COMMISSION
EUROPÉENNE

Bruxelles, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

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

MÉMORANDUM EXPLICATIF

1. CONTEXTE DE LA PROPOSITION

1.1. Raisons et objectifs de la proposition

Le présent exposé des motifs accompagne la proposition de règlement établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'intelligence artificielle). L'intelligence artificielle (IA) est une famille de technologies qui évolue rapidement et qui peut apporter un large éventail d'avantages économiques et sociétaux dans tout le spectre des industries et des activités sociales. En améliorant les prévisions, en optimisant les opérations et l'affectation des ressources et en personnalisant la prestation de services, l'utilisation de l'intelligence artificielle peut favoriser des résultats bénéfiques sur le plan social et environnemental et procurer des avantages concurrentiels essentiels aux entreprises et à l'économie européenne. Cette action est particulièrement nécessaire dans les secteurs à fort impact, notamment le changement climatique, l'environnement et la santé, le secteur public, la finance, la mobilité, les affaires intérieures et l'agriculture. Toutefois, les mêmes éléments et techniques qui alimentent les avantages socio-économiques de l'IA peuvent également entraîner de nouveaux risques ou des conséquences négatives pour les individus ou la société. Compte tenu de la rapidité de l'évolution technologique et des défis possibles, l'UE s'est engagée à s'efforcer d'adopter une approche équilibrée. Il est dans l'intérêt de l'Union de préserver le leadership technologique de l'UE et de veiller à ce que les Européens puissent bénéficier des nouvelles technologies développées et fonctionnant dans le respect des valeurs, des droits fondamentaux et des principes de l'Union.

Cette proposition répond à l'engagement politique de la présidente von der Leyen, qui a annoncé dans ses orientations politiques pour la Commission 2019-2024 "Une Union qui aspire à plus "[1], que la Commission proposerait une législation pour une approche européenne coordonnée sur les implications humaines et éthiques de l'IA. Suite à cette annonce, la Commission a publié le 19 février 2020 le Livre blanc sur l'IA - Une approche européenne de l'excellence et de la confiance2. Le livre blanc présente des options politiques sur la manière d'atteindre le double objectif de promouvoir l'adoption de l'IA et de traiter les risques associés à certaines utilisations de cette technologie. La présente proposition vise à mettre en œuvre le deuxième objectif, à savoir le développement d'un écosystème de confiance, en proposant un cadre juridique pour une IA digne de confiance. La proposition est fondée sur les valeurs et les droits fondamentaux de l'UE et vise à donner aux personnes et aux autres utilisateurs la confiance nécessaire pour adopter des solutions basées sur l'IA, tout en encourageant les entreprises à les développer. L'IA devrait être un outil pour les gens et être une force pour le bien de la société, dans le but ultime d'accroître le bien-être humain. Les règles relatives à l'IA disponible sur le marché de l'Union ou affectant d'une autre manière les personnes dans l'Union devraient donc être centrées sur l'humain, afin que les personnes puissent avoir confiance que la technologie est utilisée d'une manière sûre et conforme à la loi, y compris le respect des droits fondamentaux. À la suite de la publication du livre blanc, la Commission a lancé une vaste consultation des parties prenantes, qui a suscité un grand intérêt de la part d'un grand nombre d'entre elles, largement favorables à une intervention réglementaire pour répondre aux défis et aux préoccupations soulevés par l'utilisation croissante de l'IA.

La proposition répond également aux demandes explicites du Parlement européen (PE) et du Conseil européen, qui ont exprimé à plusieurs reprises le besoin d'une action législative pour garantir le bon fonctionnement du marché intérieur des systèmes d'intelligence artificielle ("systèmes d'IA"), où les avantages et les risques de l'IA sont traités de manière adéquate au niveau de l'Union. Elle soutient l'objectif de faire de l'Union un leader mondial dans le développement de systèmes d'intelligence artificielle sûrs, dignes de confiance et éthiques.

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf

[2] Commission européenne, Livre blanc sur l'intelligence artificielle - Une approche européenne de l'excellence et de la confiance, COM(2020) 65 final, 2020.

intelligence comme l'a déclaré le Conseil européen3 et assure la protection des principes éthiques comme l'a spécifiquement demandé le Parlement européen4.

En 2017, le Conseil européen a appelé à un "sentiment d'urgence pour faire face aux tendances émergentes", y compris "des questions telles que l'intelligence artificielle [...], tout en garantissant un niveau élevé de protection des données, des droits numériques et des normes éthiques "[5]. Dans ses conclusions de 2019 sur le plan coordonné relatif au développement et à l'utilisation de l'intelligence artificielle Made in Europe6, le Conseil a en outre souligné l'importance de veiller à ce que les droits des citoyens européens soient pleinement respectés et a appelé à un réexamen de la législation pertinente existante afin qu'elle soit adaptée aux nouvelles possibilités et aux nouveaux défis soulevés par l'IA. Le Conseil européen a également demandé que soient clairement déterminées les applications de l'IA qui doivent être considérées comme à haut risque7.

Les conclusions les plus récentes, datant du 21 octobre 2020, appellent en outre à se pencher sur l'opacité, la complexité, la partialité, un certain degré d'imprévisibilité et le comportement partiellement autonome de certains systèmes d'IA, afin de garantir leur compatibilité avec les droits fondamentaux et de faciliter l'application des règles juridiques8.

Le Parlement européen a également entrepris une quantité considérable de travaux dans le domaine de l'IA. En octobre 2020, il a adopté un certain nombre de résolutions relatives à l'IA, notamment sur l'éthique9, la responsabilité10 et le droit d'auteur11. En 2021, celles-ci ont été suivies de résolutions sur l'IA en matière pénale12 et dans l'éducation, la culture et le secteur audiovisuel13. La résolution du PE sur un cadre des aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes recommande spécifiquement à la Commission de proposer une action législative pour exploiter les possibilités et les avantages de l'IA, mais aussi pour garantir la protection des principes éthiques. La résolution comprend un texte de proposition législative pour un règlement sur les principes éthiques pour le développement, le déploiement et 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 TFUE, la présente résolution a été adoptée par le Parlement européen.

3Conseil 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 sur un cadre des aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, 2020/2012(INL).

5Conseil européen, *réunion duConseileuropéen(19octobre2017)-Conclusion* EUCO 14/17, 2017, p. 8.

6Conseil de l'Union européenne, *Intelligenceartificielleb)Conclusionsrelatives auplancoordonnésur l'intelligence artificielle-Adoption* 6177/19, 2019.

7Conseil européen, *RéunionextraordinaireduConseileuropéen(1er et2octobre2020)-Conclusions* EUCO 13/20, 2020.

8Conseil de l'Union européenne, *Conclusions de la présidence - La Charte des droits fondamentaux dans le contextede l'intelligenceartificielleet de latransformationnumérique*, 11481/20, 2020.

9Résolution du Parlement européen du 20 octobre 2020 sur un cadre des 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 d'intelligence artificielle, 2020/2015(INI).

12Projet de rapport du Parlement européen, L'intelligence artificielle en droit pénal et son utilisation par les autorités policières et judiciaires en matière pénale, 2020/2016(INI).

13Projet de rapport du Parlement européen, L'intelligence artificielle dans l'éducation, la culture et le secteur audiovisuel, 2020/2017(INI). À cet égard, la Commission a adopté le plan d'action pour l'éducation numérique 2021-2027 : Repenser l'éducation et la formation à l'ère numérique, qui prévoit l'élaboration de lignes directrices éthiques en matière d'utilisation de l'IA et des données dans l'éducation

- communication de la Commission COM(2020) 624 final.

La proposition tient compte de la résolution susmentionnée du Parlement européen dans le plein respect des principes de proportionnalité, de subsidiarité et de mieux légiférer.

Dans ce contexte politique, la Commission présente la proposition de cadre réglementaire sur l'intelligence artificielle avec les **objectifs spécifiques** suivants :

- veiller à ce que les systèmes d'IA mis sur le marché de l'Union et utilisés soient sûrs et respectent la législation existante sur les droits fondamentaux et les valeurs de l'Union ;
- garantir la sécurité juridique pour faciliter l'investissement et l'innovation dans l'IA ;
- améliorer la gouvernance et l'application effective de la législation existante sur les droits fondamentaux et les exigences de sécurité applicables aux systèmes d'IA ;
- faciliter le développement d'un marché unique pour les applications d'IA légales, sûres et dignes de confiance et prévenir la fragmentation du marché.

Pour atteindre ces objectifs, cette proposition présente une approche réglementaire horizontale équilibrée et proportionnée de l'IA, qui se limite aux exigences minimales nécessaires pour faire face aux risques et aux problèmes liés à l'IA, sans contraindre ou entraver indûment le développement technologique ni augmenter de manière disproportionnée le coût de la mise sur le marché de solutions d'IA. La proposition établit un cadre juridique solide et flexible. D'une part, elle est complète et évolutive dans ses choix réglementaires fondamentaux, notamment les exigences fondées sur des principes auxquelles les systèmes d'IA doivent se conformer. D'autre part, elle met en place un système réglementaire proportionné, centré sur une approche réglementaire fondée sur les risques bien définie qui ne crée pas de restrictions inutiles aux échanges, l'intervention juridique étant adaptée aux situations concrètes dans lesquelles il existe une cause justifiée de préoccupation ou dans lesquelles une telle préoccupation peut raisonnablement être anticipée dans un avenir proche. En même temps, le cadre juridique comprend des mécanismes souples qui lui permettent d'être adapté de manière dynamique à mesure que la technologie évolue et que de nouvelles situations préoccupantes apparaissent.

La proposition fixe des règles harmonisées pour le développement, la mise sur le marché et l'utilisation des systèmes d'IA dans l'Union, selon une approche proportionnelle fondée sur le risque. Elle propose une définition unique et évolutive de l'IA. Certaines pratiques d'IA particulièrement nuisibles sont interdites car elles sont contraires aux valeurs de l'Union, tandis que des restrictions et des garanties spécifiques sont proposées en ce qui concerne certaines utilisations des systèmes d'identification biométrique à distance à des fins répressives. La proposition établit une solide méthodologie de risque pour définir les systèmes d'IA "à haut risque" qui présentent des risques importants pour la santé et la sécurité ou les droits fondamentaux des personnes. Ces systèmes d'IA devront se conformer à une série d'exigences horizontales obligatoires pour une IA digne de confiance et suivre des procédures d'évaluation de la conformité avant de pouvoir être mis sur le marché de l'Union. Des obligations prévisibles, proportionnées et claires sont également imposées aux fournisseurs et aux utilisateurs de ces systèmes pour garantir la sécurité et le respect de la législation existante protégeant les droits fondamentaux tout au long du cycle de vie des systèmes d'IA. Pour certains systèmes d'IA spécifiques, seules des obligations minimales de transparence sont proposées, notamment en cas d'utilisation de chatbots ou de "faux profonds".

Les règles proposées seront appliquées par le biais d'un système de gouvernance au niveau des États membres, s'appuyant sur les structures déjà existantes, et d'un mécanisme de coopération au niveau de l'Union avec la création d'un Conseil européen de l'intelligence artificielle. Des mesures supplémentaires sont également proposées pour soutenir l'innovation, notamment par le biais de bacs à sable réglementaires pour l'IA et d'autres mesures visant à réduire la charge réglementaire et à soutenir les petites et moyennes entreprises ("PME") et les start-ups.

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

La nature horizontale de la proposition exige une cohérence totale avec la législation existante de l'Union applicable aux secteurs où des systèmes d'IA à haut risque sont déjà utilisés ou susceptibles de l'être dans un avenir proche.

La cohérence est également 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 des sexes. La proposition est sans préjudice et complète le règlement général sur la protection des données (règlement (UE) 2016/679) et la directive relative à l'application de la loi (directive (UE) 2016/680) par un ensemble de règles harmonisées applicables à la conception, au développement et à l'utilisation de certains systèmes d'IA à haut risque et par des restrictions à certaines utilisations des systèmes d'identification biométrique à distance. En outre, la proposition complète le droit de l'Union existant en matière de non-discrimination par des exigences spécifiques qui visent à minimiser le risque de discrimination algorithmique, notamment en ce qui concerne la conception et la qualité des ensembles de données utilisés pour le développement des systèmes d'IA complétés par des obligations en matière de tests, de gestion des risques, de documentation et de surveillance humaine 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 qui sont des composants de sécurité des produits, la présente proposition sera intégrée dans la législation sectorielle existante en matière de sécurité afin de garantir la cohérence, d'éviter les doubles emplois et de minimiser les charges supplémentaires. En particulier, en ce qui concerne les systèmes d'IA à haut risque liés à des produits couverts par la législation sur le nouveau cadre législatif (NCL) (par exemple, les machines, les dispositifs médicaux, les jouets), les exigences relatives aux systèmes d'IA énoncées dans la présente proposition seront vérifiées dans le cadre des procédures d'évaluation de la conformité existantes au titre de la législation NCL pertinente. En ce qui concerne l'interaction des exigences, si les risques de sécurité spécifiques aux systèmes d'IA sont censés être couverts par les exigences de la présente proposition, la législation du NLF vise à garantir la sécurité globale du produit final et peut donc contenir des exigences spécifiques concernant l'intégration sûre d'un système d'IA dans le produit final. La proposition de règlement sur les machines, qui est adoptée le même jour que la présente proposition, reflète pleinement cette approche. En ce qui concerne les systèmes d'IA à haut risque liés à des produits couverts par la législation pertinente de l'ancienne approche (par exemple, l'aviation, les voitures), cette proposition ne s'appliquerait pas directement. Toutefois, les exigences essentielles ex ante pour les systèmes d'IA à haut risque énoncées dans la présente proposition devront être prises en compte lors de l'adoption de la législation d'application ou déléguée pertinente au titre de ces actes.

En ce qui concerne les systèmes d'IA fournis ou utilisés par des établissements de crédit réglementés, les autorités chargées de la surveillance de la législation de l'Union sur les services financiers devraient être désignées comme autorités compétentes pour la surveillance des exigences de la présente proposition, afin de garantir une application cohérente des obligations prévues par la présente proposition et par la législation de l'Union sur les 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 encore 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 prévues par la directive 2013/36/UE concernant l'accès à l'activité des établissements de crédit et le contrôle prudentiel14.

[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. 338-436.

Cette proposition est également cohérente avec la législation de l'Union applicable aux services, y compris les services intermédiaires réglementés par la directive 2000/31/CE15 sur le commerce électronique et la récente proposition de la Commission concernant la loi sur les services numériques (ASN)[16].

En ce qui concerne les systèmes d'IA qui sont des composants de systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice gérés par l'Agence de l'Union européenne pour la gestion opérationnelle des systèmes d'information à grande échelle (eu-LISA), la proposition ne s'appliquera pas aux systèmes d'IA qui ont été mis sur le marché ou mis en service avant l'expiration d'un délai d'un an à compter de la date d'application du présent règlement, sauf si le remplacement ou la modification de ces actes juridiques entraîne un changement significatif de la conception ou de la finalité du ou des systèmes d'IA concernés.

1.3. Cohérence avec les autres politiques de l'Union

La proposition fait partie d'un ensemble plus vaste de mesures visant à résoudre les problèmes posés par le développement et l'utilisation de l'IA, comme l'examine le Livre blanc sur l'IA. La cohérence et la complémentarité sont donc assurées avec d'autres initiatives en cours ou prévues de la Commission qui visent également à résoudre ces problèmes, notamment la révision de la législation sectorielle sur les produits (par exemple, la directive "Machines", la directive sur la sécurité générale des produits) et les initiatives qui traitent des questions de responsabilité liées aux nouvelles technologies, y compris les systèmes d'IA. Ces initiatives s'appuieront sur la présente proposition et la compléteront afin d'apporter une clarté juridique et de favoriser le développement d'un écosystème de confiance dans l'IA en Europe.

