la manière dont les contrôles ex post sont effectués.

En outre, étant donné que la présente proposition contient certaines 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.

2.2. Subsidiarité (en cas de compétence non exclusive)

Du fait de la nature de l'IA, qui repose souvent sur des jeux de données vastes et diversifiés et qui peut être intégrée à tout produit ou service circulant librement au sein du marché intérieur, les objectifs de la présente proposition ne peuvent pas être atteints efficacement par les seuls États membres. En outre, la formation d'un ensemble hétérogène de règles nationales potentiellement divergentes entraverait la circulation fluide des produits et services liés aux systèmes d'IA dans l'UE et serait inefficace pour garantir la sécurité et la protection des droits fondamentaux et des valeurs de l'Union dans les différents États membres. Les approches nationales visant à résoudre les problèmes ne feront que créer une insécurité juridique et des obstacles supplémentaires, et ralentiront la pénétration de l'IA sur le marché.

L'action au niveau de l'Union est plus appropriée pour atteindre les objectifs de la présente proposition en évitant une nouvelle fragmentation du marché unique en cadres nationaux potentiellement contradictoires qui empêcheraient la libre circulation des biens et services intégrant l'IA. Un cadre réglementaire européen solide pour une IA digne de confiance garantira également des conditions de concurrence équitables et protégera toutes les personnes, tout en renforçant la compétitivité et la base industrielle de l'Europe dans le domaine de l'IA. Seule une action commune au niveau de l'Union peut également permettre de protéger la souveraineté numérique de l'Union et de tirer parti des outils et des pouvoirs réglementaires de l'Union pour définir des règles et des normes mondiales.

2.3. Proportionnalité

La proposition s'appuie sur les cadres juridiques existants et est proportionnée et nécessaire pour atteindre ses objectifs, car elle suit une approche fondée sur les risques et n'impose des charges réglementaires que lorsqu'un système d'IA est susceptible de présenter des risques élevés pour les droits fondamentaux et la sécurité. Pour les systèmes d'IA qui ne sont pas à haut risque, seules des obligations de transparence très limitées sont imposées, par exemple en ce qui concerne la fourniture d'informations signalant l'utilisation d'un système d'IA lorsque celui-ci interagit avec des humains. Pour les systèmes d'IA à haut risque, les exigences en matière de données de haute qualité, de documentation, de traçabilité, de transparence, de contrôle humain, d'exactitude et de robustesse se limitent au strict nécessaire pour atténuer les risques pour les droits fondamentaux et la sécurité qui sont associés à l'IA et qui ne sont pas couverts par d'autres cadres juridiques existants. Des normes harmonisées accompagnées d'outils d'orientation et de mise en conformité aideront les fournisseurs et les utilisateurs à respecter les exigences fixées par la proposition et à réduire au maximum leurs frais. Les coûts supportés par les opérateurs sont proportionnés aux objectifs atteints ainsi qu'aux retombées économiques et aux gages de confiance que les opérateurs peuvent attendre de la présente proposition.

2.4. Choix de l'instrument

Le choix d'un règlement en tant qu'instrument juridique se justifie par la nécessité d'une application uniforme des nouvelles règles, notamment en ce qui concerne la définition de l'IA, l'interdiction de certaines pratiques préjudiciables reposant sur l'IA et la classification de certains systèmes d'IA. L'applicabilité directe du règlement, conformément à l'article 288 du TFUE, réduira la fragmentation juridique et facilitera la mise en place d'un marché unique pour des systèmes d'IA licites, sûrs et dignes de confiance. Pour ce faire, le règlement introduira un ensemble harmonisé d'exigences fondamentales en ce qui concerne les systèmes d'IA classés à haut risque ainsi que des obligations pour les fournisseurs et les utilisateurs de ces systèmes devant permettre de mieux protéger les droits fondamentaux et d'assurer une sécurité juridique dans l'intérêt des opérateurs et des consommateurs.

Dans le même temps, les dispositions du règlement ne sont pas excessivement contraignantes et laissent aux États membres la possibilité d'agir à divers niveaux pour les éléments qui ne compromettent pas les objectifs de l'initiative, en particulier l'organisation interne du système de surveillance du marché et l'adoption de mesures visant à favoriser l'innovation.

3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

3.1. Consultations des parties intéressées

La présente proposition est le résultat d'une vaste consultation de toutes les principales parties intéressées, dans le cadre de laquelle les principes généraux et les normes minimales en ce qui concerne la consultation des parties intéressées par la Commission ont été appliqués.

Une **consultation publique en ligne** a été lancée le 19 février 2020 parallèlement à la publication du livre blanc sur l'IA et s'est poursuivie jusqu'au 14 juin 2020. L'objectif de cette consultation était de recueillir des points de vue et des opinions sur le livre blanc. La consultation s'adressait à toutes les parties prenantes intéressées issues du secteur public et du secteur privé, y compris les gouvernements, les autorités locales, les organisations commerciales et non commerciales, les partenaires sociaux, les experts, les universitaires et

les citoyens. Après avoir analysé toutes les réponses reçues, la Commission a publié un résumé des résultats ainsi que les différentes réponses sur son site internet[22].

Au total, 1 215 contributions ont été reçues, dont 352 provenant d'entreprises ou d'organisations/associations professionnelles, 406 de particuliers (92 % de particuliers de l'UE), 152 de représentants d'institutions universitaires/de recherche et 73 d'autorités publiques. La société civile était représentée par 160 répondants (dont 9 organisations de consommateurs, 129 organisations non gouvernementales et 22 syndicats), tandis que 72 répondants ont indiqué appartenir à la catégorie «autres». Sur 352 représentants d'entreprises et de secteurs d'activité, 222 étaient des entreprises et des représentants d'entreprises, dont 41,5 % de micro, petites et moyennes entreprises. Les autres étaient des associations professionnelles. Au total, 84 % des réponses de représentants d'entreprises et de secteurs d'activité provenaient de l'Union des Vingt-sept. En fonction des différentes questions, entre 81 et 598 répondants ont utilisé les espaces de texte libre pour insérer des observations. Plus de 450 documents de prise de position ont été présentés sur le site internet de l'UE consacré aux enquêtes, soit en tant que complément aux réponses au questionnaire (plus de 400), soit en tant que contribution indépendante (plus de 50).

Dans l'ensemble, les parties intéressées s'accordent à reconnaître la nécessité d'agir. Une grande majorité de parties intéressées s'accordent à reconnaître l'existence de vides juridiques ou la nécessité d'une nouvelle législation. Cependant, plusieurs parties intéressées ont invité la Commission à empêcher les doubles emplois, les obligations contradictoires et la réglementation excessive. De nombreuses observations ont souligné l'importance d'un cadre réglementaire neutre sur le plan technologique et proportionné.

Les parties intéressées ont pour la plupart demandé que l'IA soit définie de manière stricte, claire et précise. Au-delà de la nécessité de clarifier le terme «IA», elles ont également souligné l'importance de définir les termes «risque», «à haut risque», «à faible risque», «identification biométrique à distance» et «préjudice».

La plupart des répondants se sont explicitement prononcés en faveur de l'approche fondée sur les risques. Le recours à un cadre fondé sur les risques a été considéré comme préférable à une réglementation globale de tous les systèmes d'IA. Les types de risques et de menaces devraient se fonder sur une approche secteur par secteur et au cas par cas. Les risques devraient aussi être calculés en tenant compte de l'incidence sur les droits et la sécurité.

Les bacs à sable réglementaires pourraient être très utiles pour la promotion de l'IA et ont été accueillis favorablement par certaines parties intéressées, en particulier les associations professionnelles.

Parmi les parties intéressées qui ont formulé un avis sur les modèles de contrôle de l'application, plus de 50 % des répondants, dont de nombreuses associations professionnelles, se sont prononcés en faveur du modèle combinant une auto-évaluation ex ante des risques et un contrôle ex post de l'application des règles pour les systèmes d'IA à haut risque.

3.2. Obtention et utilisation d'expertise

La proposition s'appuie sur deux années d'analyse et de coopération étroite avec les parties intéressées, y compris avec des universitaires, des entreprises, des partenaires sociaux, des organisations non gouvernementales, des États membres et des citoyens. Les travaux préparatoires ont commencé en 2018 avec la mise en place du **groupe d'experts de haut niveau sur l'IA**, composé de manière inclusive et ouverte et réunissant 52 experts renommés

[22] Voir l'ensemble des résultats de la consultation ici.

chargés de conseiller la Commission sur la mise en œuvre de sa stratégie en matière d'IA. En avril 2019, la Commission a soutenu[23] les exigences essentielles énoncées dans les lignes directrices en matière d'éthique pour une IA digne de confiance du groupe d'experts de haut niveau sur l'IA[24], qui avaient été révisées pour tenir compte de plus de 500 soumissions des parties intéressées. Les exigences essentielles se situent dans la ligne d'une approche répandue et commune, comme en témoigne une pléthore de codes et de principes éthiques élaborés par plusieurs organisations privées et publiques en Europe et dans le monde, selon laquelle le développement et l'utilisation de l'IA devraient être guidés par certains principes fondamentaux axés sur des valeurs. La liste d'évaluation pour une IA digne de confiance (ALTAI)[25] a rendu ces exigences opérationnelles dans le cadre d'un processus pilote mené avec plus de 350 organisations.

En outre, la plateforme **Alliance pour l'IA**[26] a été créée, permettant à environ 4 000 parties intéressées de débattre des enjeux technologiques et sociétaux liés à l'IA et de se réunir à l'occasion d'une assemblée annuelle sur l'IA.

Le **livre blanc** sur l'IA a poussé plus loin cette approche inclusive, en permettant de recueillir les observations de plus de 1 250 parties intéressées, dont plus de 450 documents de prise de position supplémentaires. En conséquence, la Commission a publié une analyse d'impact initiale, qui à son tour a suscité plus de 130 observations[27]. **Des ateliers et des événements supplémentaires réunissant les parties intéressées** ont aussi été organisés, et les résultats obtenus ont servi de base à l'analyse d'impact et aux choix stratégiques effectués dans la présente proposition[28]. Une **étude externe** a également été réalisée pour étayer l'analyse d'impact.

3.3. Analyse d'impact

Conformément à sa politique «Mieux légiférer», la Commission a réalisé une analyse d'impact pour la présente proposition, qui a été examinée par le comité d'examen de la réglementation de la Commission. Une réunion s'est tenue le 16 décembre 2020 avec le comité d'examen de la réglementation, à la suite de laquelle celui-ci a émis un avis négatif. L'analyse d'impact a ensuite été révisée en profondeur pour répondre aux observations puis soumise à nouveau au comité d'examen de la réglementation, qui a émis un avis positif le 21 mars 2021. L'annexe 1 de l'analyse d'impact comprend les avis du comité d'examen de la réglementation et les recommandations, et précise comment ces dernières ont été prises en considération.

La Commission a étudié différentes options stratégiques pour atteindre l'objectif général de la proposition, qui est d'**assurer le bon fonctionnement du marché unique**, en créant des

---

23 Commission européenne, *Renforcer la confiance dans l'intelligence artificielle axée sur le facteur humain*, COM(2019) 168.

24 Groupe d'experts de haut niveau sur l'IA, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 2019.

25 Groupe d'experts de haut niveau sur l'IA, *Liste d'évaluation pour une IA digne de confiance (ALTAI) aux fins de l'auto-évaluation*, 2020.

26 L'Alliance pour l'IA est une enceinte pluripartite lancée en juin 2018. Voir https://ec.europa.eu/digital-single-market/en/european-ai-alliance

27 Commission européenne, *Analyse d'impact initiale pour une proposition d'acte législatif du Parlement européen et du Conseil établissant des exigences concernant l'intelligence artificielle*.

28 Pour plus de détails sur toutes les consultations qui ont été menées, voir l'annexe 2 de l'analyse d'impact.

conditions propices au développement et à l'utilisation d'une IA digne de confiance dans l'Union.

Quatre options stratégiques à différents degrés d'intervention réglementaire ont été évaluées:

- **Option nº 1**: instrument législatif de l'UE établissant un système de label non obligatoire;
- **Option nº 2**: une approche ad hoc secteur par secteur;
- **Option nº 3**: instrument législatif horizontal de l'UE suivant une approche proportionnée fondée sur les risques;
- **Option nº 3+**: instrument législatif horizontal de l'UE suivant une approche proportionnée fondée sur les risques + codes de conduite pour les systèmes d'IA qui ne sont pas à haut risque;
- **Option nº 4**: instrument législatif horizontal de l'UE établissant des exigences obligatoires pour tous les systèmes d'IA, indépendamment du niveau de risque qu'ils présentent.

Conformément à la méthode établie par la Commission, chaque option stratégique a été évaluée par rapport aux incidences économiques et sociétales, avec un accent particulier sur les incidences sur les droits fondamentaux. L'option privilégiée est l'option nº 3+, à savoir un cadre réglementaire pour les systèmes d'IA à haut risque uniquement, la possibilité étant donnée à tous les fournisseurs de systèmes d'IA qui ne sont pas à haut risque de suivre un code de conduite. Les exigences porteront sur les données, la documentation et la traçabilité, la fourniture d'informations et la transparence, le contrôle humain, la robustesse et l'exactitude, et elles seraient obligatoires pour les systèmes d'IA à haut risque. Les entreprises désireuses d'introduire des codes de conduite pour d'autres systèmes d'IA le feraient volontairement.

L'option privilégiée a été considérée comme étant appropriée pour atteindre le plus efficacement possible les objectifs de la présente proposition. En exigeant un ensemble restreint mais efficace d'actions de la part des développeurs et des utilisateurs de l'IA, l'option privilégiée limite les risques de violation des droits fondamentaux et de la sécurité des personnes et favorise une surveillance et un contrôle de l'application efficaces grâce à des exigences ciblées applicables uniquement aux systèmes pour lesquels le risque que de telles violations se produisent est élevé. En conséquence, cette option réduit les coûts de mise en conformité au maximum, évitant ainsi un ralentissement injustifié de l'adoption en raison de prix et de frais de mise en conformité plus élevés. Afin de remédier aux éventuels inconvénients pour les PME, cette option comprend plusieurs dispositions visant à aider les PME à se mettre en conformité et à réduire leurs coûts, à savoir notamment la création de bacs à sable réglementaires et l'obligation de tenir compte des intérêts des PME lors de la fixation des redevances liées à l'évaluation de la conformité.

L'option privilégiée renforcera la confiance des personnes dans l'IA, assurera une plus grande sécurité juridique pour les entreprises et dissuadera les États membres de prendre des mesures unilatérales susceptibles de fragmenter le marché unique. La hausse de la demande résultant du degré de confiance plus élevé, l'accroissement de l'offre disponible favorisé par la sécurité juridique et l'absence d'obstacles à la circulation transfrontière des systèmes d'IA sont autant de facteurs qui devraient permettre au marché unique pour l'IA de prospérer. L'UE continuera d'œuvrer à la mise en place d'un écosystème d'IA à croissance rapide pour les services et les produits innovants intégrant des technologies de l'IA ou les systèmes d'IA autonomes, ce qui se traduira par une plus grande autonomie numérique.

Les entreprises ou les autorités publiques qui développent ou utilisent des applications d'IA présentant un risque élevé pour la sécurité ou les droits fondamentaux des personnes devraient se conformer à des exigences et à des obligations spécifiques. Les coûts de mise en conformité correspondants sont estimés entre 6 000 EUR et 7 000 EUR pour la fourniture d'un système d'IA à haut risque moyen d'une valeur d'environ 170 000 EUR d'ici 2025. Des coûts annuels liés au temps consacré à assurer un contrôle humain sont aussi à prendre en charge par les utilisateurs de systèmes d'IA lorsque cela est approprié, en fonction du cas d'utilisation. Ces coûts sont estimés entre 5 000 EUR et 8 000 EUR par an. Les coûts de vérification pourraient représenter entre 3 000 EUR et 7 500 EUR supplémentaires pour les fournisseurs de systèmes d'IA à haut risque. Les entreprises ou les autorités publiques qui développent ou utilisent des applications d'IA qui ne sont pas classées à haut risque ne seraient soumises qu'à des obligations minimales concernant les informations à fournir. Cependant, elles pourraient choisir de se regrouper et d'adopter ensemble un code de conduite pour suivre les exigences appropriées et s'assurer que leurs systèmes d'IA sont dignes de confiance. Les coûts ainsi engendrés seraient tout au plus aussi élevés que pour les systèmes d'IA à haut risque, mais très probablement inférieurs.

Les incidences des options stratégiques sur différentes catégories de parties intéressées (opérateurs économiques/entreprises; organismes d'évaluation de la conformité, organismes de normalisation et autres organismes publics; particuliers/citoyens; chercheurs) sont expliquées en détail à l'annexe 3 de l'analyse d'impact réalisée à l'appui de la présente proposition.

3.4. Réglementation affûtée et simplification

La présente proposition établit des obligations qui s'appliqueront aux fournisseurs et aux utilisateurs de systèmes d'IA à haut risque. Pour les fournisseurs qui développent de tels systèmes et les mettent sur le marché de l'Union, elle créera une sécurité juridique et garantira qu'aucun obstacle ne puisse empêcher la fourniture transfrontière de services et de produits liés à l'IA. Pour les entreprises qui ont recours à l'IA, elle contribuera à instaurer un climat de confiance auprès de leurs clients. Pour les administrations publiques nationales, elle favorisera la confiance du public dans l'utilisation de l'IA et renforcera les mécanismes de contrôle de l'application (en introduisant un mécanisme de coordination européen, en prévoyant des capacités appropriées et en facilitant la vérification des systèmes d'IA avec de nouvelles exigences en matière de documentation, de traçabilité et de transparence). En outre, le cadre envisagera des mesures spécifiques de soutien à l'innovation, y compris des bacs à sable réglementaires et des mesures spécifiques visant à aider les petits utilisateurs et fournisseurs de systèmes d'IA à haut risque à se conformer aux nouvelles règles.

La proposition vise aussi spécifiquement à renforcer la compétitivité et la base industrielle de l'Europe dans le domaine de l'IA. Une cohérence parfaite est assurée avec la législation sectorielle existante de l'Union applicable aux systèmes d'IA (par exemple sur les produits et services), ce qui apportera plus de clarté et simplifiera l'application des nouvelles règles.

3.5. Droits fondamentaux

L'utilisation de l'IA, compte tenu des caractéristiques spécifiques de cette technologie (par exemple l'opacité, la complexité, la dépendance à l'égard des données, le comportement autonome), peut porter atteinte à un certain nombre de droits fondamentaux consacrés dans la charte des droits fondamentaux de l'UE (ci-après la «charte»). La présente proposition vise à garantir un niveau élevé de protection de ces droits fondamentaux et à lutter contre diverses sources de risques grâce à une approche fondée sur les risques clairement définie. Prévoyant un ensemble d'exigences pour une IA digne de confiance et des obligations proportionnées pour tous les participants à la chaîne de valeur, la proposition renforcera et favorisera la

protection des droits protégés par la charte: le droit à la dignité humaine (article 1er), le respect de la vie privée et la protection des données à caractère personnel (articles 7 et 8), la non-discrimination (article 21) et l'égalité entre les femmes et les hommes (article 23). Elle vise à prévenir un effet dissuasif sur les droits à la liberté d'expression (article 11) et à la liberté de réunion (article 12), à préserver le droit à un recours effectif et à accéder à un tribunal impartial, les droits de la défense et la présomption d'innocence (articles 47 et 48), ainsi que le principe général de bonne administration. En outre, la proposition renforcera les droits d'un certain nombre de groupes particuliers dans différents domaines d'intervention, notamment les droits des travailleurs à des conditions de travail justes et équitables (article 31), le droit des consommateurs à un niveau élevé de protection (article 28), les droits de l'enfant (article 24) et l'intégration des personnes handicapées (article 26). Le droit à un niveau élevé de protection de l'environnement et l'amélioration de la qualité de l'environnement (article 37) sont également pertinents, y compris au regard de la santé et de la sécurité des personnes. Les obligations relatives aux essais ex ante, à la gestion des risques et au contrôle humain faciliteront également le respect d'autres droits fondamentaux en réduisant au minimum le risque de décisions erronées ou biaisées assistées par l'IA dans des domaines cruciaux tels que l'éducation et la formation, l'emploi, les services essentiels et l'appareil répressif et judiciaire. Dans les situations où des violations des droits fondamentaux se produiraient encore, les personnes concernées pourront bénéficier de possibilités de recours efficaces rendues possibles grâce à la transparence et à la traçabilité des systèmes d'IA, associées à de solides contrôles ex post.

La présente proposition impose certaines restrictions à la liberté d'entreprise (article 16) et à la liberté des arts et des sciences (article 13) pour des raisons impérieuses d'intérêt général liées à la santé, à la sécurité, à la protection des consommateurs et à la protection d'autres droits fondamentaux («innovation responsable») dans le contexte du développement et de l'utilisation de technologies d'IA à haut risque. Ces restrictions sont proportionnées et limitées au strict nécessaire pour prévenir et atténuer les risques graves pour la sécurité et les éventuelles violations des droits fondamentaux.

Les obligations en matière de renforcement de la transparence ne porteront pas non plus atteinte de manière disproportionnée au droit à la protection de la propriété intellectuelle (article 17, paragraphe 2), puisqu'elles seront limitées aux informations strictement nécessaires pour permettre aux personnes d'exercer leur droit à un recours effectif et à la transparence requise de la part des autorités de contrôle et d'exécution, conformément à leurs mandats. Toute divulgation d'informations sera effectuée conformément à la législation en vigueur dans le domaine concerné, notamment la directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites. Lorsque les autorités publiques et les organismes notifiés doivent avoir accès à des informations confidentielles ou à un code source pour vérifier le respect d'obligations essentielles, ils sont soumis à des obligations de confidentialité contraignantes.

4. INCIDENCE BUDGÉTAIRE

Les États membres devront désigner des autorités de surveillance chargées de la mise en œuvre des exigences législatives. La fonction de surveillance pourrait s'appuyer sur les dispositions existantes, concernant par exemple les organismes d'évaluation de la conformité ou la surveillance du marché, mais exigerait une expertise technologique et des ressources humaines et financières suffisantes. En fonction de la structure préexistante dans chaque État membre, cela pourrait représenter de 1 à 25 équivalents temps plein par État membre.

Une vue d'ensemble détaillée des coûts engendrés est présentée dans la «fiche financière» qui accompagne la présente proposition.

5. AUTRES ÉLÉMENTS

5.1. Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information

Il est essentiel de prévoir un mécanisme solide de suivi et d'évaluation pour garantir que la proposition atteindra efficacement ses objectifs spécifiques. La Commission sera chargée de surveiller les effets de la proposition. Elle établira un système d'enregistrement des applications d'IA autonomes à haut risque dans une base de données publique à l'échelle de l'UE. Cet enregistrement permettra également aux autorités compétentes, aux utilisateurs et à d'autres personnes intéressées de vérifier si le système d'IA à haut risque est conforme aux exigences énoncées dans la proposition et d'exercer un contrôle renforcé sur les systèmes d'IA présentant des risques élevés pour les droits fondamentaux. Pour alimenter cette base de données, les fournisseurs d'IA seront tenus de fournir des informations utiles sur leurs systèmes et sur les mesures d'évaluation de la conformité de ceux-ci.

De plus, les fournisseurs d'IA seront tenus d'informer les autorités nationales compétentes des incidents ou dysfonctionnements graves qui constituent une violation des obligations en matière de droits fondamentaux dès qu'ils auront connaissance de tels faits, ainsi que de tout rappel ou retrait de systèmes d'IA du marché. Les autorités nationales compétentes enquêteront ensuite sur les incidents ou dysfonctionnements, collecteront toutes les informations nécessaires et les transmettront régulièrement à la Commission accompagnées des métadonnées appropriées. La Commission complétera ces informations sur les incidents par une analyse complète de l'ensemble du marché de l'IA.

Elle publiera un rapport d'évaluation et de révision du cadre pour l'IA proposé cinq ans après la date d'entrée en vigueur de celui-ci.

5.2. Explication détaillée des différentes dispositions de la proposition

5.2.1. CHAMP D'APPLICATION ET DÉFINITIONS (TITRE I)

Le **titre I** définit l'objet du règlement et le champ d'application des nouvelles règles qui couvrent la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA. Il énonce également les définitions utilisées dans l'ensemble de l'acte. La définition d'un système d'IA dans le cadre juridique a été pensée pour être aussi neutre que possible sur le plan technologique et pour résister à l'épreuve du temps, en tenant compte de l'évolution rapide des technologies et du marché de l'IA. Afin de fournir la sécurité juridique requise, le titre I est complété par l'annexe I, qui contient une liste détaillée d'approches et de techniques de développement de l'IA à adapter par la Commission à mesure que de nouvelles technologies apparaissent. Des définitions claires sont aussi énoncées pour les acteurs principaux de la chaîne de valeur de l'IA tels que les fournisseurs et les utilisateurs de systèmes d'IA. Celles-ci couvrent à la fois les opérateurs publics et les opérateurs privés afin de garantir des conditions de concurrence équitables.

5.2.2. PRATIQUES D'INTELLIGENCE ARTIFICIELLE INTERDITES (TITRE II)

Le **titre II** établit la liste des pratiques d'IA interdites. Le règlement suit une approche fondée sur les risques et introduit une distinction entre les utilisations de l'IA qui créent i) un risque inacceptable, ii) un risque élevé et iii) un risque faible ou minimal. La liste des pratiques interdites figurant au titre II comprend tous les systèmes d'IA dont l'utilisation est considérée comme inacceptable car contraire aux valeurs de l'Union, par exemple en raison de violations des droits fondamentaux. Les interdictions portent sur les pratiques qui présentent un risque

important de manipuler des personnes par des techniques subliminales agissant sur leur inconscient, ou d'exploiter les vulnérabilités de groupes vulnérables spécifiques tels que les enfants ou les personnes handicapées afin d'altérer sensiblement leur comportement d'une manière susceptible de causer un préjudice psychologique ou physique à la personne concernée ou à une autre personne. D'autres pratiques de manipulation ou d'exploitation visant les adultes et susceptibles d'être facilitées par des systèmes d'IA pourraient être couvertes par les actes existants sur la protection des données, la protection des consommateurs et les services numériques, qui garantissent que les personnes physiques sont correctement informées et peuvent choisir librement de ne pas être soumises à un profilage ou à d'autres pratiques susceptibles de modifier leur comportement. La proposition interdit également la notation sociale fondée sur l'IA effectuée à des fins générales par les autorités publiques. Enfin, l'utilisation de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives est également interdite, à moins que certaines exceptions limitées ne s'appliquent.

5.2.3. SYSTÈMES D'IA À HAUT RISQUE (TITRE III)

Le **titre III** contient des règles spécifiques applicables aux systèmes d'IA qui présentent un risque élevé pour la santé, la sécurité ou les droits fondamentaux des personnes physiques. Selon une approche fondée sur les risques, ces systèmes d'IA à haut risque sont autorisés sur le marché européen sous réserve du respect de certaines exigences obligatoires et d'une évaluation ex ante de la conformité. La classification d'un système d'IA comme étant à haut risque repose sur la finalité du système d'IA, conformément à la législation existante en matière de sécurité des produits. Par conséquent, la classification d'un système d'IA comme étant à haut risque ne dépend pas seulement de la fonction remplie par le système d'IA, mais également de la finalité et des modalités spécifiques pour lesquelles ce système est utilisé.

Le chapitre 1 du titre III énonce les règles de classification et définit deux grandes catégories de systèmes d'IA à haut risque:

- les systèmes d'IA destinés à être utilisés en tant que composants de sécurité de produits, qui font l'objet d'une évaluation ex ante de la conformité par un tiers;
- les autres systèmes d'IA autonomes qui soulèvent principalement des questions quant au respect des droits fondamentaux, qui sont explicitement énumérés à l'annexe III.

La liste de systèmes d'IA à haut risque de l'annexe III comprend un nombre limité de systèmes d'IA pour lesquels les risques recensés se sont déjà matérialisés ou sont susceptibles de se matérialiser dans un avenir proche. Pour garantir que le règlement puisse être adapté aux nouvelles utilisations et applications de l'IA, la Commission peut étendre la liste des systèmes d'IA à haut risque utilisés dans certains domaines prédéfinis, en appliquant un ensemble de critères et une méthode d'évaluation des risques.

Le chapitre 2 définit les exigences légales applicables aux systèmes d'IA à haut risque en ce qui concerne les données et la gouvernance des données, la documentation et la tenue de registres, la transparence et la fourniture d'informations aux utilisateurs, le contrôle humain, la robustesse, l'exactitude et la sécurité. Les exigences minimales proposées correspondent déjà aux méthodes les plus modernes utilisées par de nombreux opérateurs diligents. Elles sont le résultat de deux années de travaux préparatoires, basés sur les lignes directrices en matière d'éthique du groupe d'experts de haut niveau sur l'IA[29] et menés par plus de

[29] Groupe d'experts de haut niveau sur l'IA, *Lignes directrices en matière d'éthique pour une IA digne de confiance*, 2019.

350 organisations[30]. De plus, elles cadrent largement avec les autres recommandations et principes internationaux, ce qui garantit la compatibilité du cadre pour l'IA proposé avec les cadres adoptés par les partenaires commerciaux internationaux de l'UE. Les solutions techniques concrètes pour se conformer à ces exigences peuvent être fournies par des normes ou par d'autres spécifications techniques, ou être élaborées d'une autre manière sur la base de connaissances générales en ingénierie ou en science, selon l'appréciation du fournisseur du système d'IA. Cette flexibilité est particulièrement importante, car elle permet aux fournisseurs de systèmes d'IA de choisir la marche à suivre pour se conformer aux exigences, en tenant compte des avancées les plus récentes et des progrès technologiques et scientifiques dans ce domaine.

Le chapitre 3 impose un ensemble clair d'obligations horizontales aux fournisseurs de systèmes d'IA à haut risque. Des obligations proportionnées sont également imposées aux utilisateurs et aux autres participants situés tout au long de la chaîne de valeur de l'IA (par exemple les importateurs, les distributeurs et les mandataires).