La proposition est également cohérente avec la stratégie numérique globale de la Commission dans sa contribution à la promotion d'une technologie au service des personnes, l'un des trois principaux piliers de l'orientation politique et des objectifs annoncés dans la communication "Donner forme à l'avenir numérique de l'Europe "[17] . Elle établit un cadre cohérent, efficace et proportionné pour garantir que l'IA soit développée dans le respect des droits des personnes et en gagnant leur confiance, afin que l'Europe soit adaptée à l'ère numérique et que les dix prochaines années deviennent la **décennie numérique18**.

En outre, la promotion de l'innovation axée sur l'IA est étroitement liée à la **loi sur la gouvernance des données19, à** la **directive sur les données ouvertes20** et à d'autres initiatives relevant de la **stratégie de l'UE en matière de données21**, qui établiront des mécanismes et des services de confiance pour la réutilisation, le partage et la mise en commun des données qui sont essentielles pour le développement de modèles d'IA axés sur les données de haute qualité.

La proposition renforce également de manière significative le rôle de l'Union pour contribuer à l'élaboration de normes et de standards mondiaux et promouvoir une IA digne de confiance et conforme aux valeurs et aux intérêts de l'Union. Elle fournit à l'Union une base solide pour s'engager davantage avec ses partenaires extérieurs, y compris les pays tiers, et dans les forums internationaux sur les questions relatives à l'IA.

---

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.

16 Voir Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant un marché unique des services numériques (loi sur les services numériques) et modifiant la directive 2000/31/CE COM/2020/825 final.

17 Communication de la Commission, Façonner l'avenir numérique de l'Europe, COM/2020/67 final.

18 Boussolenumérique2030:lavoie européennepourladécennienumérique.

19 Proposition de règlement sur la gouvernance européenne des données (loi sur la gouvernance des données) COM/2020/767.

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. 56-83.

[21] Communication de la Commission, Une stratégie européenne pour les données COM/2020/66 final.

2.

2.1. Base juridique

La base juridique de la proposition est en premier lieu l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), qui prévoit l'adoption de mesures visant à assurer l'établissement et le fonctionnement du marché intérieur.

Cette proposition constitue un élément essentiel de la stratégie de l'UE pour un marché unique numérique. L'objectif premier de cette proposition est d'assurer le bon fonctionnement du marché intérieur en fixant 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 faisant appel à des technologies d'IA ou fournis en tant que systèmes d'IA autonomes. Certains États membres envisagent déjà d'adopter des règles nationales pour garantir que l'IA est sûre et qu'elle est développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Cela entraînera probablement 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 supervision par les autorités publiques, et ii) une 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. Étant donné la grande circulation des produits et des services à travers les frontières, ces deux problèmes peuvent être résolus au mieux par une législation européenne d'harmonisation.

En effet, la proposition définit des exigences communes obligatoires applicables à la conception et au développement de certains systèmes d'IA avant leur mise sur le marché, qui seront concrétisées par des normes techniques harmonisées. La proposition aborde également 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 relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, notamment des restrictions à 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, dans la mesure où ces règles spécifiques sont concernées, sur l'article 16 du TFUE.

2.2. Subsidiarité (pour les compétences non exclusives)

La nature de l'IA, qui repose souvent sur des ensembles de données vastes et variés et qui peut être intégrée dans tout produit ou service circulant librement dans le marché intérieur, implique que les objectifs de la présente proposition ne peuvent être atteints efficacement par les États membres seuls. En outre, l'émergence d'un patchwork de règles nationales potentiellement divergentes entravera la circulation fluide des produits et services liés aux systèmes d'IA dans l'UE et sera 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 pour résoudre ces problèmes ne feront que créer une incertitude juridique et des obstacles supplémentaires, et ralentiront l'adoption de l'IA par le marché.

Les objectifs de cette proposition peuvent être mieux réalisés au niveau de l'Union afin d'éviter une nouvelle fragmentation du marché unique en cadres nationaux potentiellement contradictoires empêchant 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 en matière d'IA. Seule une action commune au niveau de l'Union peut également protéger la souveraineté numérique de l'Union et tirer parti

de ses outils et de ses pouvoirs réglementaires pour façonner les règles et les normes mondiales.

2.3. Proportionnalité

La proposition s'appuie sur les cadres juridiques existants et est proportionnée et nécessaire pour atteindre ses objectifs, puisqu'elle suit une approche fondée sur le risque 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 autres systèmes d'IA, qui ne présentent pas de risque élevé, seules des obligations de transparence très limitées sont imposées, par exemple en termes de fourniture d'informations pour signaler l'utilisation d'un système d'IA lors d'une interaction avec des humains. Pour les systèmes d'IA à haut risque, les exigences en matière de données de haute qualité, de documentation et de traçabilité, de transparence, de surveillance humaine, d'exactitude et de robustesse, sont strictement nécessaires pour atténuer les risques pour les droits fondamentaux et la sécurité posés par l'IA et qui ne sont pas couverts par d'autres cadres juridiques existants. Des normes harmonisées, ainsi que des orientations et des outils de mise en conformité à l'appui, aideront les fournisseurs et les utilisateurs à se conformer aux exigences fixées par la proposition et à minimiser leurs coûts. Les coûts supportés par les opérateurs sont proportionnels aux objectifs atteints et aux avantages économiques et de réputation que les opérateurs peuvent attendre de cette proposition.

2.4. Choix de l'instrument

Le choix d'un règlement comme instrument juridique se justifie par la nécessité d'une application uniforme des nouvelles règles, telles que la définition de l'IA, l'interdiction de certaines pratiques nuisibles liées à l'IA et la classification de certains systèmes d'IA. L'applicabilité directe d'un règlement, conformément à l'article 288 du TFUE, réduira la fragmentation juridique et facilitera le développement d'un marché unique pour les systèmes d'IA légaux, sûrs et dignes de confiance. Il y parviendra notamment en introduisant un ensemble harmonisé d'exigences fondamentales en ce qui concerne les systèmes d'IA classés à haut risque et des obligations pour les fournisseurs et les utilisateurs de ces systèmes, améliorant ainsi la protection des droits fondamentaux et apportant une sécurité juridique aux opérateurs comme aux consommateurs.

Dans le même temps, les dispositions du règlement ne sont pas trop prescriptives et laissent la place à différents niveaux d'action des États membres pour les éléments qui ne compromettent pas les objectifs de l'initiative, notamment l'organisation interne du système de surveillance du marché et l'adoption de mesures visant à encourager l'innovation.

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

3.1. Consultation des parties prenantes

Cette proposition est le résultat d'une consultation approfondie avec toutes les principales parties prenantes, dans laquelle les principes généraux et les normes minimales de consultation des parties intéressées par la Commission ont été appliqués.

Une **consultation publique en ligne** a été lancée le 19 février 2020 en même temps que la publication du Livre blanc sur l'intelligence artificielle et a duré jusqu'au 14 juin 2020. L'objectif de cette consultation était de recueillir des avis et des opinions sur le livre blanc. Elle visait toutes les parties prenantes intéressées des secteurs public et 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 et les réponses individuelles sur son site web22.

Au total, 1 215 contributions ont été reçues, dont 352 provenaient d'entreprises ou d'organisations/associations commerciales, 406 de particuliers (92 % de particuliers de l'UE), 152 au nom d'organisations de la société civile et de la société civile.

[22] Voirtous lesrésultats de laconsultationici.

des institutions universitaires/de recherche, et 73 des autorités publiques. Les voix de la société civile étaient représentées par 160 répondants (dont 9 organisations de consommateurs, 129 organisations non gouvernementales et 22 syndicats), 72 répondants ayant contribué en tant que "autres". Sur les 352 représentants du monde des affaires et de l'industrie, 222 étaient des entreprises et des représentants d'entreprises, dont 41,5% de micro, petites et moyennes entreprises. Les autres étaient des associations d'entreprises. Dans l'ensemble, 84% des réponses des entreprises et de l'industrie provenaient de l'Union européenne.
27. Selon la question, entre 81 et 598 des répondants ont utilisé l'option de texte libre pour insérer des commentaires. Plus de 450 prises de position ont été soumises via le site web de l'enquête de l'UE, soit en complément des réponses au questionnaire (plus de 400), soit en tant que contributions indépendantes (plus de 50).

Dans l'ensemble, les parties prenantes s'accordent sur la nécessité d'agir. Une grande majorité d'entre elles conviennent qu'il existe des lacunes législatives ou qu'une nouvelle législation est nécessaire. Toutefois, plusieurs parties prenantes mettent en garde la Commission contre les doubles emplois, les obligations contradictoires et la surréglementation. De nombreux commentaires soulignent l'importance d'un cadre réglementaire neutre sur le plan technologique et proportionné.

Les parties prenantes ont principalement demandé une définition étroite, claire et précise de l'IA. Les parties prenantes ont également souligné qu'outre la clarification du terme IA, il est important de définir les termes "risque", "risque élevé", "risque faible", "identification biométrique à distance" et "préjudice".

La plupart des répondants sont explicitement en faveur de l'approche fondée sur le risque. L'utilisation d'un cadre fondé sur les risques est considérée comme une meilleure option qu'une réglementation générale de tous les systèmes d'IA. Les types de risques et de menaces devraient être basés sur une approche secteur par secteur et au cas par cas. Les risques devraient également être calculés en tenant compte de l'impact sur les droits et la sécurité.

Les bacs à sable réglementaires pourraient être très utiles pour la promotion de l'IA et sont bien accueillis par certaines parties prenantes, notamment les associations d'entreprises.

Parmi les personnes qui se sont prononcées sur les modèles d'application, plus de 50 %, en particulier les associations d'entreprises, étaient favorables à la combinaison d'une auto-évaluation des risques ex ante et d'une application ex post pour les systèmes d'IA à haut risque.

3.2. Collecte et utilisation de l'expertise

La proposition s'appuie sur deux années d'analyse et d'implication étroite des parties prenantes, notamment 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 d'un **groupe d'experts de haut niveau sur l'IA (HLEG)** qui avait une composition inclusive et large de 52 experts de renom chargés de conseiller la Commission sur la mise en œuvre de la stratégie de la Commission sur l'intelligence artificielle. En avril 2019, la Commission a soutenu23 les exigences clés énoncées dans les lignes directrices éthiques du HLEG pour une IA digne de confiance24, qui avaient été révisées pour tenir compte de plus de 500 soumissions de parties prenantes. Les exigences clés reflètent une approche répandue et commune, comme en témoigne une pléthore de codes et de principes éthiques élaborés par de nombreuses organisations privées et publiques en Europe et au-delà, selon laquelle le développement et l'utilisation de l'IA devraient être guidés par certains principes essentiels axés sur les valeurs. L'Assessment List for Trustworthy Artificial Intelligence (ALTAI)[25] a rendu ces exigences opérationnelles dans le cadre d'un processus de pilotage avec plus de 350 organisations.

23Commission européenne, *Établir laconfiancedans l'intelligenceartificiellecentrée sur l'humain*, COM(2019) 168.

24HLEG, *Lignes directrices éthiques pour uneIAdigne de confiance*, 2019.

25HLEG, *Liste d'évaluationpour uneintelligenceartificielle digne de confiance(ALTAI)pour l'auto-évaluation*, 2020.

En outre, l'**AI Alliance26** a été créée en tant que plateforme permettant à quelque 4 000 parties prenantes de débattre des implications technologiques et sociétales de l'IA, avec pour point d'orgue une assemblée annuelle de l'IA.

Le **livre blanc** sur l'IA a approfondi cette approche inclusive, suscitant les commentaires de plus de 1 250 parties prenantes, dont plus de 450 prises de position supplémentaires. En conséquence, la Commission a publié une analyse d'impact initiale, qui a elle-même suscité plus de 130 commentaires27. Des **ateliers et des manifestations supplémentaires** ont également été organisés à l'intention **des parties prenantes**, dont les résultats étayent l'analyse de l'analyse d'impact et les choix politiques opérés dans la présente proposition28. Une **étude externe** a également été commandée pour alimenter l'analyse d'impact.

3.3. Analyse d'impact

Conformément à sa politique "Mieux légiférer", la Commission a réalisé une analyse d'impact pour cette proposition examinée par le Regulatory Scrutiny Board de la Commission. Une réunion avec le Regulatory Scrutiny Board a eu lieu le 16 décembre 2020, qui a été suivie d'un avis négatif. Après une révision substantielle de l'analyse d'impact pour tenir compte des commentaires et une nouvelle présentation de l'analyse d'impact, le Regulatory Scrutiny Board a émis un avis positif le 21 mars 2021. Les avis du Regulatory Scrutiny Board, les recommandations et une explication de la manière dont ils ont été pris en compte sont présentés à l'annexe 1 de l'analyse d'impact.

La Commission a examiné différentes options stratégiques pour atteindre l'objectif général de la proposition, qui est d'**assurer le bon fonctionnement du marché unique** en créant les conditions nécessaires au développement et à l'utilisation d'une IA digne de confiance dans l'Union.

Quatre options politiques comportant différents degrés d'intervention réglementaire ont été évaluées :

- **Option 1** : instrument législatif européen établissant un système d'étiquetage volontaire ;
- **Option 2** : une approche sectorielle, "ad hoc" ;
- **Option 3** : Instrument législatif horizontal de l'UE suivant une approche proportionnelle fondée sur le risque ;
- **Option 3+** : instrument législatif horizontal de l'UE suivant une approche proportionnelle fondée sur le risque + codes de conduite pour les systèmes d'IA ne présentant pas de risque élevé ;
- **Option 4** : Instrument législatif horizontal de l'UE établissant des exigences obligatoires pour tous les systèmes d'IA, quel que soit le risque qu'ils présentent.

Conformément à la méthodologie établie par la Commission, chaque option politique a été évaluée en fonction de ses incidences économiques et sociétales, avec un accent particulier sur les incidences sur les droits fondamentaux. L'option privilégiée est l'option 3+, un cadre réglementaire pour les systèmes d'IA à haut risque uniquement, avec la possibilité pour tous les fournisseurs de systèmes d'IA sans 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, la surveillance humaine, la robustesse et la précision, et seront obligatoires pour les systèmes d'IA à haut risque. Les entreprises qui introduiraient des codes de conduite pour d'autres systèmes d'IA le feraient sur une base volontaire.

[26] L'AllianceAI Alliance est un forum multi-acteurs lancé en juin 2018 , AIAlliance https://ec.europa.eu/digital-single-market/en/european-ai-alliance

[27] Commission européenne , *Inception Impact Assessment ForaProposal forlegal act of theEuropean Parliamentand the Councillaying down requirementsforArtificialIntelligence.*

[28] Pour le détail de toutes les consultations qui ont été menées, voir l'annexe 2 de l'analyse d'impact.

L'option privilégiée a été jugée apte à répondre de la manière la plus efficace aux objectifs de la présente proposition. En exigeant un ensemble restreint mais efficace de mesures de la part des développeurs et des utilisateurs d'IA, l'option privilégiée limite les risques de violation des droits fondamentaux et de la sécurité des personnes et favorise une supervision et une mise en œuvre efficaces, en ciblant les exigences uniquement sur les systèmes pour lesquels il existe un risque élevé que de telles violations se produisent. Par conséquent, cette option permet de maintenir les coûts de mise en conformité à un niveau minimum, évitant ainsi un ralentissement inutile de l'adoption en raison de prix et de coûts de mise en conformité plus élevés. Afin de remédier aux inconvénients éventuels pour les PME, cette option comprend plusieurs dispositions visant à favoriser leur mise en conformité et à réduire leurs coûts, 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 gens dans l'IA, les entreprises gagneront en sécurité juridique et les États membres ne verront aucune raison de prendre des mesures unilatérales qui pourraient fragmenter le marché unique. En raison d'une demande accrue due à une plus grande confiance, d'un plus grand nombre d'offres disponibles grâce à la sécurité juridique et de l'absence d'obstacles à la circulation transfrontalière des systèmes d'IA, le marché unique de l'IA devrait prospérer. L'Union européenne continuera à développer un écosystème d'IA à croissance rapide composé de services et de produits innovants intégrant la technologie de l'IA ou de systèmes d'IA autonomes, ce qui se traduira par une autonomie numérique accrue.

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 citoyens devraient se conformer à des exigences et obligations spécifiques. Le respect de ces exigences impliquerait des coûts s'élevant à environ 6000 à 7000 euros pour la fourniture d'un système d'IA moyen à haut risque, soit environ 170000 euros d'ici 2025. Pour les utilisateurs de l'IA, il y aurait également le coût annuel du temps passé à assurer une surveillance humaine lorsque cela est approprié, selon le cas d'utilisation. Ces coûts ont été estimés à environ 5000 à 5000 euros.
8000 € par an. Les coûts de vérification pourraient s'élever à 3 000 à 7 500 euros supplémentaires pour les fournisseurs d'IA à haut risque. Les entreprises ou les autorités publiques qui développent ou utilisent des applications d'IA non classées à haut risque n'auraient que des obligations minimales d'information. Toutefois, elles pourraient choisir de se joindre à d'autres et d'adopter ensemble un code de conduite afin de respecter des exigences appropriées et de garantir que leurs systèmes d'IA sont dignes de confiance. Dans ce cas, les coûts 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 les différentes catégories de parties prenantes (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 accompagnant la présente proposition.

3.4. Adaptation et simplification de la réglementation

La présente proposition établit les obligations qui s'appliqueront aux fournisseurs et aux utilisateurs de systèmes d'IA à haut risque. Pour les fournisseurs qui développent et mettent de tels systèmes sur le marché de l'Union, elle créera une sécurité juridique et garantira qu'aucun obstacle à la fourniture transfrontalière de services et de produits liés à l'IA n'apparaisse. Pour les entreprises utilisant l'IA, elle favorisera la confiance de leurs clients. Pour les administrations publiques nationales, il favorisera la confiance du public dans l'utilisation de l'IA et renforcera les mécanismes d'application (en introduisant un mécanisme de coordination européen, en prévoyant des capacités appropriées et en facilitant les audits 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, notamment des bacs à

sable réglementaires et des mesures spécifiques d'aide aux petits utilisateurs et fournisseurs de systèmes d'IA à haut risque pour se conformer aux nouvelles règles.

La proposition vise aussi spécifiquement à renforcer la compétitivité et la base industrielle de l'Europe en matière d'IA. Une cohérence totale est assurée avec la législation sectorielle existante de l'Union applicable à

des systèmes d'IA (par exemple sur les produits et services) qui apporteront davantage de clarté et simplifieront l'application des nouvelles règles.

3.5. Droits fondamentaux

L'utilisation de l'IA avec ses caractéristiques spécifiques (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 inscrits dans la Charte des droits fondamentaux de l'Union européenne (ci-après "la Charte"). La présente proposition vise à assurer un niveau élevé de protection de ces droits fondamentaux et à traiter diverses sources de risques par une approche fondée sur les risques clairement définie. Avec 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 1), 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 tout effet paralysant sur les droits à la liberté d'expression (article 11) et à la liberté de réunion (article 12), à assurer la protection du droit à un recours effectif et à un procès équitable, des droits de la défense et de la présomption d'innocence (articles 47 et 48), ainsi que du principe général de bonne administration. En outre, dans la mesure où elle est applicable dans certains domaines, la proposition aura une incidence positive sur les droits d'un certain nombre de groupes particuliers, tels que le droit des travailleurs à des conditions de travail justes et équitables (article 31), un niveau élevé de protection des consommateurs (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 à l'amélioration de la qualité de l'environnement (article 37) est également pertinent, notamment en ce qui concerne la santé et la sécurité des personnes. Les obligations en matière de tests ex ante, de gestion des risques et de surveillance humaine 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 critiques tels que l'éducation et la formation, l'emploi, les services importants, l'application de la loi et le système judiciaire. Si des violations des droits fondamentaux se produisent malgré tout, les personnes concernées pourront obtenir réparation en garantissant la transparence et la traçabilité des systèmes d'IA, ainsi que des contrôles ex post rigoureux.

Cette proposition impose certaines restrictions à la liberté d'entreprise (article 16) et à la liberté de l'art et de la science (article 13) afin de garantir le respect de raisons impérieuses d'intérêt public telles que la santé, la sécurité, la protection des consommateurs et la protection d'autres droits fondamentaux ("innovation responsable") lors du développement et de l'utilisation de technologies d'IA à haut risque. Ces restrictions sont proportionnées et limitées au minimum nécessaire pour prévenir et atténuer les risques graves pour la sécurité et les atteintes probables aux droits fondamentaux.

Les obligations de transparence accrues 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 uniquement aux informations minimales nécessaires aux particuliers pour exercer leur droit à un recours effectif et à la transparence nécessaire à l'égard des autorités de surveillance et d'exécution, conformément à leurs mandats. Toute divulgation d'informations sera effectuée dans le respect de la législation pertinente en la matière, y compris la directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre leur acquisition, leur utilisation et leur divulgation illicites. Lorsque les autorités publiques et les organismes notifiés doivent avoir accès à des informations confidentielles ou à un code source pour examiner le respect d'obligations substantielles, ils sont soumis à des obligations de confidentialité contraignantes.

4. IMPLICATIONS BUDGÉTAIRES

Les États membres devront désigner des autorités de surveillance chargées de mettre en œuvre les exigences législatives. Leur fonction de surveillance pourrait s'appuyer sur les dispositions existantes, à savoir

par exemple en ce qui concerne les organismes d'évaluation de la conformité ou la surveillance du marché, mais elle nécessiterait 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.

Un aperçu détaillé des coûts impliqués est fourni dans la "fiche financière" liée à cette proposition.

5. AUTRES ÉLÉMENTS

5.1. Plans de mise en œuvre et dispositions en matière de suivi, d'évaluation et de rapports

Il est essentiel de prévoir un mécanisme de suivi et d'évaluation solide pour garantir que la proposition sera efficace pour atteindre ses objectifs spécifiques. La Commission sera chargée de surveiller les effets de la proposition. Elle établira un système d'enregistrement des demandes autonomes d'IA 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 aux autres personnes intéressées de vérifier si le système d'IA à haut risque est conforme aux exigences énoncées dans la proposition et d'exercer une surveillance renforcée 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 significatives sur leurs systèmes et l'évaluation de la conformité effectuée sur ces systèmes.

En outre, les fournisseurs d'IA seront tenus d'informer les autorités nationales compétentes des incidents graves ou des dysfonctionnements qui constituent une violation des obligations en matière de droits fondamentaux dès qu'ils en ont connaissance, ainsi que de tout rappel ou retrait de systèmes d'IA du marché. Les autorités nationales compétentes enquêteront alors sur les incidents ou les dysfonctionnements, collecteront toutes les informations nécessaires et les transmettront régulièrement à la Commission avec les métadonnées adéquates. La Commission complétera ces informations sur les incidents par une analyse complète du marché global de l'IA.

La Commission publiera un rapport d'évaluation et de révision du cadre proposé pour l'IA cinq ans après la date à laquelle il sera applicable.

5.2. Explication détaillée des dispositions spécifiques 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'instrument. La définition du système d'IA dans le cadre juridique vise à être aussi neutre que possible sur le plan technologique et à l'épreuve du temps, compte tenu de l'évolution rapide de la technologie et du marché en matière d'IA. Afin de fournir la sécurité juridique nécessaire, le titre I est complété par l'annexe I, qui contient une liste détaillée d'approches et de techniques pour le développement de l'IA, à adapter par la Commission en fonction des nouveaux développements technologiques. Les principaux participants à la chaîne de valeur de l'IA sont également clairement définis, comme les fournisseurs et les utilisateurs de systèmes d'IA, qui couvrent à la fois les opérateurs publics et privés afin de garantir des conditions de concurrence équitables.

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

Le **titre II** établit une liste des IA interdites. Le règlement suit une approche fondée sur le risque, en établissant 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 du titre II comprend tous les systèmes d'IA dont l'utilisation est jugée inacceptable car contraire aux valeurs de l'Union, par exemple en violant les droits fondamentaux. Les interdictions couvrent les pratiques qui ont un potentiel significatif de manipulation des personnes par des techniques subliminales au-delà de leur conscience ou qui exploitent

vulnérabilités de groupes vulnérables spécifiques tels que les enfants ou les personnes handicapées afin de déformer matériellement leur comportement d'une manière susceptible de leur causer ou de causer à une autre personne un préjudice psychologique ou physique. D'autres pratiques de manipulation ou d'exploitation touchant les adultes qui pourraient être facilitées par les systèmes d'IA pourraient être couvertes par la législation existante en matière de protection des données, de protection des consommateurs et de services numériques, qui garantit que les personnes physiques sont correctement informées et ont le libre choix de ne pas être soumises au profilage ou à d'autres pratiques susceptibles d'affecter leur comportement. La proposition interdit également le scoring social basé sur l'IA à des fins générales par les autorités publiques. Enfin, l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans les espaces accessibles au public à des fins répressives est également interdite, sauf exceptions limitées.

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

Le **titre III** contient des règles spécifiques pour les systèmes d'IA qui créent un risque élevé pour la santé et la sécurité ou les droits fondamentaux des personnes physiques. Conformément à une approche fondée sur le risque, 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 de conformité ex ante. La classification d'un système d'IA comme étant à haut risque est basée sur la finalité du système d'IA, conformément à la législation existante sur la sécurité des produits. Par conséquent, la classification en tant que système à haut risque ne dépend pas seulement de la fonction remplie par le système d'IA, mais aussi de l'objectif et des modalités spécifiques pour lesquels ce système est utilisé.

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

- Systèmes d'IA destinés à être utilisés comme composants de sécurité de produits soumis à une évaluation de conformité ex ante par un tiers ;
- d'autres systèmes d'IA autonomes ayant principalement des implications en matière de droits fondamentaux, qui sont explicitement énumérés à l'annexe III.

Cette liste de systèmes d'IA à haut risque figurant à l'annexe III contient un nombre limité de systèmes d'IA dont les risques se sont déjà matérialisés ou sont susceptibles de se matérialiser dans un avenir proche. Afin de garantir que le règlement puisse être adapté aux utilisations et applications émergentes de l'IA, la Commission peut étendre la liste des systèmes d'IA à haut risque utilisés dans certains domaines prédéfinis, en appliquant une série de critères et une méthodologie 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 d'enregistrements, la transparence et la fourniture d'informations aux utilisateurs, la surveillance humaine, la robustesse, l'exactitude et la sécurité. Les exigences minimales proposées constituent déjà un état de l'art pour de nombreux opérateurs diligents et sont le résultat de deux années de travaux préparatoires, dérivés des lignes directrices éthiques du HLEG29, pilotées par plus de 350 organisations30. Elles sont également largement conformes à d'autres recommandations et principes internationaux, ce qui garantit que le cadre proposé pour l'IA est compatible avec ceux adoptés par les partenaires commerciaux internationaux de l'UE. Les solutions techniques précises permettant de se conformer à ces exigences peuvent être fournies par des normes ou par d'autres spécifications techniques, ou encore être développées conformément aux connaissances techniques ou scientifiques générales, à la discrétion du fournisseur du système d'IA. Cette flexibilité est particulièrement importante, car elle permet aux fournisseurs de systèmes d'IA de choisir le type de système d'IA qu'ils souhaitent utiliser.

29Groupe d'experts de haut niveau sur l'intelligence artificielle, *Lignes directriceséthiquespour uneIAdigne de confiance*, 2019.

30Elles ont également été approuvées par la Commission dans sa communication de 2019 sur l'approche centrée sur l'humain de l'IA.

de manière à répondre à leurs exigences, en tenant compte de l'état de l'art 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 de la chaîne de valeur de l'IA (par exemple, les importateurs, les distributeurs, les représentants autorisés).

Le chapitre 4 définit le cadre dans lequel les organismes notifiés doivent être impliqués en tant que tierces parties indépendantes dans les procédures d'évaluation de la conformité, tandis que le chapitre 5 explique en détail les procédures d'évaluation de la conformité à suivre pour chaque type de système d'IA à haut risque. L'approche de l'évaluation de la conformité vise à minimiser la charge pour les opérateurs économiques ainsi que pour les organismes notifiés, dont la capacité doit être progressivement renforcée au fil du temps. Les systèmes d'IA destinés à être utilisés comme composants de sécurité de produits réglementés par la législation relative au nouveau cadre législatif (par exemple, machines, jouets, dispositifs médicaux, etc.) seront soumis aux mêmes mécanismes de conformité et d'application ex ante et ex post que les produits dont ils sont un composant.) seront soumis aux mêmes mécanismes de conformité et d'application ex ante et ex post que les produits dont ils sont des composants. La principale différence est que les mécanismes ex ante et ex post garantiront la conformité non seulement aux exigences établies par la législation sectorielle, mais aussi aux exigences établies par ce règlement.

En ce qui concerne les systèmes autonomes d'IA à haut risque visés à l'annexe III, un nouveau système de conformité et d'application sera mis en place. Celui-ci suit le modèle de la législation relative au nouveau cadre législatif, mis en œuvre par le biais de contrôles internes effectués par les fournisseurs, à l'exception des systèmes d'identification biométrique à distance qui seraient soumis à une évaluation de conformité par un tiers. Une évaluation de conformité ex ante complète par le biais de contrôles internes, combinée à une application ex post rigoureuse, pourrait constituer une solution efficace et raisonnable pour ces systèmes, étant donné la phase initiale de l'intervention réglementaire et le fait que le secteur de l'IA est très innovant et que l'expertise en matière d'audit ne fait que commencer à s'accumuler. Une évaluation par le biais de contrôles internes pour les systèmes d'IA "autonomes" à haut risque nécessiterait une conformité ex ante complète, efficace et correctement documentée avec toutes les exigences du règlement, ainsi que le respect de systèmes robustes de gestion de la qualité et des risques et une surveillance après la mise sur le marché. Après avoir effectué l'évaluation de conformité pertinente, le fournisseur devrait enregistrer ces systèmes d'IA autonomes à haut risque dans une base de données européenne qui sera gérée par la Commission afin d'accroître la transparence et la surveillance publiques et de renforcer la supervision ex post par les autorités compétentes. En revanche, pour des raisons de cohérence avec la législation existante sur la sécurité des produits, les évaluations de la conformité des systèmes d'IA qui sont des composants de sécurité des produits suivront un système avec des procédures d'évaluation de la conformité par des tiers déjà établies dans le cadre de la législation sectorielle pertinente sur la sécurité des produits. De nouvelles réévaluations ex ante de la conformité seront nécessaires en cas de modifications substantielles des systèmes d'IA (et notamment de changements allant au-delà de ce qui est prédéterminé par le fournisseur dans sa documentation technique et vérifié au moment de l'évaluation ex ante de la conformité).

5.2.4. OBLIGATIONS DE TRANSPARENCE POUR CERTAINS SYSTÈMES AI (TITRE IV)

Le **titre IV** concerne certains systèmes d'IA pour tenir compte des risques spécifiques de manipulation qu'ils présentent. Des obligations de transparence s'appliqueront aux systèmes qui (i) interagissent avec des personnes, (ii) sont utilisés pour détecter des émotions ou déterminer l'association à des catégories (sociales) sur la base de données biométriques, ou (iii) génèrent ou manipulent des contenus ("deep fakes"). Lorsque des personnes interagissent avec un

système d'IA ou que leurs émotions ou caractéristiques sont reconnues par des moyens automatisés, les personnes doivent être informées de cette circonstance. Si un système d'IA est utilisé pour générer ou manipuler un contenu image, audio ou vidéo qui ressemble sensiblement à un contenu authentique, il devrait y avoir une obligation de divulguer que le contenu est généré par des moyens automatisés, sous réserve de

des exceptions à des fins légitimes (application de la loi, liberté d'expression). Cela permet aux personnes de faire des choix éclairés ou de prendre du recul par rapport à une situation donnée.