Le chapitre 4 définit le cadre dans lequel les organismes notifiés doivent être associés en tant que tiers indépendants aux procédures d'évaluation de la conformité, tandis que le chapitre 5 décrit en détail les procédures d'évaluation de la conformité à suivre pour chaque type de système d'IA à haut risque. L'approche en matière d'évaluation de la conformité vise à réduire au minimum la charge pour les opérateurs économiques ainsi que pour les organismes notifiés, dont la capacité doit être progressivement augmentée au fil du temps. Les systèmes d'IA destinés à être utilisés en tant que composants de sécurité de produits réglementés par des actes du nouveau cadre législatif (les machines, les jouets et les dispositifs médicaux, par exemple) seront soumis aux mêmes mécanismes ex ante et ex post de mise en conformité et de contrôle de l'application que ceux applicables aux produits dont ils sont des composants. La principale différence est que les mécanismes ex ante et ex post garantiront le respect non seulement des exigences établies par la législation sectorielle, mais également des exigences établies par le présent règlement.

En ce qui concerne les systèmes d'IA autonomes à haut risque visés à l'annexe III, un nouveau système de mise en conformité et de contrôle de l'application sera mis en place. Ce système suit le modèle des actes du nouveau cadre législatif, dont la mise en œuvre fait l'objet de contrôles internes effectués par les fournisseurs, sauf pour les systèmes d'identification biométrique à distance, qui devraient être soumis à une évaluation de la conformité réalisée par un tiers. Une évaluation ex ante complète de la conformité, réalisée au moyen de contrôles internes et assortie d'un contrôle ex post renforcé de l'application, pourrait être une solution efficace et raisonnable pour ces systèmes, compte tenu du stade précoce de l'intervention réglementaire et du fait que le secteur de l'IA produit de nombreuses innovations et que les compétences techniques nécessaires à la vérification commencent seulement à être acquises. Une évaluation au moyen de contrôles internes pour les systèmes d'IA autonomes à haut risque exigerait une évaluation ex ante complète, efficace et correctement documentée de la conformité avec toutes les exigences du règlement ainsi que de la conformité avec les exigences en matière de robustesse, de qualité, de systèmes de gestion des risques et de surveillance après commercialisation. Une fois que le fournisseur a effectué l'évaluation de la conformité appropriée, il devrait enregistrer ces systèmes d'IA autonomes à haut risque dans une base de données de l'UE qui sera gérée par la Commission pour accroître la transparence, améliorer le contrôle public et renforcer le contrôle ex post par les autorités compétentes. En revanche, pour des raisons de cohérence avec la législation existante en matière de sécurité

[30] Elles ont également été approuvées par la Commission dans sa communication de 2019 sur l'approche de l'IA axée sur le facteur humain.

des produits, les évaluations de la conformité des systèmes d'IA utilisés en tant que composants de sécurité de produits seront effectuées selon un système doté de procédures d'évaluation de la conformité par des tiers déjà établi dans le cadre de la législation sectorielle appropriée en matière de sécurité des produits. En cas de modification substantielle des systèmes d'IA, ceux-ci devront faire l'objet de réévaluations ex ante de la conformité (notamment lorsque les modifications vont au-delà de ce qui est prédéterminé par le fournisseur dans sa documentation technique et vérifié lors de l'évaluation ex ante de la conformité).

5.2.4. OBLIGATIONS DE TRANSPARENCE POUR CERTAINS SYSTÈMES D'IA (TITRE IV)

Le **titre IV** impose des obligations à certains systèmes d'IA en raison des risques spécifiques de manipulation qu'ils présentent. Les obligations de transparence s'appliqueront aux systèmes qui i) interagissent avec les humains, ii) sont utilisés pour détecter des émotions ou déterminer l'association avec des catégories (sociales) sur la base de données biométriques, ou iii) générer ou manipuler des contenus (trucages vidéo ultra-réalistes). Lorsque des personnes interagissent avec un système d'IA ou que leurs émotions ou caractéristiques sont reconnues par des moyens automatisés, elles doivent en être informées. Si un système d'IA est utilisé pour générer ou manipuler des images ou des contenus audio ou vidéo afin de produire un résultat qui ressemble sensiblement à un contenu authentique, il devrait être obligatoire de déclarer que le contenu est généré par des moyens automatisés, sauf pour certaines finalités légitimes faisant l'objet d'exceptions (domaine répressif, liberté d'expression). Cette obligation laisse la possibilité aux personnes de prendre des décisions en connaissance de cause ou de se désengager d'une situation donnée.

5.2.5. MESURES DE SOUTIEN À L'INNOVATION (TITRE V)

Le **titre V** contribue à la réalisation de l'objectif consistant à créer un cadre juridique propice à l'innovation et résistant à l'épreuve du temps et aux perturbations. À cette fin, il encourage les autorités nationales compétentes à mettre en place des bacs à sable réglementaires et établit un cadre de base en matière de gouvernance, de surveillance et de responsabilité. Les bacs à sable réglementaires sur l'IA offrent un environnement contrôlé pour mettre à l'essai des technologies novatrices sur une durée limitée sur la base d'un plan d'essai convenu avec les autorités compétentes. Le titre V contient également des mesures visant à réduire la charge réglementaire pesant sur les PME et les start-up.

5.2.6. GOUVERNANCE ET MISE EN ŒUVRE (TITRES VI, VII ET VII)

Le **titre VI** met en place les systèmes de gouvernance au niveau de l'Union et au niveau national. Au niveau de l'Union, la proposition institue un Comité européen de l'intelligence artificielle (ci-après le «Comité»), composé de représentants des États membres et de la Commission. Le Comité facilitera la mise en œuvre fluide, efficace et harmonisée du présent règlement en contribuant à la coopération efficace entre les autorités de contrôle nationales et la Commission et en fournissant des conseils et une expertise à la Commission. Il recensera également les meilleures pratiques et les diffusera dans les États membres.

Au niveau national, les États membres devront désigner une ou plusieurs autorités nationales compétentes et, parmi elles, l'autorité de contrôle nationale chargée de contrôler l'application et la mise en œuvre du règlement. Le Contrôleur européen de la protection des données agira en tant qu'autorité compétente pour la surveillance des institutions, agences et organes de l'Union lorsqu'ils relèvent du champ d'application du présent règlement.

Le **titre VII** vise à faciliter le travail de suivi de la Commission et des autorités nationales par la création d'une base de données à l'échelle de l'UE pour les systèmes d'IA autonomes à

haut risque qui soulèvent principalement des questions quant au respect des droits fondamentaux. La base de données sera gérée par la Commission et alimentée par les fournisseurs de systèmes d'IA, qui seront tenus d'enregistrer leurs systèmes avant de les mettre sur le marché ou de les mettre en service d'une autre manière.

Le **titre VIII** énonce les obligations en matière de surveillance et d'établissement de rapports pour les fournisseurs de systèmes d'IA en ce qui concerne la surveillance après commercialisation et l'établissement de rapports et les enquêtes sur les incidents et les dysfonctionnements liés à l'IA. Les autorités de surveillance du marché seraient aussi chargées de contrôler le marché et d'enquêter sur le respect des obligations et des exigences pour tous les systèmes d'IA à haut risque déjà mis sur le marché. Les autorités de surveillance du marché seraient investies de tous les pouvoirs qui leur sont conférés en vertu du règlement (UE) 2019/1020 sur la surveillance du marché. Le contrôle ex post de l'application devrait garantir qu'une fois le système d'IA mis sur le marché, les autorités publiques ont les pouvoirs et les ressources nécessaires pour intervenir au cas où les systèmes d'IA généreraient des risques inattendus, qui justifient une action rapide. Les autorités contrôleront également le respect par les opérateurs des obligations pertinentes qui leur incombent au titre du règlement. La proposition ne prévoit pas la création automatique d'organes ou autorités supplémentaires au niveau des États membres. Les États membres peuvent donc désigner (et s'appuyer sur l'expertise) des autorités sectorielles existantes, qu'ils investiraient également des pouvoirs de suivi et de contrôle de l'application des dispositions du règlement.

Cela est sans préjudice du système existant et de l'attribution des pouvoirs de contrôle ex post du respect des obligations relatives aux droits fondamentaux dans les États membres. Lorsque cela est nécessaire à leur mandat, les autorités existantes de surveillance et de contrôle de l'application seront également habilitées à demander et à avoir accès à toute documentation conservée en vertu du présent règlement et, le cas échéant, à demander aux autorités de surveillance du marché d'organiser des essais du système d'IA à haut risque par des moyens techniques.

5.2.7. CODES DE CONDUITE (TITRE IX)

Le **titre IX** établit un cadre pour la création de codes de conduite visant à encourager les fournisseurs de systèmes d'IA ne présentant pas de risque élevé à appliquer volontairement les exigences obligatoires pour les systèmes d'IA à haut risque (telles qu'énoncées au titre III). Les fournisseurs de systèmes d'IA ne présentant pas de risque élevé peuvent créer et mettre en œuvre eux-mêmes les codes de conduite. Ces codes peuvent aussi inclure des engagements volontaires liés, 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.

5.2.8. DISPOSITIONS FINALES (TITRES X, XI ET XII)

Le **titre X** met l'accent sur l'obligation pour toutes les parties de respecter la confidentialité des informations et des données et définit des règles pour l'échange d'informations obtenues lors de la mise en œuvre du règlement. Le titre X comprend également des mesures visant à garantir la mise en œuvre efficace du règlement grâce à l'application de sanctions effectives, proportionnées et dissuasives en cas de violation des dispositions.

Le **titre XI** définit les règles relatives à l'exercice de la délégation et aux compétences d'exécution. La proposition habilite la Commission à adopter, le cas échéant, des actes d'exécution pour assurer une application uniforme du règlement ou des actes délégués pour mettre à jour ou compléter les listes des annexes I à VII.

Le **titre XII** contient une obligation pour la Commission d'évaluer régulièrement la nécessité d'une mise à jour de l'annexe III et de préparer des rapports réguliers sur l'évaluation et la révision du règlement. Il établit également des dispositions finales, y compris une période transitoire différenciée pour la date initiale d'applicabilité du règlement visant à faciliter sa mise en œuvre harmonieuse pour toutes les parties concernées.

2021/0106 (COD)

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

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[31],

vu l'avis du Comité des régions[32],

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(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 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

[31] JO C […] du […], p. […].
[32] JO C […] du […], p. […].

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) Dans le même temps, 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, le présent règlement contribue à la réalisation de l'objectif formulé par le Conseil européen[33] 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[34].

(6) Il convient de définir clairement la notion de système d'IA afin de garantir une 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 du logiciel, en particulier la capacité, pour un ensemble donné

[33] Conseil européen, Réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) – Conclusions, EUCO 13/20, 2020, p. 6.

[34] 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).

d'objectifs définis par l'homme, à générer des résultats tels que du contenu, 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. 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 être incorporé dans celui-ci (non intégré). La définition des systèmes d'IA devrait être complétée par une liste de techniques et d'approches spécifiques utilisées pour le développement de ces systèmes, laquelle devrait être mise à jour, pour tenir compte de l'évolution du marché et de la technologie, par l'adoption d'actes délégués de la Commission modifiant ladite liste.

(7) La notion de données biométriques utilisée dans le présent règlement est conforme à la notion de données biométriques telle que définie à l'article 4, paragraphe 14, du règlement (UE) 2016/679 du Parlement européen et du Conseil[35], à l'article 3, paragraphe 18, du règlement (UE) 2018/1725 du Parlement européen et du Conseil[36] et à l'article 3, paragraphe 13, de la directive (UE) 2016/680 du Parlement européen et du Conseil[37] et devrait être interprétée de manière cohérente avec celle-ci.

(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 à distance par la comparaison des données biométriques d'une personne avec les données biométriques contenues dans une base de données de référence, sans savoir au préalable si la personne ciblée sera présente et pourra être identifiée, quels que soient la technologie, les processus ou les types de données biométriques utilisés. Compte tenu de leurs caractéristiques et modes d'utilisation différents, ainsi que des différents risques encourus, il convient de faire une distinction entre les systèmes d'identification biométrique à distance «en temps réel» et «a posteriori». 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

---

35 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).

36 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).

37 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).

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 être comprise comme désignant tous les lieux physiques accessibles au public, qu'ils appartiennent à un propriétaire privé ou public. Par conséquent, cette notion ne couvre pas les lieux qui sont privés par nature et qui en temps normal ne sont pas librement accessibles à des tiers, y compris aux autorités répressives, sauf si ces tiers ont été spécifiquement invités ou autorisés, comme les logements, les clubs privés, les bureaux, les entrepôts et les usines. Les espaces en ligne ne sont pas non plus couverts, car ce ne sont pas des espaces physiques. Cependant, le simple fait que l'accès à un espace donné soit soumis à certaines conditions, telles que des billets d'entrée ou des restrictions d'âge, ne signifie pas que l'espace n'est pas accessible au public au sens du présent règlement. Par conséquent, outre les espaces publics tels que les rues, les parties pertinentes de bâtiments du secteur public et la plupart des infrastructures de transport, les espaces tels que les cinémas, les théâtres, les magasins et les centres commerciaux sont normalement aussi accessibles au public. Le caractère accessible au public ou non 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 et dont les effets ont une incidence sur des personnes physiques situées dans l'Union. 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 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.

(12) Le présent règlement devrait également s'appliquer aux institutions, organismes, organes et agences de l'Union lorsqu'ils agissent en tant que fournisseurs ou utilisateurs d'un système d'IA. Les systèmes d'IA exclusivement développés ou utilisés à des fins militaires devraient être exclus du champ d'application du présent règlement lorsque cette utilisation relève de la compétence exclusive de la politique étrangère et de sécurité commune régie par le titre V du traité sur l'Union européenne (TUE). 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 (telle que modifiée par la législation sur les services numériques).

(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 tous les 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) La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA destinés à altérer les comportements humains d'une manière qui est susceptible de causer un préjudice psychologique ou physique devraient être interdites. De tels systèmes d'IA déploient des composants subliminaux que les personnes ne peuvent pas percevoir, ou exploitent les vulnérabilités des enfants et des personnes vulnérables en raison de leur âge ou de leurs handicaps physiques ou mentaux. Ces systèmes ont pour finalité d'altérer substantiellement le comportement d'une personne d'une manière qui cause ou est susceptible de causer un préjudice à cette personne ou à une autre personne. La finalité ne peut être présumée si l'altération du comportement humain résulte de facteurs externes au système d'IA, qui échappent au contrôle du fournisseur ou de l'utilisateur. Les activités de recherche à des fins légitimes liées à de tels systèmes d'IA ne devraient pas être entravées par l'interdiction, tant que ces activités ne consistent pas à utiliser le système d'IA dans des relations homme-machine qui exposent des personnes physiques à un préjudice et tant qu'elles sont menées dans le respect de normes éthiques reconnues pour la recherche scientifique.

(17) Les systèmes d'IA permettant la notation sociale des personnes physiques à des fins générales par les autorités publiques ou pour le compte de celles-ci 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 la fiabilité des personnes physiques en fonction de leur comportement social dans plusieurs contextes ou de caractéristiques personnelles ou de personnalité connues ou prédites. 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. Il convient donc d'interdire de tels systèmes d'IA.

(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 trois situations précisément répertoriées et 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[38] du Conseil 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.

[38] 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 trois situations précisément répertoriées et 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 trois 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, sauf 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 que 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 telle que réglementée par le présent règlement, y compris lorsque ces systèmes sont utilisés par les autorités compétentes dans des espaces accessibles au public à des fins autres que répressives, devrait continuer d'être conforme à toutes les exigences découlant de l'article 9, paragraphe 1, du règlement (UE) 2016/679, de l'article 10, paragraphe 1, du règlement (UE) 2018/1725 et de l'article 10 de la directive (UE) 2016/680, selon le cas.

(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 et 3, 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 et 3, 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 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 des systèmes 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 tels que 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[39], du règlement (UE) nº 167/2013 du Parlement européen et du Conseil[40], du règlement (UE) nº 168/2013 du Parlement européen et du Conseil[41], de la directive 2014/90/UE du Parlement européen et du Conseil[42], de la directive (UE) 2016/797 du Parlement européen et du Conseil[43], du

39 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).

40 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).

41 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).

42 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).

43 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).

règlement (UE) 2018/858 du Parlement européen et du Conseil[44], du règlement (UE) 2018/1139 du Parlement européen et du Conseil[45] ou du règlement (UE) 2019/2144 du Parlement européen et du Conseil[46], 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.

(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[47] et le règlement (UE) 2017/746 du Parlement

---

44 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).

45 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).

46 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).

47 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

européen et du Conseil[48], 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.

(32) En ce qui concerne les systèmes d'IA autonomes, c'est-à-dire 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.

(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, en particulier en ce qui concerne l'âge, l'appartenance ethnique, le sexe ou les handicaps. 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 la gestion et l'exploitation du trafic routier et dans la fourniture d'eau, de gaz, de chauffage et d'électricité, car leur défaillance ou leur dysfonctionnement 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.

(35) Les systèmes d'IA utilisés dans l'éducation ou la formation professionnelle, notamment pour déterminer l'accès ou l'affectation de personnes aux établissements d'enseignement et de formation professionnelle ou pour évaluer les personnes sur la base d'épreuves dans le cadre de leur formation ou comme condition préalable à celle-ci 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 et pour le suivi ou l'évaluation des personnes dans le cadre de relations professionnelles contractuelles, devraient également être classés

---

règlement (CE) nº 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

[48] 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).

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 petits fournisseurs pour leur usage propre. Les personnes physiques sollicitant ou recevant des prestations sociales et des services 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 les systèmes d'IA sont utilisés pour déterminer si ces prestations et services devraient être refusés, réduits, révoqués ou récupérés par les autorités, 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 envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence 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.

(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 détecter les hypertrucages, 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, ainsi que d'analyse de la criminalité des personnes physiques. Les systèmes d'IA spécifiquement destinés à être utilisés pour des procédures administratives par les autorités fiscales et douanières 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; pour vérifier l'authenticité des documents pertinents de personnes physiques; et pour aider les autorités publiques compétentes à examiner les demandes d'asile, de visa et de permis de séjour ainsi que les plaintes 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[49], le règlement (CE) nº 810/2009 du Parlement européen et du Conseil[50] et toute autre législation pertinente.

(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 rechercher et 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, les tâches administratives ou l'allocation des ressources.

(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 nécessairement 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.

(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 pour les utilisateurs et les personnes concernées, 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.

(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.

---

[49] 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).

[50] 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).

(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, représentatifs, exempts d'erreurs et complets au regard de la destination du système. Ils devraient également 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. En particulier, 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 raisons d'intérêt public important, afin d'assurer la surveillance, la détection et la correction des biais liés aux systèmes d'IA à haut risque.

(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.

(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, le cas échéant.

(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.

(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. Ils doivent être résilients contre les risques liés aux limites du système (par exemple les erreurs, les défauts, les incohérences, les situations inattendues) ainsi que contre les actions malveillantes qui peuvent compromettre la sûreté du système d'IA et entraîner un comportement préjudiciable ou, plus généralement, indésirable. 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 fixant les prescriptions relatives à l'accréditation et

à la surveillance du marché pour la commercialisation des produits[51], à la décision nº 768/2008/CE du Parlement européen et du Conseil relative à un cadre commun pour la commercialisation des produits[52] et au règlement (UE) 2019/1020 du Parlement européen et du Conseil sur la surveillance du marché et la conformité des produits[53] («nouveau cadre législatif pour la commercialisation des produits»).

(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.

(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.

(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 final 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.

(57) Conformément aux principes du nouveau cadre législatif, des obligations spécifiques pour les opérateurs économiques concernés, notamment les importateurs et les distributeurs, devraient être fixées pour garantir la sécurité juridique et faciliter le respect de la réglementation par ces opérateurs.

---

51 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).

52 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).

53 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).

(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.

(59) Il convient d'envisager que l'utilisateur du système d'IA soit la personne physique ou morale, l'autorité publique, l'agence ou tout autre organisme sous l'autorité duquel le système d'IA est exploité, sauf lorsque l'utilisation s'inscrit dans le cadre d'une activité personnelle à caractère non professionnel.

(60) Étant donné la complexité de la chaîne de valeur de l'intelligence artificielle, les tiers concernés, notamment ceux qui interviennent dans la vente et la fourniture de logiciels, d'outils logiciels, de composants, de données et de modèles pré-entraînés, ou les fournisseurs de services de réseau, devraient coopérer, le cas échéant, avec les fournisseurs et les utilisateurs pour faciliter le respect des obligations qui leur incombent au titre du présent règlement, et avec les autorités compétentes établies en vertu du présent règlement.

(61) La normalisation devrait jouer un rôle essentiel pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec présent règlement. Le respect des normes harmonisées telles que définies dans le règlement (UE) nº 1025/2012 du Parlement européen et du Conseil[54] devrait être un moyen pour les fournisseurs de démontrer la conformité aux exigences du présent règlement. Cependant, la Commission pourrait adopter des spécifications techniques communes dans les domaines où il n'existe pas de normes harmonisées ou où elles sont insuffisantes.

(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]

[54] 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).

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.

(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 désignés 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.

(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 les systèmes d'IA fassent l'objet d'une nouvelle évaluation de la conformité chaque fois qu'ils subissent une modification susceptible d'avoir une incidence sur leur conformité avec le présent règlement ou que la destination du système change. En outre, pour les systèmes d'IA qui continuent à «apprendre» après avoir été mis sur le marché ou mis en service (c'est-à-dire qui adaptent automatiquement la façon dont les fonctions sont exécutées), il est nécessaire de prévoir des règles établissant que les modifications de l'algorithme et de ses performances qui ont été prédéterminées par le fournisseur et évaluées au moment de l'évaluation de la conformité ne devraient pas constituer une modification substantielle.

(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 d'enregistrer leur système d'IA à haut risque dans une base de données de l'UE, qui sera établie et gérée par la Commission. 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[55]. 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.

(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 informées du fait qu'elles interagissent avec un système d'IA, à moins que cela ne soit évident en raison des circonstances et du contexte d'utilisation. En outre, les personnes physiques devraient être informées du fait qu'elles sont exposées à un système de reconnaissance des émotions ou à un système de catégorisation biométrique. 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.

(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 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

[55] 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).

obstacles pour les petites et moyennes entreprises (PME) et les jeunes entreprises. 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. Le présent règlement devrait constituer la base juridique pour l'utilisation 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 sur l'IA, conformément à l'article 6, paragraphe 4, du règlement (UE) 2016/679 et à l'article 6 du règlement (UE) 2018/1725, et sans préjudice de l'article 4, paragraphe 2, de la directive (UE) 2016/680. 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.

(73) Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des petits fournisseurs et utilisateurs 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 petits fournisseurs 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.

(74) 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 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.

(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. Le Comité devrait être chargé d'un certain nombre de tâches consultatives, parmi lesquelles la formulation d'avis, de recommandations, de conseils ou d'orientations sur des questions liées à la mise en œuvre du présent règlement, y compris sur les spécifications techniques ou les normes existantes concernant les exigences établies dans le présent règlement, et la fourniture de conseils et d'assistance à la Commission sur des questions spécifiques liées à l'intelligence artificielle.

(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. Afin d'accroître l'efficacité de l'organisation du côté des États membres et de définir un point de contact officiel avec le public et les homologues au niveau des États membres et de l'Union, chaque État membre devrait désigner une autorité nationale unique en tant qu'autorité de contrôle nationale.

(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 ou toute violation du droit national ou de l'Union en matière de droits fondamentaux 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. Lorsque cela est nécessaire à leur mandat, les autorités ou organismes publics nationaux qui contrôlent l'application du droit de l'Union en matière de droits fondamentaux, y compris les organismes de promotion de l'égalité, devraient aussi avoir accès à toute documentation créée au titre du présent règlement.

(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, y compris, le cas échéant, la Banque centrale européenne, 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. 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[56], il convient aussi d'intégrer la procédure d'évaluation de la conformité et 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.

(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 obligatoires applicables aux systèmes d'IA à haut risque. 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[57] 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.

(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. 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.

---

[56] 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).

[57] 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).

(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 techniques et les approches visées à l'annexe I pour définir les systèmes d'IA, 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»[58]. 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.

(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[59].

(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.

(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 [...],

---

58 JO L 123 du 12.5.2016, p. 1.

59 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).

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;

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

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

(d) des règles harmonisées en matière de transparence applicables aux systèmes d'IA destinés à interagir avec des personnes physiques, aux systèmes de reconnaissance des émotions et de catégorisation biométrique, et aux systèmes d'IA utilisés pour générer ou manipuler des images ou des contenus audio ou vidéo;

(e) des règles relatives au suivi et à la surveillance du marché.

Article 2
Champ d'application

1. Le présent règlement s'applique:

(a) aux fournisseurs, 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 situés dans l'Union;

(c) aux fournisseurs et aux utilisateurs de systèmes d'IA situés dans un pays tiers, lorsque les résultats générés par le système sont utilisés dans l'Union.

2. Seul l'article 84 du présent règlement s'applique aux systèmes d'IA à haut risque qui sont des composants de sécurité de produits ou de systèmes ou qui constituent eux-mêmes des produits ou des systèmes et qui relèvent du champ d'application des actes suivants:

(a) règlement (CE) n° 300/2008;

(b) règlement (UE) nº 167/2013;

(c) règlement (UE) nº 168/2013;

(d) directive 2014/90/UE;

(e) directive (UE) 2016/797;

(f) règlement (UE) 2018/858;

(g) règlement (UE) 2018/1139;

(h) règlement (UE) 2019/2144.

3. Le présent règlement ne s'applique pas aux systèmes d'IA développés ou utilisés exclusivement à des fins militaires.

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 IV, de la directive 2000/31/CE du Parlement européen et du Conseil[60] [*qui doivent être remplacées par les dispositions correspondantes de la législation sur les services numériques*].

Article 3
Définitions

Aux fins du présent règlement, on entend par:

(1) «système d'intelligence artificielle» (système d'IA), un logiciel qui est développé au moyen d'une ou plusieurs des techniques et approches énumérées à l'annexe I et qui peut, pour un ensemble donné d'objectifs définis par l'homme, générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels il interagit;

(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 en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit;

(3) «petit fournisseur», un fournisseur qui est une micro ou petite entreprise au sens de la recommandation 2003/361/CE de la Commission[61];

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

(5) «mandataire», toute personne physique ou morale établie dans l'Union ayant reçu 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;

(6) «importateur», toute personne physique ou morale établie dans l'Union qui met sur le marché ou met en service 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 sans altérer ses propriétés;

---

60 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).

61 Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

(8) «opérateur», le fournisseur, l'utilisateur, le mandataire, l'importateur et 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 sur le marché de 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, y compris du contexte géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé;

(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;

(17) «retrait d'un système d'IA», toute mesure visant à empêcher qu'un système d'IA soit distribué, présenté et proposé;

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

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

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

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

(22) «organisme notifié», un organisme d'évaluation de la conformité 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 entraîne une modification de la destination pour laquelle le système d'IA a été évalué;

(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, du présent règlement et d'autres actes législatifs 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) «surveillance après commercialisation», l'ensemble des activités réalisées par les fournisseurs de systèmes d'IA pour recueillir et analyser de manière proactive 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) «spécifications communes», un document, autre qu'une norme, contenant des solutions techniques qui permettent de satisfaire à certaines exigences et obligations établies en vertu du présent règlement;

(29) «données d'entraînement», les données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînables, y compris les poids d'un réseau neuronal;

(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, qui permettent ou confirment son identification unique, 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 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 selon le sexe, l'âge, la couleur des

cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou l'orientation sexuelle ou politique, etc., sur la base de leurs données biométriques;

(36) «système d'identification biométrique à distance», un système d'IA destiné à identifier des personnes physiques à distance en comparant les données biométriques d'une personne avec celles qui figurent dans une base de données de référence, et sans que l'utilisateur du système d'IA ne sache au préalable si la personne sera présente et pourra être identifiée;

(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 sans décalage temporel significatif. Cela comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles.

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

(39) «espace accessible au public», tout espace physique accessible au public, indépendamment de l'existence de conditions d'accès à cet espace;

(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 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) «autorité de contrôle nationale», l'autorité qu'un État membre charge de la mise en œuvre et de l'application du présent règlement, de la coordination des activités confiées à cet État membre, du rôle de point de contact unique pour la Commission et de la représentation de l'État membre au sein du Comité européen de l'intelligence artificielle;

(43) «autorité nationale compétente», l'autorité de contrôle nationale, l'autorité notifiante et l'autorité de surveillance du marché;

(44) «incident grave», tout incident entraînant directement ou indirectement, susceptible d'avoir entraîné ou susceptible d'entraîner:

(a) le décès d'une personne ou une atteinte grave à la santé d'une personne, à des biens ou à l'environnement,

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

Article 4
Modification de l'annexe I

La Commission est habilitée à adopter des actes délégués conformément à l'article 73 afin de modifier la liste des techniques et approches énumérées à l'annexe I, en vue de mettre cette liste à jour en fonction de l'évolution du marché et des technologies sur la base de caractéristiques similaires aux techniques et approches qui y sont énumérées.

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 pour altérer substantiellement son comportement d'une manière qui cause ou est 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 ou au handicap physique ou mental d'un groupe de personnes donné pour altérer substantiellement le comportement d'un membre de ce groupe d'une manière qui cause ou est 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, par les pouvoirs publics ou pour leur compte, de systèmes d'IA destinés à évaluer ou à établir un classement de la fiabilité 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 entiers 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 entiers 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 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, notamment d'enfants disparus;

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

iii) la détection, la localisation, l'identification ou les poursuites à l'encontre de l'auteur ou du suspect d'une infraction pénale visée à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil[62] et punissable 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, 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;

(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 et de ne demander l'autorisation qu'en cours d'utilisation ou lorsque celle-ci a pris fin.

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

[62] 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).