5.2.5. MESURES EN FAVEUR DE L'INNOVATION (TITRE V)

Le **titre V** contribue à l'objectif de créer un cadre juridique favorable à l'innovation, à l'épreuve du temps et résistant aux perturbations. À cette fin, il encourage les autorités nationales compétentes à mettre en place des bacs à sable réglementaires et fixe un cadre de base en termes de gouvernance, de supervision et de responsabilité. Les bacs à sable réglementaires de l'IA établissent un environnement contrôlé pour tester des technologies innovantes pendant 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 jeunes entreprises.

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

Le **titre VI** établit les systèmes de gouvernance au niveau de l'Union et au niveau national. Au niveau de l'Union, la proposition établit un Conseil européen de l'intelligence artificielle (le "Conseil"), composé de représentants des États membres et de la Commission. Le conseil facilitera une mise en œuvre harmonieuse, efficace et harmonisée de ce règlement en contribuant à la coopération effective des autorités nationales de surveillance et de la Commission et en fournissant des conseils et une expertise à la Commission. Il recueillera et partagera également les meilleures pratiques entre 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, afin de superviser l'application et la mise en œuvre du règlement. Le contrôleur européen de la protection des données agira en tant qu'autorité compétente pour le contrôle des institutions, agences et organes de l'Union lorsqu'ils entrent dans le champ d'application du présent règlement.

Le **titre VII** vise à faciliter le travail de surveillance 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 ayant principalement des implications sur les droits fondamentaux. Cette base de données sera gérée par la Commission et alimentée en données 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.

Le **titre VIII définit** les obligations de contrôle et de notification des fournisseurs de systèmes d'IA en ce qui concerne le contrôle et la notification après la mise sur le marché et les enquêtes sur les incidents et les dysfonctionnements liés à l'IA. Les autorités de surveillance du marché contrôleraient également le marché et enquêteraient 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 auront tous les pouvoirs prévus par le règlement (UE) 2019/1020 sur la surveillance du marché. L'application ex post devrait garantir qu'une fois le système d'IA mis sur le marché, les autorités publiques disposent des pouvoirs et des ressources nécessaires pour intervenir au cas où les systèmes d'IA génèrent des risques inattendus, qui justifient une action rapide. Elles contrôleront également le respect par les opérateurs des obligations qui leur incombent en vertu du règlement. La proposition ne prévoit pas la création automatique d'organismes ou d'autorités supplémentaires au niveau des États membres. Les États membres peuvent donc désigner (et s'appuyer sur l'expertise) des autorités sectorielles existantes, qui seraient également chargées de contrôler et de faire appliquer les dispositions du règlement.

Tout ceci est sans préjudice du système existant et de la répartition des pouvoirs d'exécution ex post des obligations relatives aux droits fondamentaux dans les États membres. Lorsque leur mandat l'exige, les autorités de surveillance et d'exécution existantes auront également le

pouvoir de demander et d'accéder à toute documentation conservée conformément au présent règlement et, le cas échéant, de demander aux autorités de surveillance du marché d'organiser des tests du système d'IA à haut risque par des moyens techniques.

5.2.7. CODES DE CONDUITE (TITRE IX)

Le **titre IX** crée un cadre pour la création de codes de conduite, qui visent à encourager les fournisseurs de systèmes d'IA à faible risque à appliquer volontairement les exigences obligatoires pour les systèmes d'IA à risque élevé (telles que définies au titre III). Les fournisseurs de systèmes d'IA à risque non élevé peuvent créer et mettre en œuvre eux-mêmes les codes de conduite. Ces codes peuvent également inclure des engagements volontaires concernant, par exemple, la durabilité environnementale, l'accessibilité pour les personnes handicapées, la participation des parties prenantes à la conception et au développement des systèmes d'IA et la diversité des équipes de développement.

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

Le **titre X** souligne l'obligation de toutes les parties de respecter la confidentialité des informations et des données et définit des règles pour l'échange des informations obtenues lors de la mise en œuvre du règlement. Le titre X comprend également des mesures visant à assurer la mise en œuvre effective du règlement par des sanctions efficaces, proportionnées et dissuasives en cas de violation des dispositions.

Le **titre XI définit** les règles relatives à l'exercice des pouvoirs de délégation et 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 prévoit l'**obligation pour la Commission d'évaluer régulièrement la nécessité d'une mise à jour de l'annexe III et d'élaborer des rapports réguliers sur l'évaluation et le réexamen du règlement. Il prévoit également des dispositions finales, notamment une période transitoire différenciée pour la date initiale d'applicabilité du règlement, afin de faciliter la mise en œuvre harmonieuse pour toutes les parties concernées.

2021/0106 (COD)

Proposition de

RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

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

Vu l'avis du Comité économique et social européen31, Vu l'avis du Comité des

régions32,

Agissant 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, notamment pour le développement, la commercialisation et l'utilisation de l'intelligence artificielle, conformément aux valeurs de l'Union. Le présent règlement poursuit un certain nombre de raisons impérieuses d'intérêt général, telles qu'un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux, et il garantit la libre circulation transfrontalière des biens et services fondés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation des systèmes d'IA, sauf autorisation explicite du présent règlement.

(2) Les systèmes d'intelligence artificielle (systèmes IA) peuvent être facilement déployés dans de multiples secteurs de l'économie et de la société, y compris de manière transfrontalière, et circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales pour garantir que l'intelligence artificielle est sûre et qu'elle est développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Des règles nationales différentes peuvent entraîner une fragmentation du marché intérieur et diminuer la sécurité juridique pour les opérateurs qui développent ou utilisent des systèmes d'IA. Il convient donc d'assurer un niveau de protection élevé et cohérent dans l'ensemble de l'Union et de prévenir les divergences qui entravent la libre circulation des systèmes d'IA et des produits et services connexes dans le marché intérieur, en établissant des obligations uniformes pour les opérateurs et en garantissant la protection uniforme des raisons impérieuses d'intérêt public et des droits des personnes dans l'ensemble du marché intérieur sur la base de l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE). Dans la mesure où le présent règlement contient des règles spécifiques relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel concernant les personnes suivantes

[31] OJ C [...], [...], p. [...].
[32] OJ C [...], [...], p. [...].

des restrictions à 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, dans la mesure où ces règles spécifiques sont concernées, sur l'article 16 du TFUE. À la lumière de ces règles spécifiques et du recours à l'article 16 du TFUE, il convient de consulter le Conseil européen de la protection des données.

(3) L'intelligence artificielle est une famille de technologies qui évolue rapidement et qui peut contribuer à un large éventail d'avantages économiques et sociétaux dans tout le spectre des industries et des activités sociales. En améliorant les prévisions, en optimisant les opérations et l'allocation des ressources, et en personnalisant les solutions numériques disponibles pour les individus et les organisations, l'utilisation de l'intelligence artificielle peut fournir des avantages concurrentiels clés aux entreprises et soutenir des résultats bénéfiques sur le plan social et environnemental, par exemple dans les domaines des soins de santé, de l'agriculture, de l'éducation et de la formation, de la gestion des infrastructures, de l'énergie, du transport et de la logistique, des services publics, de la sécurité, de la justice, de l'efficacité des ressources et de l'énergie, et de l'atténuation et de l'adaptation au changement climatique.

(4) En même temps, selon les circonstances relatives à son application et à son utilisation spécifiques, l'intelligence artificielle peut générer des risques et porter atteinte aux intérêts publics et aux droits protégés par le droit de l'Union. Ces atteintes peuvent être matérielles ou immatérielles.

(5) Un cadre juridique de l'Union fixant des règles harmonisées en matière d'intelligence artificielle est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'intelligence artificielle dans le marché intérieur, tout en répondant à un niveau élevé de protection des intérêts publics, tels que la santé et la sécurité et la protection des droits fondamentaux, tels que reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, il convient d'établir des règles régissant la mise sur le marché et la mise en service de certains systèmes d'IA, assurant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des biens et des services. En établissant ces règles, le présent règlement soutient l'objectif de l'Union d'être un leader mondial dans le développement d'une intelligence artificielle sûre, digne de confiance et éthique, comme l'a déclaré le Conseil européen33, et il assure la protection des principes éthiques, comme l'a spécifiquement demandé le Parlement européen34.

(6) La notion de système d'IA doit être clairement définie pour garantir la sécurité juridique, tout en offrant la souplesse nécessaire pour s'adapter aux évolutions technologiques futures. La définition devrait se fonder sur les principales caractéristiques fonctionnelles du logiciel, en particulier la capacité, pour un ensemble donné d'objectifs définis par l'homme, de 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 avec différents niveaux d'autonomie et être utilisés de manière autonome ou en tant que composant d'un produit, que le système soit physiquement intégré au produit (embarqué) ou qu'il serve la fonctionnalité du produit sans y être intégré (non embarqué). La définition du système d'IA doit être complétée par une liste de techniques et d'approches spécifiques utilisées pour son développement, qui doit être mise à jour en fonction de l'évolution du marché et des technologies.

33Conseil européen, Réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) - Conclusions,

EUCO 13/20, 2020, p. 6.
34Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission sur un cadre des aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, 2020/2012(INL).

par l'adoption d'actes délégués par la Commission pour modifier cette liste.

(7) La notion de données biométriques utilisée dans le présent règlement est conforme à la notion de données biométriques définie à l'article 4, paragraphe 14, du règlement (UE) 2016/679 du Parlement européen et du Conseil35, à l'article 3, paragraphe 18, du règlement (UE) 2018/1725 du Parlement européen et du Conseil36 et à l'article 3, paragraphe 13, de la directive (UE) 2016/680 du Parlement européen et du Conseil37, et devrait être interprétée de manière cohérente avec cette notion.

(8) La notion de système d'identification biométrique à distance telle qu'utilisée dans le présent règlement devrait être définie de manière fonctionnelle, comme un système d'IA destiné à l'identification de 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, et sans savoir au préalable si la personne visée sera présente et pourra être identifiée, indépendamment de la technologie, des procédés ou des types de données biométriques particuliers utilisés. Compte tenu de leurs différentes caractéristiques et de leurs modes d'utilisation, ainsi que des différents risques qu'ils comportent, il convient d'établir 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 saisie des données biométriques, la comparaison et l'identification se font instantanément, quasi instantanément ou, en tout état de cause, sans délai important. À cet égard, il ne devrait pas être possible de contourner les règles du présent règlement relatives à l'utilisation "en temps réel" des systèmes d'IA en question en prévoyant des délais mineurs. Les systèmes "en temps réel" impliquent l'utilisation de matériel "en direct" ou "quasi en direct", tel que des séquences vidéo, générées par une caméra ou un autre dispositif doté de fonctionnalités similaires. Dans le cas des systèmes "post", en revanche, les données biométriques ont déjà été saisies et la comparaison et l'identification n'interviennent qu'après un délai important. Il s'agit d'éléments, tels que des images ou des séquences vidéo générées par des caméras de télévision en circuit fermé ou des dispositifs privés, qui ont été générés 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 doit être comprise comme désignant tout lieu physique accessible au public, que le lieu en question soit de propriété privée ou publique. Par conséquent, cette notion ne couvre pas les lieux qui sont de nature privée et qui ne sont normalement pas librement accessibles à des tiers, y compris les services répressifs, à moins que ces derniers n'aient été spécifiquement invités ou autorisés, comme les domiciles, les clubs privés, les bureaux, les entrepôts et les usines. Les espaces en ligne ne sont pas non plus couverts, car ils ne sont pas des espaces physiques. Toutefois, le simple fait que certaines conditions d'accès à un espace en ligne ne soient pas remplies n'est pas un motif de refus.

35Règlement (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).

36Règlement (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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

37Directive (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 relative à l'application des lois) (JO L 119 du 4.5.2016,

p. 89).

Le fait qu'un espace particulier puisse être soumis à des restrictions, telles que des billets d'entrée ou des restrictions d'âge, ne signifie pas que cet 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 des bâtiments publics 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. Il convient toutefois de déterminer au cas par cas si un espace donné est accessible au public, en tenant compte des spécificités de chaque situation.

(10) Afin de garantir des conditions de concurrence équitables et une protection efficace des droits et libertés des personnes dans l'ensemble de l'Union, les règles établies par le présent règlement devraient s'appliquer aux fournisseurs de systèmes d'IA de manière non discriminatoire, 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 entrer dans le champ d'application du présent règlement même lorsqu'ils ne sont ni mis sur le marché, ni mis en service, ni utilisés dans l'Union. C'est le cas par exemple d'un opérateur établi dans l'Union qui sous-traite certains services à un opérateur établi en dehors de l'Union dans le cadre d'une activité à réaliser par un système d'IA qui serait qualifié de risque élevé et dont les effets impactent des personnes physiques situées dans l'Union. Dans ces circonstances, le système d'IA utilisé par l'opérateur établi en dehors de l'Union pourrait traiter des données légalement collectées dans l'Union et transférées à partir de celle-ci, et fournir à l'opérateur contractant établi dans l'Union les résultats de ce système d'IA résultant de ce traitement, sans que ce système d'IA soit mis sur le marché, mis en service ou utilisé dans l'Union. Afin d'empêcher le contournement 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 la sortie produite par ces systèmes est utilisée dans l'Union. Néanmoins, pour tenir compte des arrangements existants 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 et aux organisations internationales lorsqu'elles agissent dans le cadre d'accords internationaux conclus au niveau national ou européen en matière de coopération policière et judiciaire avec l'Union ou avec ses États membres. Ces 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 et des pays tiers et des organisations internationales.

(12) Le présent règlement devrait également s'appliquer aux institutions, offices, organes et agences de l'Union lorsqu'ils agissent en tant que fournisseurs ou utilisateurs d'un système d'IA. Les systèmes d'IA développés ou utilisés exclusivement 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 devrait être sans préjudice des 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 loi sur les services numériques].

(13) Afin d'assurer un niveau élevé et cohérent de protection des intérêts publics en matière de santé, de sécurité et de droits fondamentaux, il convient d'établir des normes normatives communes pour tous les systèmes d'IA à haut risque. Ces normes devraient être compatibles avec la Charte des droits fondamentaux de l'Union européenne (la

Charte) et devraient être non discriminatoires et conformes aux 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 d'intelligence artificielle, de fixer des exigences pour les systèmes d'IA à haut risque et des obligations pour les opérateurs concernés, et de prévoir des obligations de transparence pour certains systèmes d'IA.

(15) Outre les nombreuses utilisations bénéfiques de l'intelligence artificielle, cette technologie peut également être utilisée à mauvais escient et fournir des outils nouveaux et puissants pour des pratiques de manipulation, d'exploitation et de contrôle social. Ces pratiques sont particulièrement néfastes et devraient être interdites car elles sont en contradiction avec les valeurs de l'Union que sont le respect de la dignité humaine, la liberté, l'égalité, la démocratie et l'État de droit, ainsi qu'avec les droits fondamentaux de l'Union, notamment le droit à la non-discrimination, la protection des données et de la vie privée et les droits de l'enfant.

(16) Il convient d'interdire la mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA destinés à fausser le comportement humain, de sorte que des dommages physiques ou psychologiques sont susceptibles de se produire. Ces systèmes d'IA déploient des composants subliminaux que les individus ne peuvent percevoir ou exploitent les vulnérabilités des enfants et des personnes en raison de leur âge ou de leurs incapacités physiques ou mentales. Ils le font avec l'intention de déformer matériellement le comportement d'une personne et d'une manière qui cause ou est susceptible de causer un préjudice à cette personne ou à une autre. L'intention ne peut être présumée si la distorsion du comportement humain résulte de facteurs extérieurs au système d'IA qui échappent au contrôle du fournisseur ou de l'utilisateur. La recherche à des fins légitimes en relation avec de tels systèmes d'IA ne devrait pas être étouffée par l'interdiction, si cette recherche n'équivaut pas à une utilisation du système d'IA dans les relations homme-machine qui expose les personnes physiques à un préjudice et si cette recherche est menée conformément aux normes éthiques reconnues pour la recherche scientifique.