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

   (a) le système d'IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par les actes législatifs d'harmonisation de l'Union énumérés à l'annexe II, ou constitue lui-même un tel produit;

   (b) le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, est soumis à une évaluation de la 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 d'harmonisation de l'Union énumérés à l'annexe II.

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

Article 7

Modifications de l'annexe III

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 afin de mettre à jour 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 sont 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.

CHAPITRE 2

EXIGENCES APPLICABLES AUX SYSTÈMES D'IA À HAUT RISQUE

Article 8
Respect des exigences

1. Les systèmes d'IA à haut risque respectent les exigences établies dans le présent chapitre.

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 consiste en un processus itératif continu qui 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 associés à chaque système d'IA à haut risque;

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

   (c) l'évaluation d'autres risques susceptibles d'apparaître, sur la base de l'analyse des données recueillies au moyen du système de surveillance après commercialisation visé à l'article 61;

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

3. Les mesures de gestion des risques visées au paragraphe 2, point d), tiennent dûment compte des effets et des interactions possibles résultant de l'application combinée des exigences énoncées dans le présent chapitre 2. Elles prennent en considération l'état de la technique généralement reconnu, notamment tel qu'il ressort des normes harmonisées ou des spécifications communes pertinentes.

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, à condition que le système d'IA à haut risque soit utilisé conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible. L'utilisateur est informé de ces risques résiduels.

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

   (a) éliminer ou réduire les risques autant que possible grâce à une conception et à un développement appropriés;

   (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.

   Lors 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 testés afin de déterminer les mesures de gestion des risques les plus appropriées. Ces tests garantissent que les systèmes d'IA à haut

risque fonctionnent de manière cohérente conformément à leur destination et qu'ils sont conformes aux exigences énoncées dans le présent chapitre.

6. Les procédures de test sont appropriées pour remplir la destination du système d'IA et ne doivent pas aller au-delà de ce qui est nécessaire pour atteindre cet objectif.

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. Lors de la mise en œuvre du système de gestion des risques décrit aux paragraphes 1 à 7, il convient d'étudier avec attention la probabilité que des enfants puissent avoir accès au système d'IA à haut risque ou que ce dernier ait une incidence sur eux.

9. Pour les établissements de crédit couverts par la directive 2013/36/UE, les aspects décrits aux paragraphes 1 à 8 font partie des procédures de gestion des risques établies par ces établissements conformément à l'article 74 de ladite directive.

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) la 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;

   (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, 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. Des pratiques appropriées en matière de gouvernance et de gestion des données s'appliquent au développement de systèmes d'IA à haut risque autres que ceux qui font appel à des techniques impliquant l'entraînement de modèles afin de garantir que ces systèmes d'IA à haut risque sont conformes au paragraphe 2.

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 pour évaluer la conformité du système d'IA avec ces exigences. Elle contient, au minimum, les éléments énoncés à l'annexe IV.

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. La conception et le développement des systèmes d'IA à haut risque prévoient des fonctionnalités permettant l'enregistrement automatique des événements («journaux») pendant le fonctionnement de ces systèmes. Ces fonctionnalités d'enregistrement sont conformes à des normes ou à des spécifications communes reconnues.

2. Les fonctionnalités d'enregistrement garantissent un degré de traçabilité du fonctionnement du système d'IA tout au long de son cycle de vie qui soit adapté à la destination du système.

3. En particulier, ces fonctionnalités permettent de surveiller le fonctionnement du système d'IA à haut risque dans l'éventualité de situations ayant pour effet que l'IA présente un risque au sens de l'article 65, paragraphe 1, ou entraînant une modification substantielle, et facilitent la surveillance après commercialisation visée à l'article 61.

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 permettre aux utilisateurs d'interpréter les résultats du système et de l'utiliser de manière appropriée. Un type et un niveau adéquats de transparence permettent de veiller au respect des obligations pertinentes incombant à l'utilisateur et au fournisseur énoncées au chapitre 3 du présent titre.

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;

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

      iii) toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des

conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé et la sécurité ou pour les droits fondamentaux;

iv) ses performances en ce qui concerne les personnes ou groupes de personnes 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.

(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) la durée de vie attendue du système d'IA à haut risque et toutes les mesures de maintenance et de suivi nécessaires pour assurer le bon fonctionnement de ce système d'IA, notamment en ce qui concerne les mises à jour logicielles.

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 mesures suivantes:

(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. Les mesures prévues au paragraphe 3 donnent aux personnes chargées d'effectuer un contrôle humain, en fonction des circonstances, la possibilité:

(a) d'appréhender totalement les capacités et les limites du système d'IA à haut risque et d'être en mesure de surveiller correctement son fonctionnement, afin de pouvoir détecter et traiter dès que possible les signes d'anomalies, de dysfonctionnements et de performances inattendues;

(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»), en particulier pour les systèmes d'IA à haut risque utilisés pour fournir des informations ou des recommandations concernant les décisions à prendre par des personnes physiques;

(c) d'être en mesure d'interpréter correctement les résultats du système d'IA à haut risque, compte tenu notamment des caractéristiques du système et des outils et méthodes d'interprétation disponibles;

(d) d'être en mesure 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'être capable 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 par au moins deux personnes physiques.

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.

4. 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.

5. 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 telle sorte que les éventuels biais dus à l'utilisation de résultats comme données d'entrée pour les opérations futures («boucles de rétroaction») fassent l'objet d'un traitement adéquat au moyen de mesures d'atténuation appropriées.

6. 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;

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

(c) établissent la documentation technique du système d'IA à haut risque;

(d) assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque, dans la mesure où ces journaux se trouvent sous leur contrôle;

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

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

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

(h) informent les autorités nationales compétentes 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 des incidents graves et des dysfonctionnements 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.

3. Si les fournisseurs sont des établissements de crédit régis par la directive 2013/36/UE, la conformité avec les règles relatives aux dispositifs, processus et mécanismes de gouvernance interne prévues à l'article 74 de ladite directive vaut respect de l'obligation de mettre en place un système de gestion de la qualité. Dans ce contexte, toute norme harmonisée visée à l'article 40 du présent règlement est prise en considération.

Article 18
Obligation d'établir une documentation technique

1. Les fournisseurs de systèmes d'IA à haut risque établissent la documentation technique prévue à l'article 11 conformément à l'annexe IV.

2. Si les fournisseurs sont des établissements de crédit régis par la directive 2013/36/UE, ils tiennent à jour la documentation technique dans le cadre de la documentation à établir sur les dispositifs, processus et mécanismes de gouvernance interne au sens de l'article 74 de ladite directive.

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 «CE» de conformité conformément à l'article 49.

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 5 b), mis sur le marché ou mis en service par des fournisseurs qui sont des établissements de crédit régis par la directive 2013/36/UE, l'évaluation de la conformité est effectuée dans le cadre de la procédure visée aux articles 97 à 101 de ladite directive.

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, 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. Les journaux sont conservés pendant une période appropriée au regard de la destination du système d'IA à haut risque et des obligations légales applicables en vertu du droit de l'Union ou du droit national.

2. Si les fournisseurs sont des établissements de crédit régis par la directive 2013/36/UE, ils assurent la tenue des journaux générés automatiquement par leurs systèmes d'IA à haut risque dans le cadre de la documentation prévue à l'article 74 de ladite directive.

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 prennent immédiatement 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 officielle de l'Union définie par 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, 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 24
Obligations des fabricants de produits

Lorsqu'un système d'IA à haut risque lié à des produits auxquels s'appliquent les actes juridiques énumérés à l'annexe II, section A, est mis sur le marché ou mis en service en même temps que le produit fabriqué conformément à ces actes juridiques et sous le nom du fabricant du produit, ce dernier assume la responsabilité de la conformité du système d'IA avec le présent règlement et est soumis, pour ce qui concerne le système d'IA, aux mêmes obligations que celles imposées au fournisseur par le présent règlement.

Article 25
Mandataires

1. Avant de mettre leurs systèmes à disposition sur le marché de l'Union, si aucun importateur ne peut être identifié, 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. Le mandat habilite le mandataire à exécuter les tâches suivantes:

   (a) tenir à la disposition des autorités nationales compétentes et des autorités nationales visées à l'article 63, paragraphe 7, une copie de la déclaration de conformité UE et de la documentation technique;

   (b) à la demande motivée d'une autorité nationale compétente, communiquer à cette dernière toutes les informations et tous les documents 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, 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.

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:

   (a) le fournisseur de ce système d'IA a suivi la procédure appropriée d'évaluation de la conformité;

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

   (c) le système porte le marquage de conformité requis et est accompagné de la documentation et de la notice d'utilisation requises.

2. Lorsqu'un importateur considère ou a des raisons de considérer qu'un système d'IA à haut risque n'est pas conforme au présent règlement, 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 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.

5. À la demande motivée des autorités nationales compétentes, les importateurs communiquent à ces dernières toutes les informations et tous les documents nécessaires 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, et leur accordent notamment l'accès aux journaux automatiquement générés par le système d'IA à haut risque, 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. Ils coopèrent également avec ces autorités à toute mesure prise par l'autorité nationale compétente à l'égard de ce système.

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 de la documentation et de la notice d'utilisation requises et que le fournisseur et l'importateur du système, selon le cas, ont respecté les obligations énoncées dans le présent règlement.

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 pour démontrer la conformité d'un système à haut risque avec les exigences énoncées au chapitre 2 du présent titre. Les distributeurs coopèrent également avec cette autorité nationale compétente à toute mesure prise par cette autorité.

Article 28

Obligations des distributeurs, des importateurs, des utilisateurs ou de tout autre tiers

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

   (a) il met sur le marché ou met en service un système d'IA à haut risque sous son propre nom ou sa propre marque;

   (b) il modifie la destination d'un système d'IA à haut risque déjà mis sur le marché ou mis en service;

   (c) il apporte une modification substantielle au système d'IA à haut risque.

2. Lorsque les circonstances visées au paragraphe 1, point b) 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.

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.

2. Les obligations énoncées au paragraphe 1 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 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 ou un dysfonctionnement au sens de l'article 62 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.

5. Si les utilisateurs sont des établissements de crédit régis par la directive 2013/36/UE, la conformité avec les règles relatives aux dispositifs, processus et mécanismes de gouvernance interne prévues à l'article 74 de ladite directive vaut respect de l'obligation de surveillance énoncée au premier alinéa.

6. Les utilisateurs de systèmes d'IA à haut risque assurent la tenue des journaux générés automatiquement par ce système d'IA à haut risque, dans la mesure où ces journaux se trouvent sous leur contrôle. Les journaux sont conservés pendant une période appropriée au regard de la destination du système d'IA à haut risque et des obligations légales applicables en vertu du droit de l'Union ou du droit national.

   Si les utilisateurs sont des établissements de crédit régis par la directive 2013/36/UE, ils assurent la tenue des journaux dans le cadre de la documentation à établir sur les dispositifs, processus et mécanismes de gouvernance interne au sens de l'article 74 de ladite directive.

7. 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.

CHAPITRE 4

AUTORITÉS NOTIFIANTES ET ORGANISMES NOTIFIÉS

Article 30
Autorités notifiantes

1. Chaque État membre désigne ou établit 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 désigner comme autorité notifiante un organisme national d'accréditation au sens du règlement (CE) nº 765/2008.

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.

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

8. Les autorités notifiantes veillent à ce que les évaluations de la conformité soient effectuées de manière proportionnée, en évitant les charges inutiles pour les fournisseurs, et à ce que les organismes notifiés accomplissent leurs activités en tenant 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.

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 technologies d'intelligence artificielle pour lesquelles 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 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.

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 énoncées à l'article 33.

2. Les autorités notifiantes les notifient 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 comprend des informations complètes sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et les technologies d'intelligence artificielle concernées.

4. L'organisme d'évaluation de la conformité concerné ne peut effectuer les activités propres à un organisme notifié que si aucune objection n'est émise par la Commission ou les autres États membres dans le mois qui suit la notification.

5. Les autorités notifiantes informent la Commission et les autres États membres de toute modification pertinente apportée ultérieurement à la notification.

Article 33
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 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, 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 concerné sur la base de la législation nationale ou que l'évaluation de la conformité ne soit réalisée directement par cet État membre.

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. À cette fin, en toutes circonstances et pour chaque procédure d'évaluation de la conformité et chaque type de système d'IA à haut risque pour lequel ils ont été désignés, les organismes notifiés disposent en permanence d'un personnel administratif, technique 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. 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 lui permettre de réaliser ses activités d'évaluation, de désignation, de notification, de contrôle et de surveillance et pour faciliter les évaluations décrites au présent chapitre.

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 organismes notifiés tiennent à la disposition de l'autorité notifiante 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.

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. Lorsqu'une autorité notifiante soupçonne ou a été informée 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 procède immédiatement à une enquête avec la plus grande diligence. Dans ce contexte, elle informe l'organisme notifié concerné des objections soulevées et lui donne la possibilité de faire valoir son point de vue. Si l'autorité notifiante conclut que l'organisme notifié faisant l'objet de l'enquête 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, selon le cas, en fonction de la gravité du manquement. De plus, elle en informe immédiatement la Commission et les autres États membres.

2. En cas de restriction, de suspension ou de retrait d'une notification, ou lorsque l'organisme notifié a cessé ses activités, l'autorité notifiante prend les mesures qui s'imposent pour faire en sorte que les dossiers dudit organisme notifié soient pris en charge par un autre organisme notifié ou tenus à la disposition des autorités notifiantes qui en font la demande.

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.

4. Lorsque la Commission établit qu'un organisme notifié ne répond pas ou ne répond plus aux exigences fixées à l'article 33, elle adopte une décision motivée demandant à l'État membre notifiant de prendre les mesures correctives qui s'imposent, y compris le retrait de la notification si nécessaire. 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, dans les domaines couverts par le présent règlement, une coordination et une coopération appropriées entre les organismes notifiés intervenant dans les procédures d'évaluation de la conformité des systèmes d'IA conformément au présent règlement soient mises en place et gérées de manière adéquate dans le cadre d'un groupe sectoriel d'organismes notifiés.

2. Les États membres veillent 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.

CHAPITRE 5

NORMES, ÉVALUATION DE LA CONFORMITÉ, CERTIFICATS, ENREGISTREMENT

Article 40
Normes harmonisées

Les systèmes d'IA à haut risque 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, dans la mesure où celles-ci sont couvertes par ces normes.

Article 41
Spécifications communes

1. S'il n'existe pas de normes harmonisées au sens de l'article 40 ou si la Commission estime que les normes harmonisées pertinentes sont insuffisantes ou qu'il est nécessaire de pallier des difficultés particulières en matière de sécurité ou de droits fondamentaux, la Commission peut, au moyen d'actes d'exécution, adopter des spécifications communes en ce qui concerne les exigences énoncées au chapitre 2 du présent titre. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.

2. Lorsqu'elle élabore les spécifications communes visées au paragraphe 1, la Commission recueille les avis des organismes ou groupes d'experts concernés établis en vertu de la législation sectorielle pertinente de l'Union.

3. Les systèmes d'IA à haut risque conformes aux spécifications communes visées au paragraphe 1 sont présumés conformes aux exigences énoncées au chapitre 2 du présent titre, dans la mesure où celles-ci sont couvertes par ces spécifications communes.