(17) Les systèmes d'IA fournissant une notation sociale des personnes physiques à des fins générales par les autorités publiques ou en leur nom peuvent conduire à des résultats discriminatoires et à l'exclusion de certains groupes. Ils peuvent violer le droit à la dignité et à la non-discrimination ainsi que les valeurs d'égalité et de justice. Ces systèmes d'IA évaluent ou classent la fiabilité des personnes physiques sur la base de leur comportement social dans de multiples contextes ou de caractéristiques personnelles ou de personnalité connues ou prédites. Le score social obtenu par ces systèmes d'IA peut conduire à un traitement préjudiciable ou défavorable de personnes physiques ou de groupes entiers de celles-ci dans des contextes sociaux sans rapport avec le contexte dans lequel les données ont été initialement générées ou collectées, ou à un traitement préjudiciable disproportionné ou injustifié par rapport à la gravité de leur comportement social. De tels systèmes d'IA devraient donc être interdits.

(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 attentatoire aux droits et libertés des personnes concernées, dans la mesure où elle peut affecter 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, l'immédiateté de l'impact et les possibilités limitées de vérifications ou de corrections ultérieures liées à l'utilisation de ces systèmes fonctionnant en "temps réel"

comportent des risques accrus pour les droits et 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 limitativement énumérées et étroitement définies, où

l'utilisation est strictement nécessaire pour atteindre un intérêt public substantiel, dont l'importance l'emporte sur les risques. Ces situations concernent la recherche de victimes potentielles de la criminalité, y compris d'enfants disparus, certaines menaces pour la vie ou la sécurité physique de personnes physiques ou d'une attaque terroriste, et la détection, la localisation, l'identification ou la poursuite d'auteurs ou de suspects des infractions pénales visées dans la décision-cadre 2002/584/JAI du Conseil38 si ces infractions pénales sont punissables dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins trois ans et telles qu'elles sont définies dans le droit de cet État membre. Ce seuil pour la peine ou la mesure de sûreté privatives de liberté, conformément au droit national, contribue à garantir que l'infraction est suffisamment grave pour justifier l'utilisation de systèmes d'identification biométrique à distance en temps réel. En outre, parmi 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 la mesure où le recours à l'identification biométrique à distance "en temps réel" sera vraisemblablement nécessaire et proportionné, à des degrés très divers, à la détection, à la localisation, à l'identification ou à la poursuite d'un auteur ou d'un suspect des différentes infractions pénales énumérées, compte tenu des différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des conséquences négatives possibles.

(20) Afin de garantir que ces systèmes sont utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune de ces trois situations limitativement énumérées et étroitement définies, certains éléments devraient être pris en compte, notamment en ce qui concerne la nature de la situation à l'origine de la demande et les conséquences de l'utilisation sur les droits et libertés de toutes les personnes concernées, ainsi que les garanties et conditions prévues pour l'utilisation. En outre, l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public aux fins de l'application de la loi devrait être soumise à des limites appropriées dans le temps et dans l'espace, compte tenu notamment des preuves ou des indications concernant les menaces, les victimes ou l'auteur. Le référentiel de personnes devrait être approprié 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 soumise à une 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 telle qu'il est effectivement et objectivement impossible d'obtenir une autorisation avant de commencer l'utilisation. Dans ces situations d'urgence, l'utilisation devrait être limitée au strict minimum nécessaire et être soumise à des garanties et conditions appropriées, déterminées par le droit national et précisées dans le contexte de chaque cas d'utilisation urgente par le service répressif lui-même. En outre, le service répressif devrait, dans de telles situations, chercher à obtenir une autorisation dès que possible, tout en fournissant les raisons pour lesquelles il n'a pas été en mesure de la demander plus tôt.

(22) En outre, il convient de prévoir, dans le cadre exhaustif fixé par le présent règlement, qu'une telle utilisation sur le territoire d'un État membre conformément au présent règlement ne devrait être possible que si et dans la mesure où l'État membre en question a décidé de prévoir expressément la possibilité d'autoriser une telle utilisation dans son

38Décision-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).

les règles détaillées du droit national. Par conséquent, les États membres restent libres, en vertu du présent règlement, de ne pas prévoir du tout une telle possibilité ou de ne prévoir une telle possibilité que pour certains des objectifs susceptibles de justifier une utilisation autorisée identifiés 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 implique nécessairement le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, qui sont fondées sur l'article 16 du TFUE, devraient s'appliquer en tant que *lex specialis à l'*égard des règles relatives au 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 concernées. 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, en dehors de ce cadre, pour les autorités compétentes, lorsqu'elles agissent à des fins répressives, d'utiliser ces systèmes et de traiter ces données en relation avec ceux-ci pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement n'est pas destiné à fournir la base juridique du traitement des données à caractère personnel en vertu de l'article 8 de la directive 2016/680. Toutefois, 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 cette utilisation à des fins répressives fixé par le présent règlement. Cette utilisation à des fins autres que répressives ne devrait donc pas être soumise à l'exigence d'une autorisation en vertu du présent règlement et des règles détaillées applicables du droit national qui peuvent lui donner effet.

(24) Tout traitement de données biométriques et d'autres données à caractère personnel intervenant dans l'utilisation de systèmes d'IA pour l'identification biométrique, autre que dans le cadre de l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives telles que réglementées 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 à respecter toutes les exigences résultant 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 n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, tel qu'annexé au TUE et au TFUE, l'Irlande n'est pas liée par les règles énoncées à l'article 5, paragraphe 1, point d), 2 et 3 du présent règlement adopté sur la base de l'article 16 du TFUE, qui concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou chapitre 5, du TFUE, lorsque l'Irlande n'est pas liée par les règles régissant les formes de coopération judiciaire en matière pénale ou de coopération policière qui exigent le respect des dispositions établies sur la base de l'article 16 du TFUE.

(26) Conformément aux articles 2 et 2 bis du protocole n° 22 sur la position du Danemark, annexé au TUE et au TFUE, le Danemark n'est pas lié par les règles prévues à l'article 5, paragraphe 1, point d), et paragraphes 2 et 3, du présent règlement, adoptées sur la base de l'article 16 du TFUE, ou sous réserve de leur application, qui concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités relevant du champ d'application de la troisième partie, titre V, chapitre 4 ou

chapitre 5, 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 sont conformes à certaines exigences obligatoires. Ces exigences devraient garantir que les systèmes d'IA à haut risque disponibles dans l'Union ou dont la production est utilisée d'une autre manière dans l'Union ne présentent pas de risques inacceptables pour les intérêts publics importants de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union. Les systèmes d'IA identifiés comme étant à haut risque devraient être limités à ceux qui ont un impact négatif significatif sur la santé, la sécurité et les droits fondamentaux des personnes dans l'Union et cette limitation réduit au minimum toute restriction potentielle au commerce international, le cas échéant.

(28) Les systèmes d'IA pourraient avoir des effets néfastes sur la santé et la sécurité des personnes, en particulier lorsque ces systèmes fonctionnent 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 dans le marché intérieur et à garantir que seuls les produits sûrs et conformes par ailleurs trouvent leur place sur le marché, il est important que les risques pour la sécurité que peut générer un produit dans son ensemble en raison de ses composants numériques, y compris les systèmes d'IA, soient dûment prévenus et atténués. Par exemple, les robots de plus en plus autonomes, que ce soit dans le contexte de la fabrication ou de l'assistance et des soins aux personnes, doivent être capables de fonctionner et d'exécuter 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 élevés, les systèmes de diagnostic de plus en plus sophistiqués et les systèmes d'aide à la décision humaine devraient être fiables et précis. L'ampleur de l'impact négatif causé par le système d'IA sur les droits fondamentaux protégés par la Charte est particulièrement importante pour classer un système d'IA comme étant 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, la non-discrimination, la protection des consommateurs, les droits des travailleurs, les droits des personnes handicapées, le droit à un recours effectif et à un procès équitable, les droits de la défense et la présomption d'innocence, le droit à une bonne administration. Outre ces droits, il est important de souligner que les enfants ont des droits spécifiques consacrés par l'article 24 de la Charte de l'Union européenne et par la Convention des Nations unies relative aux droits de l'enfant (précisée dans l'observation générale n° 25 de la CNUDE concernant l'environnement numérique), qui exigent tous deux de prendre en considération les vulnérabilités des enfants et de leur fournir la protection et les soins nécessaires à leur bien-être. Le droit fondamental à un niveau élevé de protection de l'environnement, consacré par la Charte et mis en œuvre dans les politiques de l'Union, devrait également être pris en compte lors de l'évaluation de la gravité des dommages qu'un système d'IA peut causer, notamment en ce qui concerne la santé et la sécurité des personnes.

(29) En ce qui concerne les systèmes d'IA à haut risque qui sont 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) n° 300/2008 du Parlement européen et du Conseil39, du règlement (UE) n° 167/2013 du Parlement européen et du Conseil40, du règlement (UE) n° 168/2013 du Parlement européen et du Conseil41, de la directive 2014/90/UE du

[39] Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) n° 2320/2002 (JO L 97 du 9.4.2008, p. 72).

[40] Règlement (UE) n° 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1).

[41] Règlement (UE) n° 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52).

du Parlement européen et du Conseil42, de la directive (UE) 2016/797 du Parlement européen et du Conseil43, du règlement (UE) 2018/858 du Parlement européen et du Conseil44, du règlement (UE) 2018/1139 du Parlement européen et du Conseil45 et du règlement (UE) 2019/2144 du Parlement européen et du Conseil46, il convient de modifier ces actes pour faire en sorte que la Commission tienne compte, sur la base des spécificités techniques et réglementaires de chaque secteur, et sans interférer avec les mécanismes et autorités de gouvernance, d'évaluation de la conformité et de mise en œuvre existants qui y sont établis, les exigences obligatoires relatives aux systèmes d'IA à haut risque définies dans le présent règlement lorsqu'elle adopte tout acte délégué ou d'exécution futur pertinent sur la base de ces actes.

(30) En ce qui concerne les systèmes d'IA qui sont des composants de sécurité de produits, ou qui sont eux-mêmes des produits, entrant dans le champ d'application de certaines législations d'harmonisation de l'Union, il convient de les classer comme présentant un risque élevé au titre du présent règlement si le produit en question est soumis à la procédure d'évaluation de la conformité auprès d'un organisme tiers d'évaluation de la conformité conformément à cette législation d'harmonisation de l'Union. Ces produits sont notamment les machines, les jouets, les ascenseurs, les appareils et les systèmes de protection destinés à être utilisés dans des atmosphères potentiellement explosives, les équipements hertziens, les équipements sous pression, les équipements pour bateaux de plaisance, les installations à câbles, les appareils à combustibles gazeux, les dispositifs médicaux et les dispositifs médicaux de diagnostic in vitro.

(31) La classification d'un système d'IA comme présentant un risque élevé en vertu du présent règlement ne devrait pas nécessairement signifier que le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, est considéré comme présentant un "risque élevé" selon les critères établis dans la législation d'harmonisation de l'Union pertinente qui s'applique au produit. C'est notamment le cas du règlement (UE) 2017/745 du Parlement européen et du Conseil.

---

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).

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 destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

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 la sécurité aérienne de l'Union européenne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil et le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

46 Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 concernant les exigences relatives à la réception des véhicules à moteur, de leurs remorques et des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements de la Commission (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 (JO L 325 du 16.12.2019, p. 1).

Conseil47 et le règlement (UE) 2017/746 du Parlement européen et du Conseil48, où une évaluation de la conformité par un tiers est prévue pour les produits à risque moyen et à risque élevé.

(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 sont des composants de sécurité de produits ou qui sont eux-mêmes des produits, il convient de les classer comme systèmes à haut risque si, compte tenu de leur finalité, ils présentent un risque élevé d'atteinte à la santé et à la sécurité ou aux droits fondamentaux des personnes, compte tenu à la fois de la gravité de l'atteinte éventuelle et de sa probabilité d'occurrence, et s'ils sont utilisés dans un certain nombre de domaines spécifiquement prédéfinis dans le règlement. L'identification de ces systèmes est basée sur la même méthodologie et les mêmes critères que ceux envisagés pour toute modification future de la liste des systèmes d'IA à haut risque.

(33) Les imprécisions techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Cela est particulièrement vrai en ce qui concerne l'âge, l'origine ethnique, le sexe ou les handicaps. Par conséquent, les systèmes d'identification biométrique à distance "en temps réel" et "a posteriori" doivent être classés comme présentant un risque élevé. Compte tenu des risques qu'ils présentent, ces deux types de systèmes d'identification biométrique à distance doivent 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 à haut risque les systèmes d'IA destinés à être utilisés comme éléments de sécurité dans la gestion et l'exploitation du trafic routier et la fourniture d'eau, de gaz, de chauffage et d'électricité, étant donné que leur défaillance ou leur mauvais fonctionnement peut mettre en danger la vie et la santé de personnes à grande échelle et entraîner des perturbations sensibles dans le déroulement normal des activités sociales et économiques.

(35) Les systèmes d'IA utilisés dans le cadre de l'éducation ou de la formation professionnelle, notamment pour déterminer l'accès ou l'affectation des personnes dans les établissements d'enseignement et de formation professionnelle ou pour évaluer les personnes lors de tests dans le cadre ou comme condition préalable à leur éducation, doivent être considérés comme à haut risque, car ils peuvent déterminer le parcours éducatif et professionnel d'une personne et donc affecter sa capacité à assurer sa subsistance. Lorsqu'ils sont mal conçus et utilisés, ces systèmes peuvent violer le droit à l'éducation et à la formation ainsi que le droit de ne pas être victime de discrimination et perpétuer des schémas historiques de discrimination.

(36) Les systèmes d'IA utilisés dans le cadre de l'emploi, de la gestion des travailleurs et de l'accès au travail indépendant, notamment pour le recrutement et la sélection des personnes, pour la prise de décisions en matière de promotion et de licenciement et pour la répartition des tâches, le suivi ou l'évaluation des personnes dans le cadre de relations contractuelles liées au travail, devraient également être classés comme présentant un risque élevé, étant donné que ces systèmes peuvent avoir une incidence sensible sur les perspectives de carrière et les moyens de subsistance futurs de ces personnes. Les relations contractuelles pertinentes liées au travail devraient concerner les employés et les personnes fournissant des services par l'intermédiaire des plateformes visées dans le programme de travail 2021 de la Commission. 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 dans les

[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) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

[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).

l'évaluation, la promotion ou le maintien des personnes dans des relations contractuelles liées au travail, ces systèmes peuvent perpétuer des schémas historiques de discrimination, par exemple à l'égard des femmes, de certains groupes d'âge, des personnes handicapées, des personnes de certaines origines raciales ou ethniques ou de certaines orientations sexuelles. Les systèmes d'IA utilisés pour surveiller les performances et le comportement de ces personnes peuvent également avoir un impact sur leurs droits à la protection des données et à la vie privée.