4. Lorsque les fournisseurs ne respectent pas les spécifications communes visées au paragraphe 1, ils justifient dûment avoir adopté des solutions techniques au moins équivalentes auxdites spécifications.

Article 42
Présomption de conformité avec certaines exigences

1. Compte tenu de leur destination, les systèmes d'IA à haut risque qui ont été entraînés et testés avec les données relatives au contexte géographique, comportemental et fonctionnel spécifique dans lequel ils sont destinés à être utilisés sont présumés conformes à l'exigence énoncée à l'article 10, paragraphe 4.

2. Les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au règlement (UE) 2019/881 du Parlement européen et du Conseil[63] 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 suit l'une des procédures suivantes:

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

   (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.

   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.

[63] 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. 1).

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI, qui ne prévoit pas d'intervention d'un organisme notifié. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 5 b), mis sur le marché ou mis en service par des établissements de crédit régis par la directive 2013/36/UE, l'évaluation de la conformité est effectuée dans le cadre de la procédure visée aux articles 97 à 101 de ladite directive.

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

   Pour les systèmes d'IA à haut risque qui continuent leur apprentissage après avoir été mis sur le marché ou mis en service, les modifications apportées au système d'IA à haut risque et à 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.

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 en vue d'introduire des éléments des procédures d'évaluation de la conformité qui s'avèrent nécessaires 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 officielle de l'Union déterminée par l'État membre d'établissement de l'organisme notifié ou, à défaut, dans une langue officielle de l'Union acceptée par l'organisme notifié.

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.

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

Les États membres veillent à ce qu'une procédure de recours contre les décisions des organismes notifiés soit disponible pour les parties ayant un intérêt légitime dans ces décisions.

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 technologies d'intelligence artificielle des informations pertinentes sur les aspects liés à des résultats négatifs et, sur demande, à des résultats positifs d'évaluation de la conformité.

Article 47
Dérogation à la procédure d'évaluation de la conformité

1. Par dérogation à l'article 43, 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, et prend fin lorsque ces procédures sont achevées. Ces procédures sont menées à bien dans les meilleurs délais.

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.

3. Si aucune objection n'est émise, dans un délai de quinze jours civils suivant la réception des informations visées au paragraphe 2, par un État membre ou par la Commission à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un État membre conformément au paragraphe 1, cette autorisation est réputée justifiée.

4. Si, dans un délai de quinze jours civils suivant la réception de la notification visée au paragraphe 2, un État membre soulève des objections à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un autre État membre, ou si la Commission estime que l'autorisation est contraire au droit de l'Union ou que la conclusion des États membres quant à la conformité du système visée au paragraphe 2 n'est pas fondée, la Commission entame sans délai des consultations avec l'État membre concerné; le ou les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Sur cette base, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre concerné ainsi qu'à l'opérateur ou aux opérateurs concernés.

5. Si l'autorisation est jugée injustifiée, elle est retirée par l'autorité de surveillance du marché de l'État membre concerné.

6. Par dérogation aux paragraphes 1 à 5, en ce qui concerne les systèmes d'IA à haut risque destinés à être utilisés comme composants de sécurité de dispositifs relevant

du règlement (UE) 2017/745 et du règlement (UE) 2017/746, ou qui constituent eux-mêmes de tels dispositifs, l'article 59 du règlement (UE) 2017/745 et l'article 54 du règlement (UE) 2017/746 s'appliquent également à l'égard de la dérogation à l'évaluation de la conformité attestant le respect des exigences énoncées au chapitre 2 du présent titre.

Article 48
Déclaration UE de conformité

1. Le fournisseur établit, par écrit, une déclaration UE de conformité 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 ou des langues officielles de l'Union requises par le ou les 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 II 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 CE est apposé de façon visible, lisible et indélébile sur les systèmes d'AI 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.

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

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
Conservation des documents

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.

Article 51
Enregistrement

Avant de mettre sur le marché ou de mettre en service un système d'IA à haut risque visé à l'article 6, paragraphe 2, le fournisseur ou, le cas échéant, le mandataire enregistre ce système dans la base de données de l'UE visée à l'article 60.

TITRE IV

OBLIGATIONS DE TRANSPARENCE POUR CERTAINS SYSTÈMES D'IA

Article 52
Obligations de transparence pour 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 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, 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 des émotions ou d'un système de catégorisation 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.

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 lorsqu'elle est nécessaire à l'exercice du droit à la liberté

d’expression et du droit à la liberté des arts et des sciences garantis par la charte des droits fondamentaux de l’UE, et sous réserve de garanties appropriées pour les droits et libertés des tiers.

4. Les paragraphes 1, 2 et 3 n’ont pas d'incidence sur les exigences et obligations énoncées au titre III du présent règlement.

TITRE V

MESURES DE SOUTIEN À L’INNOVATION

Article 53
Bacs à sable réglementaires de l’IA

1. Les bacs à sable réglementaires de l’IA créés par une ou plusieurs autorités compétentes des États membres ou par le Contrôleur européen de la protection des données offrent un environnement contrôlé qui facilite le développement, la mise à l’essai et la validation de systèmes d’IA innovants pendant une durée limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique. Cela se fait sous la surveillance et le contrôle directs des autorités compétentes afin de garantir le respect des exigences du présent règlement et, le cas échéant, d’autres dispositions législatives de l’Union et des États membres contrôlées au sein du bac à sable.

2. Les États membres veillent à ce que, dans la mesure où les systèmes d’IA innovants impliquent le traitement de données à caractère personnel ou relèvent à d'autres titres de la surveillance d’autres autorités nationales ou autorités compétentes assurant ou encadrant l’accès aux données, les autorités nationales chargées de la protection des données et ces autres autorités nationales soient associées au fonctionnement du bac à sable réglementaire de l’IA.

3. Les bacs à sable réglementaires de l’IA n’ont pas d'incidence sur les pouvoirs des autorités compétentes en matière de contrôle et de mesures correctives. Tout risque significatif pour la santé, la sécurité et les droits fondamentaux constaté lors du développement et des tests de ces systèmes donne lieu à des mesures d’atténuation immédiates et, à défaut, à la suspension du processus de développement et d’essai jusqu’à ce que cette atténuation soit effective.

4. Les participants au bac à sable réglementaire de l’IA demeurent responsables, en vertu de la législation applicable de l’Union et des États membres en matière de responsabilité, de tout préjudice infligé à des tiers en raison de l’expérimentation menée dans le bac à sable.

5. Les autorités compétentes des États membres qui ont mis en place des bacs à sable réglementaires de l’IA coordonnent leurs activités et coopèrent dans le cadre du Comité européen de l’intelligence artificielle. Ils soumettent au Comité et à la Commission des rapports annuels sur les résultats de la mise en œuvre de ce dispositif, 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.

6. Les modalités et les conditions de fonctionnement des bacs à sable réglementaires de l’IA, y compris les critères d’admissibilité et la procédure de demande, de sélection, de participation et de sortie du bac à sable, ainsi que les droits et obligations des

participants sont définis dans des actes d'exécution. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.

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 sont traitées aux fins du développement et du test de certains systèmes d'IA innovants dans le bac à sable, dans les conditions suivantes:

   (a) les systèmes d'IA innovants sont développés pour préserver des intérêts publics importants dans un ou plusieurs des domaines suivants:

      i) la prévention et la détection d'infractions pénales, ainsi que 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, sous le contrôle et la responsabilité des autorités compétentes. Le traitement est fondé sur le droit des États membres ou de l'Union,

      ii) la sécurité publique et la santé publique, y compris la prévention, le contrôle et le traitement des maladies,

      iii) un niveau élevé de protection et d'amélioration de la qualité de l'environnement;

   (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 fondamentaux des personnes concernées 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 n'est transmise, transférée ou consultée d'une autre manière par d'autres parties;

   (f) aucun traitement de données à caractère personnel effectué dans le cadre du bac à sable ne débouche sur des mesures ou des décisions affectant les personnes concernées;

   (g) les données à caractère personnel traitées dans le cadre du bac à sable sont 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 journaux du traitement des données à caractère personnel effectué dans le cadre du bac à sable sont conservés pendant la durée de la participation au bac

à sable et 1 an après son expiration, aux seules fins de satisfaire aux obligations en matière de responsabilité et de documentation prévues par le présent article ou d'autres dispositions applicatives de la législation de l'Union ou des États membres, et uniquement pour la durée nécessaire à cette satisfaction;

(i) une description complète et détaillée du processus et de la justification de l'entraînement, des tests et de la validation du système d'IA est conservée avec les résultats des tests, 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.

2. Le paragraphe 1 est sans préjudice de la législation de l'Union ou des États membres excluant le traitement à des fins autres que celles expressément mentionnées dans cette législation.

Article 55
Mesures en faveur des petits fournisseurs et utilisateurs

1. Les États membres:

(a) accordent aux petits fournisseurs et aux jeunes entreprises un accès prioritaire aux bacs à sable réglementaires de l'IA dans la mesure où ils remplissent les conditions d'éligibilité;

(b) organisent des activités spécifiques de sensibilisation à l'application du présent règlement, adaptées aux besoins des petits fournisseurs et utilisateurs;

(c) le cas échéant, établissent un canal de communication privilégié avec les petits fournisseurs et utilisateurs et d'autres innovateurs afin de fournir des orientations et de répondre aux questions relatives à la mise en œuvre du présent règlement.

2. Les intérêts et besoins spécifiques des petits fournisseurs 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 la taille et à la taille du marché des petits fournisseurs.

TITRE VI

GOUVERNANCE

CHAPITRE 1

COMITÉ EUROPÉEN DE L'INTELLIGENCE ARTIFICIELLE

Article 56
Création du Comité européen de l'intelligence artificielle

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

2. Le Comité fournit des conseils et une assistance à la Commission afin:

(a) de contribuer à la coopération efficace des autorités de contrôle nationales et de la Commission en ce qui concerne les matières relevant du présent règlement;

(b) de coordonner les orientations et analyses de la Commission et des autorités de contrôle nationales et d'autres autorités compétentes sur les questions émergentes dans l'ensemble du marché intérieur en ce qui concerne les matières relevant du présent règlement, et de contribuer à ces orientations et analyses;

(c) d'aider les autorités de contrôle nationales et la Commission à assurer une application cohérente du présent règlement.

Article 57
Structure du Comité

1. Le Comité est composé des autorités de contrôle nationales, qui sont représentées par leur directeur ou un de leurs hauts fonctionnaires de niveau équivalent, et du Contrôleur européen de la protection des données. D'autres autorités nationales peuvent être invitées aux réunions, lorsque les questions examinées relèvent de leurs compétences.

2. Le Comité adopte son règlement intérieur à la majorité simple de ses membres une fois celui-ci approuvé par la Commission. Le règlement intérieur contient également les aspects opérationnels en rapport avec l'exécution des tâches du Comité telles qu'énumérées à l'article 58. Le Comité peut créer des sous-groupes, s'il y a lieu, afin d'examiner des questions spécifiques.

3. Le Comité est présidé par la Commission. 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.

4. Le Comité peut inviter des experts et des observateurs externes à participer à ses réunions, et peut organiser des échanges avec des tiers intéressés afin d'éclairer ses activités dans une mesure appropriée. À cette fin, la Commission peut faciliter les échanges entre le Comité et d'autres organes, bureaux, agences et groupes consultatifs de l'Union.

Article 58
Tâches du Comité

Lorsqu'il fournit des conseils et une assistance à la Commission dans le cadre de l'article 56, paragraphe 2, le Comité, en particulier:

(a) recueille l'expertise et les bonnes pratiques et les partage entre les États membres;

(b) contribue à l'harmonisation des pratiques administratives dans les États membres, y compris en ce qui concerne le fonctionnement des bacs à sable réglementaires visés à l'article 53;

(c) formule des avis, des recommandations ou des contributions écrites sur des questions liées à la mise en œuvre du présent règlement, en particulier

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.

CHAPITRE 2

AUTORITÉS NATIONALES COMPÉTENTES

Article 59
Désignation des autorités nationales compétentes

1. Des autorités nationales compétentes sont établies ou désignées par chaque État membre aux fins d'assurer l'application et la mise en œuvre du présent règlement. Les autorités nationales compétentes sont organisées de manière à garantir l'objectivité et l'impartialité de leurs activités et de leurs tâches.

2. Chaque État membre désigne une autorité de contrôle nationale parmi les autorités nationales compétentes. L'autorité de contrôle nationale agit en tant qu'autorité notifiante et autorité de surveillance du marché, sauf si un État membre a des raisons organisationnelles et administratives de désigner plus d'une autorité.

3. Les États membres font connaître à la Commission le ou les noms de la ou des autorités désignées et, le cas échéant, les raisons pour lesquelles ils ont désigné plusieurs autorités.

4. Les États membres veillent à ce que les autorités nationales compétentes disposent de ressources financières et humaines suffisantes pour mener à bien les tâches qui leur sont confiées en vertu du présent règlement. En particulier, les autorités nationales compétentes disposent en permanence d'un personnel en nombre suffisant, qui possède, parmi ses compétences et son expertise, une compréhension approfondie des technologies de l'intelligence artificielle, des données et du traitement de données, des droits fondamentaux, des risques pour la santé et la sécurité, et une connaissance des normes et exigences légales en vigueur.

5. Les États membres font annuellement rapport à la Commission sur l'état des ressources financières et humaines des autorités nationales compétentes, et lui présentent une évaluation de l'adéquation de ces ressources. La Commission transmet ces informations au Comité 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 orientations et des conseils sur la mise en œuvre du présent règlement, y compris aux petits fournisseurs. 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 AUTONOMES

Article 60

Base de données de l'UE pour les systèmes d'IA à haut risque autonomes

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 systèmes d'IA à haut risque visés à l'article 6, paragraphe 2, qui sont enregistrés conformément à l'article 51.
2. Les données énumérées à l'annexe VIII sont introduites dans la base de données de l'UE par les fournisseurs. Ces derniers bénéficient du soutien technique et administratif de la Commission.
3. Les informations contenues dans la base de données de l'UE sont accessibles au public.
4. La base de données de l'UE ne contient des données à caractère personnel que dans la mesure où celles-ci sont nécessaires à la collecte et au traitement d'informations conformément au présent règlement. Ces informations incluent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et légalement autorisées à représenter le fournisseur.
5. La Commission est la responsable du traitement pour la base de données de l'UE. Elle veille également à apporter un soutien technique et administratif approprié aux fournisseurs.

TITRE VIII

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

CHAPITRE 1

SURVEILLANCE APRÈS 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 à la nature des technologies de l'intelligence artificielle et des risques du système d'IA à haut risque.

2. Le système de surveillance après commercialisation collecte, documente et analyse, de manière active et systématique, les données pertinentes fournies par les utilisateurs ou collectées via d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur cycle de vie, et permet au fournisseur d'évaluer si les systèmes d'IA respectent en permanence les exigences énoncées au titre III, chapitre 2.

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, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de cette législation, les éléments décrits aux paragraphes 1, 2 et 3 sont intégrés dans ce système et ce plan, le cas échéant.