(37) Un autre domaine dans lequel l'utilisation de systèmes d'IA mérite une attention particulière est celui de l'accès à certains services et prestations privés et publics essentiels, et de la jouissance de ces services et prestations, nécessaires pour participer pleinement à la société ou pour améliorer son niveau de vie. En particulier, les systèmes d'IA utilisés pour évaluer le score de crédit ou la solvabilité des personnes physiques doivent être classés comme des systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes aux ressources financières ou aux 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 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, l'orientation sexuelle, ou créer de nouvelles formes d'impacts discriminatoires. Compte tenu de l'ampleur très limitée de l'impact et des solutions de rechange disponibles sur le marché, il convient d'exempter les systèmes d'IA destinés à l'évaluation de la solvabilité et au scoring de crédit lorsqu'ils sont mis en service par des fournisseurs à petite échelle pour leur propre usage. Les personnes physiques qui demandent ou reçoivent des prestations et des services d'assistance publique des autorités publiques sont généralement dépendantes de ces prestations et services et se trouvent dans une position vulnérable par rapport aux autorités responsables. Si des systèmes d'IA sont utilisés pour déterminer si ces prestations et services doivent être refusés, réduits, révoqués ou réclamés par les autorités, ils peuvent avoir un impact significatif sur les moyens de subsistance des personnes et porter atteinte à leurs droits fondamentaux, tels que le droit à la protection sociale, à la non-discrimination, à la dignité humaine ou à un recours effectif. Ces systèmes devraient donc être classés comme étant à haut risque. Néanmoins, le présent règlement ne devrait pas entraver le développement et l'utilisation d'approches innovantes dans l'administration publique, qui aurait tout à gagner d'une utilisation plus large de systèmes d'IA conformes et sûrs, pour autant que ces systèmes ne comportent pas de risque élevé pour les personnes morales et physiques. Enfin, les systèmes d'IA utilisés pour envoyer ou établir la priorité dans l'envoi des services de première intervention d'urgence devraient également être classés comme présentant un risque élevé, car ils prennent des décisions dans des situations très critiques pour la vie et la santé des personnes et de leurs biens.

(38) Les actions des autorités chargées de l'application de la loi impliquant certaines utilisations des systèmes d'IA se caractérisent par un degré important de déséquilibre des pouvoirs et peuvent conduire à la surveillance, à l'arrestation ou à la privation de liberté d'une personne physique, ainsi qu'à d'autres effets négatifs sur les droits fondamentaux garantis par la Charte. En particulier, si le système d'IA n'est pas formé avec des données de haute qualité, ne répond pas à des exigences adéquates en termes de précision ou de robustesse, ou n'est pas correctement conçu et testé avant d'être mis sur le marché ou mis en service d'une autre manière, il peut isoler des personnes de manière discriminatoire ou autrement incorrecte ou injuste. En outre, l'exercice d'importants droits fondamentaux procéduraux, tels que le droit à un recours effectif et à un procès équitable 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 présentant un risque élevé un certain nombre de systèmes d'IA destinés à être utilisés dans le contexte de l'application de la loi, où l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter les incidences négatives, conserver la confiance du public et garantir la responsabilité et les recours effectifs. Compte tenu de la nature des activités en question et des risques qui y sont liés, ces systèmes d'IA à haut risque devraient inclure en particulier les systèmes d'IA destinés à être utilisés par les services répressifs.

Les systèmes d'IA spécifiquement destinés aux procédures administratives des autorités fiscales et douanières ne devraient pas être considérés comme des systèmes d'IA à haut risque utilisés par les services répressifs à des fins de prévention, de détection, d'enquête et de poursuite des infractions pénales. Les systèmes d'IA spécifiquement destinés à être utilisés dans le cadre de procédures administratives par les autorités fiscales et douanières ne devraient pas être considérés comme des systèmes d'IA à haut risque utilisés par les services répressifs à des fins de prévention, de détection, d'enquête et de poursuite d'infractions pénales.

(39) Les systèmes d'IA utilisés dans le cadre de la gestion des migrations, de l'asile et des contrôles aux frontières touchent des personnes qui se trouvent souvent dans une situation particulièrement vulnérable et qui dépendent du résultat des actions des autorités publiques compétentes. La précision, 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 la protection internationale et à la bonne administration. Il convient donc de classer comme 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 des migrations, de l'asile et des contrôles aux frontières comme polygraphes et outils similaires ou pour détecter 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 demandant un visa ou l'asile ; pour vérifier l'authenticité des documents pertinents des personnes physiques ; pour assister les autorités publiques compétentes dans l'examen des demandes d'asile, de visa et de permis de séjour et des plaintes qui y sont associées, dans le but d'établir l'éligibilité des personnes physiques qui demandent un statut. Les systèmes d'IA dans le domaine de la gestion des migrations, 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 Conseil49, le règlement (CE) n° 810/2009 du Parlement européen et du Conseil50 et d'autres textes législatifs pertinents.

(40) Certains systèmes d'IA destinés à l'administration de la justice et aux processus démocratiques devraient être classés à haut risque, compte tenu de leur impact potentiellement important sur la démocratie, l'État de droit, les libertés individuelles ainsi que le droit à un recours effectif et à un procès équitable. En particulier, pour faire face aux risques de biais, d'erreurs et d'opacité potentiels, il convient de qualifier de à haut risque les systèmes d'IA destinés à aider les autorités judiciaires dans la recherche et l'interprétation des faits et du droit et dans l'application du droit à un ensemble concret de faits. Cette qualification ne devrait toutefois pas s'étendre aux systèmes d'IA destinés à des activités administratives purement accessoires qui n'affectent pas l'administration effective de la justice dans des cas individuels, comme l'anonymisation ou la pseudonymisation de décisions, de documents ou de données judiciaires, la communication entre les personnels, les tâches administratives ou l'allocation de ressources.

49Directive 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).

50Règlement (CE) n° 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).

(41) Le fait qu'un système d'IA soit classé comme étant à haut risque en vertu du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système est nécessairement légale en vertu d'autres actes du droit de l'Union ou du droit national compatible avec le droit de l'Union, tels que la protection des données à caractère personnel, l'utilisation de polygraphes et d'outils similaires ou d'autres systèmes permettant de détecter l'état émotionnel des personnes physiques. Une telle utilisation devrait continuer à se faire uniquement dans le respect des exigences applicables résultant 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 prévoyant le fondement juridique du traitement des données à caractère personnel, y compris les catégories particulières de données à caractère personnel, le cas échéant.

(42) Afin d'atténuer les risques que présentent les systèmes d'IA à haut risque placés 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 finalité de l'utilisation du système et en fonction du système de gestion des risques que doit établir le fournisseur.

(43) Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la qualité des ensembles de données utilisés, la documentation technique et l'archivage, la transparence et la fourniture d'informations aux utilisateurs, la supervision humaine, ainsi que la robustesse, la précision et la cybersécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux, le cas échéant à la lumière de la finalité du système, et aucune autre mesure moins restrictive pour le commerce n'est raisonnablement disponible, évitant ainsi des restrictions injustifiées au commerce.

(44) Une haute qualité des données est essentielle pour la performance de nombreux systèmes d'IA, en particulier lorsque des techniques impliquant la formation de modèles sont utilisées, en vue de garantir que le système d'IA à haut risque fonctionne comme prévu et en toute sécurité et qu'il ne devienne pas la source de discriminations interdites par le droit de l'Union. Des ensembles de données de formation, de validation et de test de haute qualité nécessitent la mise en œuvre de pratiques appropriées de gouvernance et de gestion des données. Les ensembles de données de formation, de validation et d'essai doivent être suffisamment pertinents, représentatifs, exempts d'erreurs et complets au regard de l'objectif visé par le système. Ils doivent également présenter les propriétés statistiques appropriées, notamment en ce qui concerne les personnes ou groupes de personnes sur lesquels le système d'IA à haut risque est censé être utilisé. En particulier, les ensembles de données de formation, de validation et d'essai devraient tenir compte, dans la mesure où cela est nécessaire compte tenu de l'objectif visé, des caractéristiques ou des éléments propres 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'autrui contre la discrimination qui pourrait résulter de la partialité des systèmes d'IA, les fournisseurs devraient pouvoir traiter également des catégories particulières de données à caractère personnel, pour des raisons d'intérêt public majeur, afin d'assurer la surveillance, la détection et la correction de la partialité des 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, comme les pôles d'innovation numérique, les installations d'expérimentation et les chercheurs, devraient pouvoir accéder à des ensembles de données de haute qualité et les utiliser dans leurs domaines d'activités respectifs qui sont liés au présent règlement. Les espaces communs de données européens établis par la Commission et la facilitation du partage des données

entre les entreprises et avec les pouvoirs publics dans l'intérêt public contribueront à fournir un accès fiable, responsable et non discriminatoire à des données de haute qualité pour la formation, la validation et 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 des algorithmes d'intelligence artificielle sur ces ensembles de données, d'une manière préservant la vie privée, sécurisée, opportune, transparente et digne de confiance, et avec une gouvernance institutionnelle appropriée. Autorités compétentes concernées,

y compris sectorielles, le fait de fournir ou de soutenir l'accès aux données peut également favoriser la fourniture de données de haute qualité pour la formation, la validation et 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 leurs performances tout au long de leur cycle de vie pour vérifier la conformité aux exigences du présent règlement. Pour ce faire, il est nécessaire de tenir des registres et de disposer d'une documentation technique contenant les informations nécessaires pour évaluer la conformité du système d'IA aux exigences applicables. Ces informations doivent comprendre les caractéristiques générales, les capacités et les limites du système, les algorithmes, les données, les processus de formation, d'essai et de validation utilisés ainsi que la documentation sur le système de gestion des risques pertinent. La documentation technique doit être tenue à jour.

(47) Pour 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 exigé pour les systèmes d'IA à haut risque. Les utilisateurs doivent être en mesure d'interpréter les résultats du système et de les utiliser de manière appropriée. Les systèmes d'IA à haut risque devraient donc être accompagnés d'une documentation et d'un mode d'emploi pertinents et comporter des informations concises et claires, notamment en ce qui concerne les risques éventuels pour les droits fondamentaux et la discrimination, le cas échéant.

(48) Les systèmes d'IA à haut risque doivent être conçus et développés de manière à ce que des personnes physiques puissent superviser leur fonctionnement. À cette fin, des mesures de surveillance humaine appropriées devraient être définies par le fournisseur du système avant sa mise sur le marché ou sa mise en service. En particulier, le cas échéant, ces mesures devraient garantir que le système est soumis à des contraintes opérationnelles intégrées qui ne peuvent être ignorées par le système lui-même et qu'il est sensible à l'opérateur humain, et que les personnes physiques auxquelles la surveillance humaine a été confiée ont la compétence, la formation et l'autorité nécessaires pour remplir ce rôle.

(49) Les systèmes d'IA à haut risque doivent avoir des performances constantes tout au long de leur cycle de vie et atteindre un niveau approprié de précision, de robustesse et de cybersécurité, conformément à l'état de l'art généralement reconnu. Le niveau de précision et les paramètres de précision doivent être communiqués aux utilisateurs.

(50) La robustesse technique est une exigence essentielle pour les systèmes d'IA à haut risque. Ils doivent être résistants aux risques liés aux limites du système (par exemple, les erreurs, les défauts, les incohérences, les situations inattendues) ainsi qu'aux actions malveillantes qui peuvent compromettre la sécurité du système d'IA et entraîner un comportement nuisible ou autrement indésirable. L'absence de protection contre ces risques pourrait avoir des répercussions sur la sécurité ou affecter négativement les droits fondamentaux, par exemple en raison de décisions erronées ou de résultats erronés ou biaisés générés par le système d'IA.

(51) La cybersécurité joue un rôle crucial en garantissant la résilience des systèmes d'IA contre les tentatives de modification de leur utilisation, de leur comportement, de leurs performances ou de la compromission de leurs propriétés de sécurité par des tiers malveillants exploitant les vulnérabilités du système. Les cyberattaques contre les systèmes d'IA peuvent exploiter des actifs spécifiques à l'IA, tels que des ensembles de données d'entraînement (par exemple, empoisonnement de données) ou des modèles entraînés (par exemple, attaques adverses), ou exploiter les vulnérabilités des actifs 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, le cas échéant, 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 des systèmes d'IA à haut risque doivent être établies conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil51 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché des produits, à la décision n° 768/2008/CE du Parlement européen et du Conseil52 relative à un cadre commun pour la commercialisation des produits et au règlement (UE) 2019/1020 du Parlement européen et du Conseil53 relatif à la surveillance du marché et à la conformité des produits ("nouveau cadre législatif pour la commercialisation des produits").

(53) Il convient qu'une personne physique ou morale spécifique, définie comme 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 celle qui a conçu ou développé le système.

(54) Le fournisseur doit établir un système de gestion de la qualité solide, veiller à l'accomplissement de la procédure d'évaluation de la conformité requise, établir la documentation pertinente et mettre en place un système solide de surveillance après la mise sur le marché. Les autorités publiques qui mettent en service des systèmes d'IA à haut risque pour leur propre usage peuvent adopter et mettre en œuvre les règles du 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 une législation sectorielle pertinente 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 dans la législation pertinente du nouveau cadre législatif devrait se conformer aux obligations du fournisseur établies dans le présent règlement et notamment veiller à ce que le système d'IA intégré dans le produit final soit conforme aux exigences du présent règlement.

(56) Pour permettre 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 des 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, avant de mettre à disposition leurs systèmes d'IA dans l'Union, lorsqu'un importateur ne peut être identifié, les fournisseurs établis en dehors de l'Union désignent, par mandat écrit, un représentant autorisé établi dans l'Union.

(57) Conformément aux principes du nouveau cadre législatif, il convient de fixer des obligations spécifiques pour les opérateurs économiques concernés, tels que les importateurs et les distributeurs, afin de garantir la sécurité juridique et de faciliter le respect de la réglementation par ces opérateurs concernés.

---

51 Règlement (CE) n° 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) n° 339/93 (JO L 218 du 13.8.2008, p. 30).

52 Décision n° 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 relatif à la surveillance du marché et à la conformité des produits et modifiant la directive 2004/42/CE ainsi que les règlements (CE) n° 765/2008 et (UE) n° 305/2011 (Texte présentant de l'intérêt pour l'EEE) (JO L 169 du 25.6.2019,

p. 1-44).

(58) Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux qui peuvent être associés à leur utilisation, y compris en ce qui concerne la nécessité d'assurer un contrôle 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 notamment utiliser les systèmes d'IA à haut risque conformément aux instructions d'utilisation et certaines autres obligations devraient être prévues en ce qui concerne le contrôle du fonctionnement des systèmes d'IA et la tenue de registres, le cas échéant.

(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 est faite dans le cadre d'une activité personnelle non professionnelle.

(60) Compte tenu de la complexité de la chaîne de valeur de l'intelligence artificielle, les tiers concernés, notamment ceux qui participent à la vente et à la fourniture de logiciels, d'outils et de composants logiciels, de modèles et de données préformés, ou les fournisseurs de services de réseau, devraient coopérer, le cas échéant, avec les fournisseurs et les utilisateurs pour leur permettre de se conformer aux obligations prévues par le présent règlement et avec les autorités compétentes établies en vertu du présent règlement.

(61) La normalisation devrait jouer un rôle clé pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec le présent règlement. La conformité aux normes harmonisées telles que définies dans le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil54 devrait être un moyen pour les fournisseurs de démontrer la conformité aux exigences du présent règlement. Toutefois, la Commission pourrait adopter des spécifications techniques communes dans les domaines où il n'existe pas de normes harmonisées ou lorsque celles-ci 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) Il convient, afin de réduire au minimum la charge imposée aux opérateurs et d'éviter toute duplication éventuelle, que, pour les systèmes d'IA à haut risque liés à des produits qui sont couverts par la législation d'harmonisation de l'Union en vigueur selon l'approche du nouveau cadre législatif, la conformité de ces systèmes d'IA aux exigences du présent règlement soit évaluée dans le cadre de l'évaluation de la conformité déjà prévue par cette législation. L'applicabilité des exigences du présent règlement ne devrait donc pas affecter la logique, la méthodologie ou la structure générale spécifiques de l'évaluation de la conformité en vertu de la législation spécifique du nouveau cadre législatif. Cette approche est pleinement reflétée dans l'interaction entre le présent règlement et le [règlement "Machines"]. Alors que les risques de sécurité des systèmes d'IA assurant des fonctions de sécurité dans les machines sont traités par les exigences du présent règlement, certaines exigences spécifiques du [règlement relatif aux machines] garantiront l'intégration sûre du système d'IA dans l'ensemble de la machine, de manière à ne pas compromettre la sécurité de la machine dans son ensemble.