   Le premier alinéa s'applique également aux systèmes d'IA à haut risque visés à l'annexe III, point 5 b), mis sur le marché ou mis en service par des établissements de crédit visés par la directive 2013/36/UE.

CHAPITRE 2

PARTAGE D'INFORMATIONS SUR LES INCIDENTS ET LES DYSFONCTIONNEMENTS

Article 62
Notification des incidents graves et des dysfonctionnements

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union notifient tout incident grave ou tout dysfonctionnement de ces systèmes qui constitue une violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux aux autorités de surveillance du marché des États membres où a eu lieu cet incident ou cette violation.

   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 ou le dysfonctionnement et, en tout état de cause, au plus tard 15 jours après que le fournisseur a eu connaissance de l'incident grave ou du dysfonctionnement.

2. Dès réception d'une notification relative à une violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux, l'autorité de surveillance du marché 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 b), qui sont mis sur le marché ou mis en service par des fournisseurs qui sont des établissements de crédit régis par la directive 2013/36/UE et 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 ou des dysfonctionnements est limitée à ceux qui constituent une violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux.

CHAPITRE 3

CONTRÔLE 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 au titre III, chapitre 3, 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. L'autorité de contrôle nationale communique régulièrement à la Commission les résultats des activités de surveillance du marché pertinentes. L'autorité de contrôle nationale communique sans retard à la Commission et aux autorités nationales de la concurrence concernées toute information recueillie dans le cadre des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de l'Union relatif aux règles de concurrence.

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.

4. Pour les systèmes d'IA 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 responsable de la surveillance financière de ces établissements en vertu de cette législation.

5. Pour les systèmes d'IA énumérés à l'annexe III, point 1 a), dans la mesure où ils sont utilisés à des fins répressives, et points 6 et 7, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités compétentes en matière de contrôle de la protection des données en vertu de la directive (UE) 2016/680 ou du règlement (UE) 2016/679, soit les autorités nationales compétentes pour surveiller les activités des autorités répressives, des services de l'immigration ou des autorités compétentes en matière d'asile qui mettent en service ou utilisent ces systèmes.

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.

Article 64
Accès aux données et à la documentation

1. En ce qui concerne l'accès aux données et à la documentation dans le cadre de leurs activités, les autorités de surveillance du marché ont pleinement accès aux jeux de données d'entraînement, de validation et de test utilisés par le fournisseur, y compris par l'intermédiaire d'interfaces de programmation d'applications (API) ou d'autres moyens et outils techniques appropriés permettant d'octroyer un accès à distance.

2. Lorsque cela est nécessaire pour évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au titre III, chapitre 2, et sur demande motivée, les autorités de surveillance du marché ont accès au code source du système d'IA.

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 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 une liste à la disposition du public sur le site web de l'autorité de contrôle nationale. 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 la protection des 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. Lorsqu'il existe un risque pour la protection des droits fondamentaux, 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 tarder 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 raisonnable et proportionné à la nature du risque, qu'elle prescrit.

   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 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 informe sans retard la Commission et les autres États membres de ces mesures.

6. Les informations visées au paragraphe 5 contiennent toutes les précisions disponibles, notamment en ce qui concerne les données 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, par le système d'IA, 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.

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 la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent à propos de la non-conformité du

système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans les trois mois suivant la réception 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.

9. Les autorités de surveillance du marché de tous les États membres veillent à ce que les mesures restrictives appropriées soient prises sans retard à l'égard du produit 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, 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 suivant la notification visée à l'article 65, paragraphe 5, et communique sa décision à l'État membre concerné.

2. Si la mesure nationale est jugée justifiée, tous les États membres prennent les mesures nécessaires pour s'assurer du retrait du système d'IA non conforme de leur marché et ils en informent la Commission. Si la mesure nationale est jugée non justifiée, l'État membre concerné la retire.

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 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 conforme au présent règlement comporte néanmoins un risque pour la santé ou la sécurité des personnes, pour le respect des obligations au titre du droit de l'Union ou du droit national visant à protéger les droits fondamentaux ou pour d'autres aspects relatifs à la protection de l'intérêt public, 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 dans un délai raisonnable, proportionné à la nature du risque, qu'elle prescrit.

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 des consultations avec les États membres et l'opérateur concerné 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 communique sa décision aux 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:

   (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.

TITRE IX

CODES DE CONDUITE

Article 69
Codes de conduite

1. La Commission et les États membres encouragent et facilitent l'élaboration de codes de conduite destinés à favoriser l'application volontaire aux systèmes d'IA autres que les systèmes d'IA à haut risque des exigences énoncées au titre III, chapitre 2, sur la base de spécifications et solutions techniques appropriées pour garantir le respect de ces exigences à la lumière de la destination des systèmes.

2. La Commission et le Comité encouragent et facilitent l'élaboration de codes de conduite destinés à favoriser l'application volontaire aux systèmes d'IA d'exigences liées, par exemple, à la viabilité 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 sur

la base d'objectifs clairs et d'indicateurs de performance clés pour mesurer la réalisation de ces objectifs.

3. Les codes de conduite 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. 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 le Comité prennent en considération les intérêts et les besoins spécifiques des petits fournisseurs et des jeunes entreprises lorsqu'ils encouragent et facilitent l'élaboration de codes de conduite.

TITRE X

CONFIDENTIALITÉ ET SANCTIONS

Article 70
Confidentialité

1. Les autorités nationales compétentes et les organismes notifiés associés à l'application du présent règlement respectent la confidentialité des informations et des données obtenues dans l'exécution 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) la mise en œuvre effective du présent règlement, notamment en ce qui concerne les inspections, les investigations ou les audits; c) les intérêts en matière de sécurité nationale et publique;

   (c) l'intégrité des procédures pénales ou administratives.

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 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.

   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 des organismes notifiés en matière d'échange d'informations et de diffusion de mises en garde et sur les obligations d'information incombant aux parties concernées en vertu du droit pénal des États membres.

4. La Commission et les États membres peuvent échanger, si nécessaire, des informations confidentielles avec les autorités de réglementation de pays tiers avec lesquels ils ont conclu des accords bilatéraux ou multilatéraux en matière de confidentialité garantissant un niveau de confidentialité approprié.

Article 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 des intérêts des petits fournisseurs et des jeunes entreprises, ainsi que de leur viabilité économique.

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

3. Les infractions suivantes font l'objet d'amendes administratives 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:

   (a) non-respect de l'interdiction frappant les pratiques en matière d'intelligence artificielle visées à l'article 5;

   (b) non-conformité du système d'IA avec les exigences énoncées à l'article 10.

4. 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 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.

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.

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;

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

(c) la taille et la part de marché de l'opérateur qui commet l'infraction.

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.

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. Les infractions suivantes font l'objet d'une amende administrative pouvant aller jusqu'à 500 000 EUR:

(a) non-respect de l'interdiction frappant les pratiques en matière d'intelligence artificielle visées à l'article 5;

(b) non-conformité du système d'IA avec les exigences énoncées à l'article 10.

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 4, à l'article 7, paragraphe 1, 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 indéterminée à partir du [*date d'entrée en vigueur du présent règlement*].

3. La délégation de pouvoir visée à l'article 4, à l'article 7, paragraphe 1, 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 4, de l'article 7, paragraphe 1, 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) nº 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. 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. 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. 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. La Commission évalue la nécessité de modifier la liste figurant à l'annexe III une fois par an après l'entrée en vigueur du présent règlement.

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 et 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, la Commission évalue l'impact et l'efficacité des codes de conduite destinés à favoriser l'application des exigences énoncées au titre III, chapitre 2, et éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à haut risque.

5. Aux fins des paragraphes 1 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 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 [*24 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 [*trois 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	*Le président*

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaine(s) politique(s) concerné(s)

1.3. La proposition/l'initiative porte sur:

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

1.4.2. Objectif(s) spécifique(s)

1.4.3. Résultat(s) et incidence(s) attendus

1.4.4. Indicateurs de performance

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

1.5.3. Leçons tirées d'expériences similaires

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

1.5.5 Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

1.6. Durée et incidence financière de la proposition/de l'initiative

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

2.3. Mesures de prévention des fraudes et irrégularités

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les crédits opérationnels

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

3.2.5. Participation de tiers au financement

3.3. Incidence estimée sur les recettes

FICHE FINANCIÈRE LÉGISLATIVE

1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

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

1.2. Domaine(s) politique(s) concerné(s)

Réseaux de communication, contenus et technologies;

marché intérieur, industrie, entrepreneuriat et PME.

L'incidence budgétaire concerne les nouvelles tâches confiées à la Commission, dont l'appui au Comité européen de l'intelligence artificielle.

Activité(s): façonner l'avenir numérique de l'Europe.

1.3. La proposition/l'initiative porte sur:

X **une action nouvelle**

☐ **une action nouvelle suite à un projet pilote/une action préparatoire**[64]

☐ **la prolongation d'une action existante**

☐ **une action réorientée vers une nouvelle action**

1.4. Objectif(s)

1.4.1. Objectif général / objectifs généraux

L'objectif général de l'intervention est de garantir le bon fonctionnement du marché unique en créant les conditions propices au développement et à l'utilisation d'une intelligence artificielle digne de confiance dans l'Union.

1.4.2. Objectif(s) spécifique(s)

Objectif spécifique nº 1

Définir des exigences spécifiques aux systèmes d'IA et des obligations pour tous les participants à la chaîne de valeur afin de garantir que les systèmes d'IA mis sur le marché et utilisés sont sûrs et respectent la législation en vigueur en matière de droits fondamentaux et les valeurs de l'Union.

Objectif spécifique nº 2

Garantir la sécurité juridique pour faciliter les investissements et l'innovation dans le domaine de l'IA en précisant clairement quelles exigences essentielles, obligations et procédures de (mise en) conformité doivent être respectées pour mettre ou utiliser un système d'IA sur le marché de l'Union.

Objectif spécifique nº 3

Renforcer la gouvernance et l'application effective de la législation existante en matière de droits fondamentaux et des exigences de sécurité applicables aux

[64] Tel(le) que visé(e) à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

systèmes d'IA en dotant les autorités concernées de nouvelles compétences et ressources et en leur fournissant des règles claires en ce qui concerne les procédures d'évaluation de la conformité et de contrôle ex post et la répartition des tâches de gouvernance et de surveillance entre les niveaux national et européen.

Objectif spécifique nº 4

Faciliter le développement d'un marché unique pour des applications d'IA légales, sûres et fiables et empêcher la fragmentation du marché en prenant des mesures au niveau de l'UE visant à fixer des exigences minimales relatives à la mise sur le marché de l'Union des systèmes d'IA et à leur utilisation, conformément à la législation existante en matière de droits fondamentaux et de sécurité.

1.4.3. Résultat(s) et incidence(s) attendus

Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.

Les fournisseurs d'IA devraient bénéficier d'un ensemble d'exigences minimal, mais clair, créant une sécurité juridique et garantissant l'accès à l'ensemble du marché unique.

Les utilisateurs d'IA devraient bénéficier de la sécurité juridique quant au fait que les systèmes d'IA à haut risque qu'ils achètent sont conformes à la législation et aux valeurs européennes.

Les consommateurs devraient en tirer profit en raison de la réduction du risque d'atteinte à leur sécurité ou de violation de leurs droits fondamentaux.

1.4.4. Indicateurs de performance

Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative.

Indicateur nº 1

Nombre d'incidents graves ou de performances en matière d'IA qui constituent un incident grave ou une violation des obligations en matière de droits fondamentaux (sur une base semestrielle) par domaine d'application et calculé a) en termes absolus, b) en pourcentage des applications déployées et c) en pourcentage des citoyens concernés.

Indicateur nº 2

a) Total des investissements dans le domaine de l'IA dans l'UE (annuel)

b) Total des investissements dans le domaine de l'IA par État membre (annuel)

c) Pourcentage des entreprises utilisant l'IA (annuel)

d) Part des PME utilisant l'IA (annuelle)

a) et b) seront calculés sur la base de sources officielles et comparés aux estimations du secteur privé.

c) et d) seront collectés au moyen d'enquêtes régulières auprès des entreprises.

1.5. Justification(s) de la proposition/de l'initiative

1.5.1. Besoin(s) à satisfaire à court ou à long terme, assorti(s) d'un calendrier détaillé pour la mise en œuvre de l'initiative

Le règlement devrait être pleinement applicable un an et demi après son adoption. Toutefois, des éléments de la structure de gouvernance devraient être en place avant cette date. En particulier, les États membres nomment des autorités existantes et/ou établissent de nouvelles autorités pour accomplir les tâches énoncées dans la législation avant cette date et le Comité européen de l'intelligence artificielle devrait être mis en place et effectif. Au moment de l'applicabilité, la base de données européenne des systèmes d'IA devrait être pleinement opérationnelle. Parallèlement au processus d'adoption, il est donc nécessaire que le développement de la base de données soit achevé lors de l'entrée en vigueur du règlement.

1.5.2. Valeur ajoutée de l'intervention de l'Union (celle-ci peut résulter de différents facteurs, par exemple gains de coordination, sécurité juridique, efficacité accrue, complémentarités, etc.). Aux fins du présent point, on entend par «valeur ajoutée de l'intervention de l'Union» la valeur découlant de l'intervention de l'Union qui vient

s'ajouter à la valeur qui, sans cela, aurait été générée par la seule action des États membres.

L'émergence d'un cadre disparate de règles nationales potentiellement divergentes entravera la fourniture ininterrompue de systèmes d'IA dans l'ensemble de l'UE et ne garantit pas la sécurité et la protection des droits fondamentaux et des valeurs de l'Union dans les différents États membres. Une action législative commune de l'UE en matière d'IA pourrait stimuler le marché intérieur et offre à l'industrie européenne des possibilités importantes pour se doter d'un avantage concurrentiel sur la scène mondiale et faire des économies d'échelle qui ne peuvent être réalisées par les seuls États membres.

1.5.3. Leçons tirées d'expériences similaires

La directive 2000/31/CE sur le commerce électronique constitue le cadre principal pour le fonctionnement du marché unique et la surveillance des services numériques et établit une structure de base pour un mécanisme de coopération générale entre États membres, couvrant en principe l'ensemble des exigences applicables aux services numériques. L'évaluation de ladite directive a mis en évidence des lacunes concernant plusieurs aspects de ce mécanisme de coopération, dont des aspects procéduraux importants tels que l'absence de délais de réponse clairs pour les États membres, associée à un manque général de réactivité aux demandes de leurs homologues. Cela a entraîné au fil des années un manque de confiance entre les États membres pour ce qui est de répondre aux préoccupations concernant les fournisseurs proposant des services numériques transfrontières. L'évaluation de la directive a montré le besoin de définir un ensemble différencié de règles et d'exigences au niveau européen. Pour cette raison, la mise en œuvre des obligations spécifiques établies dans le présent règlement nécessiterait un mécanisme de coopération dédié au niveau de l'UE, doté d'une structure de gouvernance prévoyant une coordination des organes responsables spécifiques au niveau de l'UE.

1.5.4. Compatibilité avec le cadre financier pluriannuel et synergies éventuelles avec d'autres instruments appropriés

Le règlement établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union définit un nouveau cadre commun d'exigences applicables aux systèmes d'IA, qui va bien au-delà du cadre prévu par la législation existante. Pour cette raison, la présente proposition doit mettre en place une nouvelle fonction réglementaire et de coordination nationale et européenne.