---

54 Règlement (UE) n° 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 et 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 n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316, 14.11.2012, p. 12).

Le [règlement sur les machines] applique la même définition du système d'IA que le présent règlement.

(64) Compte tenu de la plus grande expérience des certificateurs professionnels avant la 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 de l'évaluation de la conformité par un tiers pour les systèmes d'IA à haut risque autres que ceux liés à des produits. Par conséquent, l'évaluation de la conformité de ces systèmes devrait être effectuée en règle générale 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 des personnes, pour lesquels l'intervention d'un organisme notifié dans l'évaluation de la conformité devrait être prévue, dans la mesure où elle n'est pas interdite.

(65) Afin de procéder à l'évaluation de la conformité par une tierce partie des systèmes d'IA destinés à être utilisés pour l'identification biométrique à distance des personnes, des organismes notifiés devraient être désignés en vertu du présent règlement par les autorités nationales compétentes, à condition qu'ils respectent un ensemble d'exigences, notamment en matière d'indépendance, de compétence et d'absence de conflits d'intérêts.

(66) Conformément à la notion communément admise de modification substantielle pour les produits régis par la législation d'harmonisation de l'Union, il convient qu'un système d'IA fasse l'objet d'une nouvelle évaluation de la conformité chaque fois que se produit un changement susceptible d'affecter la conformité du système avec le présent règlement ou lorsque la finalité du système change. En outre, en ce qui concerne les systèmes d'IA qui continuent à "apprendre" après avoir été mis sur le marché ou mis en service (c'est-à-dire qu'ils adaptent automatiquement la manière dont les fonctions sont exécutées), il est nécessaire de prévoir des règles établissant que les changements apportés à l'algorithme et à ses performances qui ont été prédéterminés par le fournisseur et évalués au moment de l'évaluation de la conformité ne doivent pas constituer une modification substantielle.

(67) Les systèmes d'IA à haut risque devraient porter le marquage CE pour indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement dans le marché intérieur. Les États membres ne devraient pas créer d'obstacles injustifiés à la mise sur le marché ou à la mise en service de systèmes d'IA à haut risque qui sont conformes aux exigences définies 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 raisons exceptionnelles de sécurité publique ou de protection de la vie et de la santé des personnes physiques et de 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 le travail de la Commission et des États membres dans le domaine de l'intelligence artificielle ainsi que 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 entrant dans le champ d'application de la législation d'harmonisation de l'Union existante pertinente, 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 être le contrôleur de cette base de données, conformément au règlement (UE) 2018/1725 du Parlement européen et du Conseil.

Conseil55. Afin de garantir la pleine fonctionnalité de la base de données, une fois déployée, la procédure de mise en place de la base de données devrait inclure l'élaboration de spécifications fonctionnelles par la Commission et 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 qualifiés de systèmes à haut risque ou non. Dans certaines circonstances, l'utilisation de ces systèmes devrait donc être soumise à des obligations de transparence spécifiques, sans préjudice des exigences et obligations applicables aux systèmes d'IA à haut risque. En particulier, les personnes physiques devraient être informées qu'elles interagissent avec un système d'IA, à moins que cela ne soit évident d'après les circonstances et le contexte d'utilisation. En outre, les personnes physiques devraient être informées lorsqu'elles sont exposées à un système de reconnaissance des émotions ou à un système de catégorisation biométrique. Ces informations et notifications devraient être fournies dans des formats accessibles aux personnes handicapées. En outre, les utilisateurs qui utilisent un système d'intelligence artificielle pour générer ou manipuler des contenus image, audio ou vidéo qui ressemblent sensiblement à des personnes, des lieux ou des événements existants et qui donneraient à une personne l'impression d'être authentique, devraient indiquer que le contenu a été créé ou manipulé artificiellement en étiquetant le résultat de l'intelligence artificielle en conséquence et en divulguant son origine artificielle.

(71) L'intelligence artificielle est une famille de technologies qui se développe rapidement et qui nécessite de nouvelles formes de surveillance réglementaire et un espace sûr pour l'expérimentation, tout en garantissant une innovation responsable et l'intégration de mesures de sauvegarde et d'atténuation des risques appropriées. Pour garantir un cadre juridique favorable à l'innovation, à l'épreuve du temps et résistant aux perturbations, les autorités nationales compétentes d'un ou de plusieurs États membres devraient être encouragées à créer des "bacs à sable" réglementaires pour l'intelligence artificielle afin de faciliter le développement et l'expérimentation de systèmes d'IA innovants sous une surveillance réglementaire stricte avant que ces systèmes ne soient mis sur le marché ou mis en service d'une autre manière.

(72) Les objectifs des bacs à sable réglementaires devraient être de favoriser l'innovation en matière d'IA en établissant un environnement d'expérimentation et de test contrôlé dans la phase de développement et de pré-commercialisation en vue de garantir la conformité des systèmes d'IA innovants avec le présent règlement et les autres législations pertinentes de l'Union et des États membres ; de renforcer la sécurité juridique pour les innovateurs ainsi que la surveillance et la compréhension par les autorités compétentes des possibilités, des risques émergents et des incidences de l'utilisation de l'IA, et d'accélérer l'accès aux marchés, notamment en supprimant les obstacles pour les petites et moyennes entreprises (PME) et les jeunes pousses. Afin de garantir une mise en œuvre uniforme dans toute l'Union et de réaliser des économies d'échelle, il convient d'établir des règles communes pour la mise en œuvre des bacs à sable réglementaires et un cadre de coopération entre les autorités compétentes participant à la supervision des bacs à sable. Le présent règlement devrait fournir la base juridique pour l'utilisation des données à caractère personnel collectées à d'autres fins pour le développement de certains systèmes d'IA dans l'intérêt public au sein du bac à sable réglementaire de 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 doivent assurer des garanties appropriées et coopérer avec les autorités compétentes, notamment en suivant leurs conseils et en agissant.

55Règlement (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).

rapidement et de bonne foi pour atténuer les risques élevés pour la sécurité et les droits fondamentaux qui peuvent survenir au cours du développement et de l'expérimentation dans le bac à sable. Le comportement des participants au bac à sable devrait être pris en compte lorsque les autorités compétentes décident d'imposer ou non une amende administrative en vertu de l'article 83, paragraphe 2, du règlement 2016/679 et de l'article 57 de la directive 2016/680.

(73) Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des fournisseurs et des utilisateurs de systèmes d'IA à petite échelle soient particulièrement pris en compte. À cette fin, les États membres devraient élaborer des initiatives destinées à ces opérateurs, notamment en matière de sensibilisation et de communication d'informations. En outre, les intérêts et les besoins spécifiques des fournisseurs à petite échelle doivent être pris en compte lorsque les organismes notifiés fixent les frais 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 autres opérateurs, notamment ceux de petite taille. Les États membres devraient éventuellement veiller à ce que l'une des langues qu'ils déterminent et acceptent pour la documentation des prestataires concernés et pour la communication avec les opérateurs soit une langue largement comprise par le plus grand nombre possible d'utilisateurs transfrontaliers.

(74) Afin de minimiser les risques pour la mise en œuvre résultant du manque de connaissances et d'expertise sur le marché, ainsi que de faciliter le respect par les fournisseurs et les organismes notifiés des obligations qui leur incombent en vertu du présent règlement, la plateforme d'IA à la demande, les pôles européens d'innovation numérique et les installations d'essai et d'expérimentation établis 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 leur mission et de leurs domaines de compétence respectifs, ils peuvent notamment apporter un soutien technique et scientifique aux prestataires et aux organismes notifiés.

(75) Il convient que la Commission facilite, dans la mesure du possible, l'accès aux installations d'essai et d'expérimentation aux organismes, groupes ou laboratoires établis ou accrédités en vertu de toute 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 cette législation d'harmonisation de l'Union. C'est notamment le cas des groupes d'experts, des laboratoires d'experts 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 harmonieuse, efficace et harmonisée du présent règlement, il convient d'établir un conseil européen de l'intelligence artificielle. Le conseil devrait être chargé d'un certain nombre de tâches consultatives, notamment l'émission 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, ainsi que la fourniture de conseils et d'une 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 la mise en œuvre du présent règlement. À cet égard, chaque État membre devrait désigner une ou plusieurs autorités nationales compétentes chargées de superviser l'application et la mise en œuvre du présent règlement. Afin d'accroître l'efficacité de l'organisation du côté des États membres et d'établir un point de contact officiel avec le public et d'autres interlocuteurs aux niveaux des États membres et de l'Union, une autorité nationale devrait être désignée

dans chaque État membre comme autorité nationale de surveillance.

(78) Afin de garantir que les fournisseurs de systèmes d'IA à haut risque puissent tenir compte de l'expérience acquise lors de l'utilisation de ces systèmes pour améliorer leurs systèmes et les systèmes d'IA à haut risque.

Si les fournisseurs ne sont pas en mesure de mener à bien le processus de conception et de développement ou de prendre des mesures correctives en temps utile, ils devraient tous mettre en place un système de surveillance post-commercialisation. Ce système est également essentiel pour garantir que les risques éventuels liés aux systèmes d'IA qui continuent à "apprendre" après leur mise sur le marché ou leur mise en service puissent être traités plus efficacement et plus rapidement. Dans ce contexte, les fournisseurs devraient également être tenus de mettre en place un système permettant de signaler aux autorités compétentes tout incident grave ou toute violation du droit national et de l'Union protégeant les droits fondamentaux résultant de l'utilisation de leurs systèmes d'IA.

(79) Afin de garantir une mise en œuvre appropriée et efficace des exigences et obligations énoncées par le présent règlement, qui est une législation d'harmonisation de l'Union, le système de surveillance du marché et de conformité des produits établi par le règlement (UE) 2019/1020 devrait s'appliquer dans son intégralité. Lorsque cela est nécessaire pour leur mandat, les autorités ou organismes publics nationaux qui contrôlent l'application du droit de l'Union protégeant les droits fondamentaux, y compris les organismes de promotion de l'égalité, devraient également avoir accès à toute documentation créée en vertu 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 prestation de ces services, y compris lorsqu'ils ont recours à des systèmes d'IA. Afin de garantir l'application et le respect cohérents 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 de l'application de la législation sur les services financiers, y compris, le cas échéant, la Banque centrale européenne, devraient être désignées comme 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 les établissements financiers réglementés et surveillés. Pour renforcer encore la cohérence entre le présent règlement et les règles applicables aux établissements de crédit réglementés en vertu de la directive 2013/36/UE du Parlement européen et du Conseil56, il convient également d'intégrer la procédure d'évaluation de la conformité et certaines des obligations procédurales des fournisseurs en matière de gestion des risques, de surveillance post-commercialisation et de documentation dans les obligations et procédures existantes en vertu de la directive 2013/36/UE. Afin d'éviter les chevauchements, des dérogations limitées devraient également être envisagées en ce qui concerne le système de gestion de la qualité des prestataires et l'obligation de surveillance imposée aux utilisateurs de systèmes d'IA à haut risque dans la mesure où ceux-ci 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 conformément aux exigences du présent règlement peut conduire à une adoption plus large de l'intelligence artificielle digne de confiance dans l'Union. Les fournisseurs de systèmes d'IA autres que ceux 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 également être encouragés à appliquer, sur une base volontaire, des exigences supplémentaires concernant, par exemple, la durabilité environnementale, l'accessibilité aux personnes handicapées, la participation des parties prenantes à la conception et au développement des systèmes d'IA et la diversité des équipes de développement. La Commission peut mettre en place des initiatives, y compris des initiatives sectorielles.

[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).

nature, pour faciliter l'abaissement des obstacles techniques qui entravent l'échange transfrontalier 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 de différents types de données.

(82) Il est important que les systèmes d'IA liés à des produits qui ne sont pas à haut risque conformément au présent règlement et qui ne sont donc pas tenus de respecter les exigences qui y sont énoncées soient néanmoins sûrs lorsqu'ils sont mis sur le marché ou mis en service. Pour contribuer à cet objectif, la directive 2001/95/CE du Parlement européen et du Conseil57 s'appliquerait en tant que filet de sécurité.

(83) Afin d'assurer une coopération confiante et constructive des autorités compétentes au niveau de l'Union et au niveau national, toutes les parties concernées par l'application du présent règlement devraient respecter la confidentialité des informations et des données obtenues dans l'accomplissement de leurs tâches.

(84) Les États membres devraient prendre toutes les mesures nécessaires pour assurer la mise en œuvre des dispositions du présent règlement, notamment en prévoyant des sanctions efficaces, proportionnées et dissuasives en cas d'infraction. Pour certaines infractions spécifiques, les États membres devraient tenir compte des marges et des critères énoncés dans le présent règlement. Le contrôleur européen de la protection des données devrait avoir le pouvoir d'imposer des amendes aux institutions, agences et organes de l'Union relevant du champ d'application du présent règlement.

(85) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, le pouvoir d'adopter des actes conformément à l'article 290 du TFUE devrait être délégué à la Commission pour modifier les techniques et approches visées à l'annexe I pour définir les systèmes d'IA, la législation d'harmonisation de l'Union énumérée à l'annexe II, les systèmes d'IA à haut risque énumérés à l'annexe III, les dispositions relatives à la documentation technique figurant à l'annexe IV, le contenu de la déclaration de conformité de l'UE figurant à l'annexe V, les dispositions relatives aux procédures d'évaluation de la conformité figurant aux annexes VI et VII et les dispositions établissant les systèmes d'IA à haut risque auxquels 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 doit s'appliquer. Il est particulièrement important que la Commission procède à des consultations appropriées au cours de ses travaux préparatoires, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer "58. En particulier, pour 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 traitant de la préparation des actes délégués.

(86) Afin d'assurer des conditions uniformes pour la mise en œuvre du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil59.

(87) Étant donné que l'objectif du présent règlement ne peut pas être réalisé de manière suffisante par les États membres et peut plutôt, en raison de l'ampleur ou des effets de l'action, être mieux réalisé

---

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).

[58]OJ L 123 du 12.5.2016, p. 1.

[59] Règlement (UE) n° 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).

au niveau de l'Union, l'Union peut adopter des mesures conformément au principe de subsidiarité tel qu'énoncé 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 partir du ... [*PO - 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 partir du ... [*PO - veuillez insérer la date - trois mois après l'entrée en vigueur du présent règlement*]. En outre, les États membres devraient établir et notifier à la Commission les règles relatives aux sanctions, y compris les amendes administratives, et veiller à ce qu'elles soient correctement et effectivement mises en œuvre à la date d'application du présent règlement. Par conséquent, les dispositions relatives aux sanctions devraient s'appliquer à partir du [*PO - 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 conseil 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 sur [...]".

ONT ADOPTÉ CE RÈGLEMENT :

TITRE I

DISPOSITIONS

GÉNÉRALES

Article 1 Objet

Le présent règlement
établit :

(a) des règles harmonisées pour la mise sur le marché, la mise en service et l'utilisation des systèmes d'intelligence artificielle ("systèmes IA") dans l'Union ;

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

(b) des exigences spécifiques pour les systèmes d'IA à haut risque et des obligations pour les opérateurs de ces systèmes ;

(c) des règles de transparence harmonisées pour les systèmes d'IA destinés à interagir avec des personnes physiques, les systèmes de reconnaissance des émotions et les systèmes de catégorisation biométrique, ainsi que les systèmes d'IA utilisés pour générer ou manipuler des contenus image, audio ou vidéo ;

(d) les règles relatives au contrôle et à la surveillance du marché.

s'applique à :

1. Le présent règlement

Art cle 2 Champ d'application

(a) les prestataires mettant sur le marché ou mettant en service des systèmes d'IA dans l'Union, que ces prestataires soient établis dans l'Union ou dans un pays tiers ;

(b) les utilisateurs de systèmes d'IA situés dans l'Union ;

(c) les fournisseurs et les utilisateurs de systèmes d'IA situés dans un pays tiers, lorsque le résultat produit par le système est utilisé dans l'Union ;

2. Pour les systèmes IA à haut risque qui sont des composants de sécurité de produits ou de systèmes, ou qui sont eux-mêmes des produits ou des systèmes, relevant du champ d'application des actes suivants, seul l'article 84 du présent règlement s'applique :

(a) Règlement (CE) 300/2008 ;

(b) Règlement (UE) n° 167/2013 ;

(c) Règlement (UE) n° 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 policière et judiciaire 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 de services intermédiaires énoncées au chapitre II, section IV, de la directive 2000/31/CE du Parlement européen et du Conseil60 [*telle qu'elle doit être remplacée par les dispositions correspondantes de la loi sur les services numériques*].