En ce qui concerne les synergies éventuelles avec d'autres instruments appropriés, le rôle des autorités notifiantes au niveau national peut être assumé par les autorités nationales exerçant des fonctions similaires au titre d'autres règlements de l'UE.

En outre, le renforcement de la confiance dans l'IA et, partant, la promotion des investissements dans le développement et l'adoption de celle-ci complètent l'Europe numérique, dont l'une des cinq priorités consiste à encourager la diffusion de l'IA.

1.5.5. Évaluation des différentes possibilités de financement disponibles, y compris des possibilités de redéploiement

Le personnel sera redéployé. Les autres coûts seront financés par l'enveloppe consacrée au programme pour une Europe numérique, l'objectif du présent règlement, à savoir garantir une IA digne de confiance, contribuant directement à

l’un des principaux objectifs de l’Europe numérique: accélérer le développement et le déploiement de l’IA en Europe.

1.6. Durée et incidence financière de la proposition/de l'initiative

☐ **durée limitée**

– ☐ en vigueur à partir de [JJ/MM]AAAA jusqu'en/au [JJ/MM]AAAA

– ☐ incidence financière de AAAA jusqu'en AAAA pour les crédits d'engagement et de AAAA jusqu'en AAAA pour les crédits de paiement.

X **durée illimitée**

– Mise en œuvre avec une période de montée en puissance de un/deux (à confirmer) an(s),

– puis un fonctionnement en rythme de croisière au-delà.

1.7. Mode(s) de gestion prévu(s)[65]

X **Gestion directe** par la Commission

– ☐ dans ses services, y compris par l'intermédiaire de son personnel dans les délégations de l'Union;

– ☐ par les agences exécutives

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant des tâches d'exécution budgétaire:

– ☐ à des pays tiers ou des organismes qu'ils ont désignés;

– ☐ à des organisations internationales et à leurs agences (à préciser);

– ☐ à la BEI et au Fonds européen d'investissement;

– ☐ aux organismes visés aux articles 70 et 71 du règlement financier;

– ☐ à des organismes de droit public;

– ☐ à des organismes de droit privé investis d'une mission de service public, pour autant qu'ils présentent les garanties financières suffisantes;

– ☐ à des organismes de droit privé d'un État membre qui sont chargés de la mise en œuvre d'un partenariat public-privé et présentent les garanties financières suffisantes;

– ☐ à des personnes chargées de l'exécution d'actions spécifiques relevant de la PESC, en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné.

– *Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

Remarques

[65] Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

Préciser la fréquence et les conditions de ces dispositions.

Le règlement sera réexaminé et évalué dans un délai de cinq ans à compter de son entrée en vigueur. La Commission présentera au Parlement européen, au Conseil et au Comité économique et social européen un rapport sur les conclusions de cette évaluation.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du (des) mode(s) de gestion, du (des) mécanisme(s) de mise en œuvre des financements, des modalités de paiement et de la stratégie de contrôle proposée

Le règlement établit une nouvelle politique en ce qui concerne les règles harmonisées pour la fourniture de systèmes d'intelligence artificielle au sein du marché intérieur tout en garantissant le respect de la sécurité et des droits fondamentaux. Ces nouvelles règles nécessitent un mécanisme de contrôle de la cohérence pour l'application transfrontière des obligations prévues par le présent règlement, sous la forme d'un nouveau groupe consultatif chargé de coordonner les activités des autorités nationales.

Afin qu'ils soient en mesure d'assumer ces nouvelles tâches, il est nécessaire de doter les services de la Commission des ressources appropriées. Le contrôle de l'application du nouveau règlement devrait nécessiter 10 ETP (5 ETP pour l'appui aux activités du Comité et 5 ETP pour le Contrôleur européen de la protection des données agissant en tant qu'organisme notifiant pour les systèmes d'IA déployés par un organe de l'Union européenne).

2.2.2. Informations sur les risques recensés et sur le(s) système(s) de contrôle interne mis en place pour les atténuer

Pour faire en sorte que les membres du Comité aient la possibilité d'effectuer des analyses éclairées sur la base d'éléments factuels, il est prévu que le Comité soit appuyé par la structure administrative de la Commission et qu'un groupe d'experts soit créé en vue d'apporter une expertise supplémentaire s'il y a lieu.

2.2.3. Estimation et justification du rapport coût/efficacité des contrôles (rapport «coûts du contrôle ÷ valeur des fonds gérés concernés»), et évaluation du niveau attendu de risque d'erreur (lors du paiement et lors de la clôture)

En ce qui concerne les frais de réunion, compte tenu du faible montant par transaction (par exemple, remboursement des frais de déplacement d'un délégué pour une réunion), les procédures de contrôle types semblent suffisantes. Pour ce qui est du développement de la base de données, la procédure d'attribution de contrat prévoit un solide système de contrôle interne à la DG CNECT grâce à des activités de passation de marchés centralisées.

2.3. Mesures de prévention des fraudes et irrégularités

Préciser les mesures de prévention et de protection existantes ou envisagées, au titre de la stratégie antifraude par exemple.

Les mesures de prévention des fraudes existantes applicables à la Commission couvriront les crédits supplémentaires nécessaires aux fins du présent règlement.

3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

- Lignes budgétaires existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

Rubrique du cadre financier pluriannuel	Ligne budgétaire	Nature de la dépense	Contribution			
	Numéro	CD/CND[66].	de pays AELE[67]	de pays candidats[68]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier
7	20 02 06 Dépenses de gestion	CND	NON	NON	NON	NON
1	02 04 03 Intelligence artificielle	CD	OUI	NON	NON	NON
1	02 01 30 01 Dépenses d'appui pour le «programme pour une Europe numérique»	CND	OUI	NON	NON	NON

3.2. Incidence financière estimée de la proposition sur les crédits

3.2.1. Synthèse de l'incidence estimée sur les dépenses concernant les crédits opérationnels

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels

– X La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

[66] CD = crédits dissociés/CND = crédits non dissociés.

[67] AELE: Association européenne de libre-échange.

[68] Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

En Mio EUR (à la 3e décimale)

Rubrique du cadre financier pluriannuel	1	

DG: CNECT				Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**[69]	**TOTAL**	
• Crédits opérationnels											
Ligne budgétaire[70] 02 04 03		Engagements	(1a)		1,000						**1,000**
		Paiements	(2 a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Ligne budgétaire		Engagements	(1b)								
		Paiements	(2b)								
Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[71]											
Ligne budgétaire 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
TOTAL des crédits pour la DG CNECT		Engagements	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Paiements	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 À titre indicatif et en fonction des disponibilités budgétaires.

70 Selon la nomenclature budgétaire officielle.

71 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

• TOTAL des crédits opérationnels	Engagements	(4)		1,000						**1,000**
	Paiements	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
TOTAL des crédits pour la RUBRIQUE 1 du cadre financier pluriannuel	Engagements	=4+ 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Paiements	=5+ 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Si plusieurs rubriques sont concernées par la proposition/l'initiative, dupliquer la section qui précède:

• TOTAL des crédits opérationnels (toutes les rubriques opérationnelles)	Engagements	(4)								
	Paiements	(5)								
• TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques (toutes les rubriques opérationnelles)		(6)								
TOTAL des crédits pour les RUBRIQUES 1 à 6 du cadre financier pluriannuel (Montant de référence)	Engagements	=4+ 6								
	Paiements	=5+ 6								

Rubrique du cadre financier pluriannuel	**7**	«Dépenses administratives»

Cette partie est à compléter en utilisant les «données budgétaires de nature administrative», à introduire d'abord dans l'annexe de la fiche financière législative (annexe 5 des règles internes), à charger dans DECIDE pour les besoins de la consultation interservices.

En Mio EUR (à la 3e décimale)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	**Année 2027**	**Après 2027**[72]	**TOTAL**
DG: CNECT								
• Ressources humaines		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Autres dépenses administratives		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
TOTAL DG CNECT	**Crédits**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Contrôleur européen de la protection des données								
• Ressources humaines		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Autres dépenses administratives								
TOTAL CEPD	**Crédits**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
TOTAL des crédits pour la RUBRIQUE 7 du cadre financier pluriannuel	(Total engagements = Total paiements)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

En Mio EUR (à la 3e décimale)

		Année **2022**	Année **2023**	Année **2024**	Année **2025**	**Année 2026**	**Année 2027**		**TOTAL**
TOTAL des crédits	Engagements		2,770	1,770	1,770	1,770	1,770		**9,850**

[72] Tous les chiffres dans cette colonne sont indicatifs et sous réserve de la continuation des programmes et de la disponibilité des crédits

pour les RUBRIQUES 1 à 7 du cadre financier pluriannuel	Paiements		2,370	1,870	1,870	1,870	1,870	**9,850**

3.2.2. Estimation des réalisations financées avec des crédits opérationnels

Crédits d'engagement en Mio EUR (à la 3e décimale)

Indiquer les objectifs et les réalisations ⇩			Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		Après **2027**[73]		**TOTAL**	
	RÉALISATIONS (outputs)																	
	Type	Coût moyen	Non	Coût	Non	Coût	Non	Coût	Non	Coût	Non	Coût	Non	Coût	Non	Coût	Nbre total	Coût total
OBJECTIF SPÉCIFIQUE nº 1[74]…																		
Base de données					1	1,000	1		1		1		1		1	0,100	1	1,000
Réunions —					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Activités de communication					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Sous-total objectif spécifique nº 1																		
OBJECTIF SPÉCIFIQUE nº 2…																		
- Réalisation																		
Sous-total objectif spécifique nº 2																		
TOTAUX					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Tous les chiffres dans cette colonne sont indicatifs et sous réserve de la continuation des programmes et de la disponibilité des crédits

[74] Tel que décrit au point 1.4.2. «Objectif(s) spécifique(s)…».

3.2.3. Synthèse de l'incidence estimée sur les crédits administratifs

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– X La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En Mio EUR (à la 3e décimale)

	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**Tous les ans après 2027**[75]	**TOTAL**
RUBRIQUE 7 du cadre financier pluriannuel								
Ressources humaines		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Autres dépenses administratives		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Sous-total RUBRIQUE 7 du cadre financier pluriannuel		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Hors RUBRIQUE 7[76] **du cadre financier pluriannuel**								
Ressources humaines								
Autres dépenses de nature administrative		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Sous-total hors RUBRIQUE 7 du cadre financier pluriannuel		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
TOTAL		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

75 Tous les chiffres dans cette colonne sont indicatifs et sous réserve de la continuation des programmes et de la disponibilité des crédits.

76 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

Les besoins en crédits pour les ressources humaines et les autres dépenses de nature administrative seront couverts par les crédits de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

3.2.3.1. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– X La proposition/l'initiative engendre l'utilisation de ressources humaines, comme expliqué ci-après:

Estimation à exprimer en équivalents temps plein

.		Année **2023**	**Année 2024**	**Année 2025**	**2026**	**2027**	**Après 2027**[77]	
• Emplois du tableau des effectifs (fonctionnaires et agents temporaires)								
20 01 02 01 (au siège et dans les bureaux de représentation de la Commission)		10	10	10	10	10	10	
20 01 02 03 (en délégation)								
01 01 01 01 (recherche indirecte)								
01 01 01 11 (recherche directe)								
Autres lignes budgétaires (à préciser)								
• Personnel externe (en équivalents temps plein: ETP)[78]								
20 02 01 (AC, END, INT de l'enveloppe globale)								
20 02 03 (AC, AL, END, INT et JPD dans les délégations)								
XX 01 xx **yy zz** [79]	- au siège							
	- en délégation							
01 01 01 02 (AC, END, INT sur recherche indirecte)								
01 01 01 12 (AC, END, INT sur recherche directe)								
Autres lignes budgétaires (à préciser)								
TOTAL		**10**	**10**	**10**	**10**	**10**	**10**	

XX est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires existantes.

Le CEPD devrait fournir la moitié des ressources nécessaires.

Description des tâches à effectuer:

Fonctionnaires et agents temporaires	Afin de préparer un total de 13 à 16 réunions, de rédiger des rapports, de poursuivre les travaux au niveau politique, par exemple en ce qui concerne les futures modifications de la liste des applications d'IA à haut risque, et d'entretenir des relations avec les autorités des États membres, quatre AD ETP et 1 AST ETP seront nécessaires. En ce qui concerne les systèmes d'IA développés par les institutions de l'UE, le Contrôleur européen de la protection des données est responsable. À la lumière de l'expérience acquise, on peut estimer que 5 AD ETP sont nécessaires pour assumer les

[77] Tous les chiffres dans cette colonne sont indicatifs et sous réserve de la continuation des programmes et de la disponibilité des crédits.

[78] AC = agent contractuel; AL = agent local; END = expert national détaché; INT = intérimaire; JPD = jeune professionnel en délégation.

[79] Sous-plafonds de personnel externe financés sur crédits opérationnels (anciennes lignes «BA»).

	responsabilités du CEPD dans le cadre du projet de législation.
Personnel externe	

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/l'initiative:

– X peut être intégralement financée par voie de redéploiement au sein de la rubrique concernée du cadre financier pluriannuel (CFP).

Aucune reprogrammation n'est nécessaire.

– ☐ nécessite l'utilisation de la marge non allouée sous la rubrique correspondante du CFP et/ou le recours aux instruments spéciaux comme le prévoit le règlement CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées, les montants correspondants et les instruments dont le recours est proposé.

– ☐ nécessite une révision du CFP.

Expliquez le besoin, en précisant les rubriques et lignes budgétaires concernées et les montants correspondants.

3.2.5. Participation de tiers au financement

La proposition/l'initiative:

– X ne prévoit pas de cofinancement par des tierces parties

– ☐ prévoit le cofinancement par des tierces parties estimé ci- après:

Crédits en Mio EUR (à la 3e décimale)

	Année **N**[80]	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)			Total
Préciser l'organisme de cofinancement								
TOTAL crédits cofinancés								

[80] L'année N est l'année du début de la mise en œuvre de la proposition/de l'initiative. Veuillez remplacer «N» par la première année de mise en œuvre prévue (par exemple: 2021). Procédez de la même façon pour les années suivantes.

3.3. Incidence estimée sur les recettes

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

– ☐ La proposition/l'initiative a une incidence financière décrite ci-après:

– ☐ sur les autres recettes

– ☐ sur les autres recettes

– Veuillez indiquer si les recettes sont affectées à des lignes de dépenses ☐

En Mio EUR (à la 3e décimale)

Ligne budgétaire de recettes:	Montants inscrits pour l'exercice en cours	Incidence de la proposition/de l'initiative[81]						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Insérer autant d'années que nécessaire, pour refléter la durée de l'incidence (cf. point 1.6)		
Article …….								

Pour les recettes affectées, préciser la (les) ligne(s) budgétaire(s) de dépenses concernée(s).

Autres remarques (relatives, par exemple, à la méthode/formule utilisée pour le calcul de l'incidence sur les recettes ou toute autre information).

[81] En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sur le sucre), les montants indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % de frais de perception.