Article 3
Définitions

Aux fins du présent règlement, les définitions suivantes s'appliquent :

(1) "système d'intelligence artificielle" (système IA) : un logiciel développé à l'aide d'une ou plusieurs des techniques et approches énumérées à l'annexe I et capable, pour un ensemble donné d'objectifs définis par l'homme, de générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels ils interagissent ;

(1) "fournisseur" : une personne physique ou morale, une autorité publique, une agence ou un 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 ;

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).

(3) petit prestataire" : un prestataire qui est une micro ou une petite entreprise au sens de la recommandation 2003/361/CE de la Commission61 ;

(4) utilisateur" : toute personne physique ou morale, autorité publique, agence ou autre organisme utilisant un système d'IA sous son autorité, sauf lorsque le système d'IA est utilisé dans le cadre d'une activité personnelle non professionnelle ;

(5) représentant autorisé" : toute personne physique ou morale établie dans l'Union qui a reçu un mandat écrit du fournisseur d'un système d'IA pour, respectivement, remplir et exécuter en son nom les obligations et 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 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 en modifier les propriétés ;

(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 en vue de sa distribution ou de son utilisation 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 pour une première utilisation directement à l'utilisateur ou pour une utilisation propre sur le marché de l'Union, aux fins prévues ;

(12) finalité" : l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions d'utilisation spécifiques, tels que spécifiés dans les informations fournies par le fournisseur dans les instructions d'utilisation, le matériel promotionnel ou de vente et les déclarations, ainsi que dans la documentation technique ;

(13) abus raisonnablement prévisible" : l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa finalité, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction 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) mode d'emploi" : les informations fournies par le fournisseur pour informer l'utilisateur, en particulier, de la finalité et de la bonne utilisation d'un système d'IA, y compris le cadre géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est censé être utilisé ;

(16) rappel d'un système d'IA", toute mesure visant à obtenir le rendement pour le fournisseur d'un système d'IA mis à la disposition des utilisateurs ;

---

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).

(17) retrait d'un système d'IA" : toute mesure visant à empêcher la distribution, la présentation et l'offre d'un système d'IA ;

(18) performance d'un système d'IA", la capacité d'un système d'IA à atteindre l'objectif prévu ;

(19) autorité notifiante" : l'autorité nationale chargée de mettre en place et d'appliquer les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité, ainsi qu'à leur contrôle ;

(20) évaluation de la conformité" : le processus consistant à vérifier si les exigences énoncées au titre III, chapitre 2, du présent règlement concernant un système d'IA ont été respectées ;

(21) organisme d'évaluation de la conformité" : un organisme qui effectue des activités d'évaluation de la conformité par une tierce partie, y compris des essais, une certification et une inspection ;

(22) organisme notifié" : organisme d'évaluation de la conformité désigné conformément au présent règlement et aux autres dispositions législatives d'harmonisation pertinentes de l'Union ;

(23) modification substantielle" : un changement apporté au système d'IA après sa mise sur le marché ou sa mise en service, qui a une incidence sur la conformité du système d'IA aux exigences énoncées au titre III, chapitre 2, du présent règlement ou qui entraîne une modification de la finalité pour laquelle le système d'IA a été évalué ;

(24) Marquage CE de conformité" (marquage CE) : marquage par lequel un fournisseur indique qu'un système d'IA est conforme aux exigences énoncées au titre III, chapitre 2, du présent règlement et à toute autre législation de l'Union applicable harmonisant les conditions de commercialisation des produits ("législation d'harmonisation de l'Union") prévoyant son apposition ;

(25) surveillance post-commercialisation" : toutes les activités menées par les fournisseurs de systèmes d'IA pour recueillir et examiner de manière proactive l'expérience acquise dans le cadre de l'utilisation des systèmes d'IA qu'ils mettent sur le marché ou en service, afin de déterminer s'il est nécessaire d'appliquer immédiatement les mesures correctives ou préventives requises ;

(26) autorité de surveillance du marché" : l'autorité nationale qui exerce les activités et prend les mesures conformément au règlement (UE) 2019/1020 ;

(27) "norme harmonisée" : une norme européenne telle que définie à l'article 2, paragraphe 1, point c), du règlement (UE) n° 1025/2012 ;

(28) spécifications communes", un document, autre qu'une norme, contenant des solutions techniques permettant de se conformer à certaines exigences et obligations établies en vertu du présent règlement ;

(29) données d'apprentissage" : données utilisées pour l'apprentissage d'un système d'IA par l'ajustement de ses paramètres apprenables, y compris les poids d'un réseau neuronal ;

(30) données de validation" : données utilisées pour fournir une évaluation du système d'intelligence artificielle formé et pour régler ses paramètres non apprenables et son processus d'apprentissage, entre autres choses, afin d'éviter un surajustement ; l'ensemble de données de validation peut être un ensemble de données distinct ou une partie de l'ensemble de données de formation, sous la forme d'une division fixe ou variable ;

(31) données d'essai", les données utilisées pour fournir une évaluation indépendante du

système d'IA formé 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 acquises directement par celui-ci, sur la base desquelles le système produit un résultat ;

(33) données biométriques" : les données à caractère personnel résultant d'un traitement technique spécifique relatif aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment l'identification unique de cette personne physique, telles que les images faciales ou les données dactyloscopiques ;

(34) système de reconnaissance des émotions", un système d'intelligence artificielle destiné à identifier ou à déduire les émotions ou les intentions des personnes physiques sur la base de leurs données biométriques ;

(35) système de catégorisation biométrique" : un système d'IA permettant d'attribuer des personnes physiques à des catégories spécifiques, telles que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou l'orientation sexuelle ou politique, 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 par comparaison des données biométriques d'une personne avec les données biométriques contenues dans une base de données de référence, et sans que l'utilisateur du système d'IA sache au préalable si la personne sera présente et pourra être identifiée ;

(37) Système d'identification biométrique à distance "en temps réel" : système d'identification biométrique à distance dans lequel la saisie des données biométriques, la comparaison et l'identification s'effectuent toutes sans délai important. Cela comprend non seulement l'identification instantanée, mais aussi des délais courts et limités afin d'éviter les contournements.

(38) système d'identification biométrique à distance "post"" : système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance "en temps réel" ;

(39) espace accessible au public" : tout lieu physique accessible au public, indépendamment du fait que certaines conditions d'accès puissent s'appliquer ;

(40) Par "autorité chargée de l'application de la loi", on entend

(a) toute autorité publique compétente pour la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la sauvegarde et la prévention des menaces à la sécurité publique ; ou

(b) tout autre organe ou entité chargé par le droit des États membres d'exercer l'autorité et les pouvoirs publics aux fins de la prévention, de la recherche, de la détection ou de la poursuite d'infractions pénales ou de l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et leur prévention ;

(41) Par "application de la loi", on entend les activités menées par les autorités chargées de l'application de la loi pour la prévention, les enquêtes, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la protection et la prévention des menaces pour la sécurité publique ;

(42) autorité de surveillance nationale" : l'autorité à laquelle un État membre confie la responsabilité de la mise en œuvre et de l'application du présent règlement, de la coordination des activités confiées à cet État membre, de la fonction de point de contact unique pour la Commission et de la représentation de l'État membre au sein du Conseil européen de l'intelligence artificielle ;

(43) autorité nationale compétente", l'autorité nationale de surveillance, l'autorité de notification et l'autorité de surveillance du marché ;

(44) incident grave" : tout incident qui, directement ou indirectement, conduit, aurait pu conduire ou pourrait conduire à l'une des situations suivantes :

(a) la mort d'une personne ou des dommages graves à la santé d'une personne, aux biens ou à l'environnement,

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

Article 4
Modifications de l'annexe I

La Commission est habilitée à adopter des actes délégués conformément à l'article 73 pour modifier la liste des techniques et approches énumérées à l'annexe I, afin d'actualiser cette liste 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 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 déploie des techniques subliminales au-delà de la conscience d'une personne afin de déformer matériellement le comportement d'une personne d'une manière qui cause ou est susceptible de causer à cette personne ou à une autre un préjudice physique ou psychologique ;

(b) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite l'une des vulnérabilités d'un groupe spécifique de personnes en raison de leur âge ou de leur handicap physique ou mental, afin de fausser matériellement le comportement d'une personne appartenant à ce groupe d'une manière qui cause ou est susceptible de causer à cette personne ou à une autre un préjudice physique ou psychologique ;

(c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA par les autorités publiques ou en leur nom pour l'évaluation ou la classification de la fiabilité des personnes physiques pendant une certaine période de temps, sur la base de leur comportement social ou de caractéristiques personnelles ou de personnalité connues ou prévues, le score social conduisant à l'un ou l'autre des éléments suivants, ou aux deux :

(i) traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de celles-ci dans des contextes sociaux sans rapport avec les contextes dans lesquels les données ont été initialement générées ou collectées ;

(ii) un traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de celles-ci, injustifié ou disproportionné

par rapport à leur comportement social ou à sa gravité ;

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

(i) la recherche ciblée de victimes potentielles spécifiques de la criminalité, y compris les enfants disparus ;

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

(iii) la détection, la localisation, l'identification ou la poursuite 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 Conseil62 et punie dans l'État membre concerné d'une peine ou d'une mesure de sûreté privatives de liberté d'un maximum d'au moins trois ans, conformément à la législation de cet État membre.

2. L'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans les espaces accessibles au public à des fins répressives pour l'un des objectifs visés au paragraphe 1, point d), tient compte des éléments suivants :

(a) la nature de la situation donnant lieu à l'utilisation éventuelle, notamment la gravité, la probabilité et l'ampleur du préjudice causé en l'absence de l'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 biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives pour l'un des objectifs visés au paragraphe 1, point d), est assortie des garanties et conditions nécessaires et proportionnées relatives à cette utilisation, notamment en ce qui concerne les limitations temporelles, géographiques et personnelles.

3. En ce qui concerne le paragraphe 1, point d), et le paragraphe 2, chaque utilisation individuelle, à des fins répressives, d'un système d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public est soumise à une autorisation préalable accordée par une autorité judiciaire ou par une autorité administrative indépendante de l'État membre dans lequel l'utilisation doit avoir lieu, délivrée sur demande motivée et conformément aux modalités du droit national visées au paragraphe 4. Toutefois, dans une situation d'urgence dûment justifiée, l'utilisation du système peut être commencée sans autorisation et l'autorisation ne peut être demandée que pendant ou après l'utilisation.

L'autorité judiciaire ou administrative compétente n'accorde l'autorisation que si elle est convaincue, 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 question est nécessaire et proportionnée à la réalisation de l'un des objectifs spécifiés au paragraphe 1, point d), tels qu'identifiés dans la demande. Pour statuer sur la demande, l'autorité judiciaire ou administrative compétente prend en compte les 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 biométrique à distance "en temps réel" dans les espaces accessibles au public à des fins répressives, dans les limites et sous les conditions suivantes

62Décision-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).

les conditions énumérées au paragraphe 1, point d), et aux paragraphes 2 et 3. Cet État membre fixe dans son droit national les modalités nécessaires pour la demande, la délivrance et l'exercice des autorisations visées au paragraphe 3, ainsi que pour le contrôle y afférent. Ces règles précisent également pour quels objectifs énumérés au paragraphe 1, point d), y compris pour quelles infractions pénales visées au point iii), les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives.

TITRE III

SYSTÈMES D'AI À

HAUT RISQUE CHAPITRE

1

CLASSIFICATION DES SYSTÈMES AI COMME ÉTANT À HAUT RISQUE

Article 6
Règles de classification pour les systèmes d'IA à haut risque

1. Indépendamment du fait qu'un système d'IA soit mis sur le marché ou mis en service indépendamment des produits visés aux points a) et b), ce système d'IA 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, ou est lui-même un produit, couvert par la législation d'harmonisation de l'Union énumérée à l'annexe II ;

   (b) le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, doit faire l'objet d'une évaluation de conformité par une tierce partie en vue de la mise sur le marché ou de la mise en service de ce produit, conformément à la législation d'harmonisation de l'Union visée 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 pour mettre à jour la liste de l'annexe III en 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 aux points 1 à 8 de l'annexe III ;

   (b) les systèmes d'IA présentent un risque d'atteinte à la santé et à la sécurité, ou un risque d'impact négatif sur les droits fondamentaux, qui est, en ce qui concerne sa gravité et sa probabilité d'occurrence, équivalent ou supérieur au risque d'atteinte ou d'impact négatif présenté par les systèmes d'IA à haut risque déjà

visés à l'annexe III.

2. Lorsqu'il s'agit d'évaluer, aux fins du paragraphe 1, si un système d'IA présente un risque d'atteinte à la santé et à la sécurité ou un risque d'impact négatif sur les droits fondamentaux qui est équivalent ou supérieur au risque d'atteinte présenté par les systèmes d'IA à haut risque

déjà visés à l'annexe III, la Commission prend en compte les critères suivants :

(a) l'objectif visé par le 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 ou un impact négatif sur les droits fondamentaux, ou a suscité des préoccupations importantes quant à la matérialisation de ce préjudice ou de cet impact négatif, comme le démontrent les rapports ou les allégations documentées soumis aux autorités nationales compétentes ;

(d) l'étendue potentielle d'un tel préjudice ou d'un tel impact négatif, notamment en termes d'intensité et de capacité à affecter une pluralité de personnes ;

(e) la mesure dans laquelle les personnes potentiellement lésées ou ayant subi des effets négatifs dépendent du résultat produit par un système d'IA, notamment parce que, pour des raisons pratiques ou juridiques, il n'est pas raisonnablement possible de renoncer à ce résultat ;

(f) la mesure dans laquelle les personnes potentiellement lésées ou ayant subi un impact négatif se trouvent dans une position 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 de l'âge ;

(g) la mesure dans laquelle le résultat produit par un système d'IA est facilement réversible, les résultats ayant un impact sur la santé ou la sécurité des personnes n'étant pas considérés comme facilement réversibles ;

(h) la mesure dans laquelle la législation existante de l'Union prévoit :

(i) des mesures de réparation efficaces par rapport aux risques posés par un système d'IA, à l'exclusion des demandes de dommages et intérêts ;

(ii) des mesures efficaces pour prévenir ou minimiser substantiellement ces risques.

CHAPITRE 2

EXIGENCES POUR LES SYSTÈMES AI À HAUT RISQUE

Article 8
Respect des exigences

1. Les systèmes d'IA à haut risque doivent être conformes aux exigences établies dans le présent chapitre.

2. La finalité du système d'IA à haut risque et du système de gestion des risques visés à l'article 9 est prise en compte pour assurer le respect de ces exigences.

Article 9
Système de gestion des risques

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

2. Le système de gestion des risques consiste en un processus itératif continu qui se déroule tout au long du cycle de vie d'un système d'IA à haut risque et qui nécessite une mise à jour systématique régulière. Il comprend les étapes suivantes :

(a) identification et analyse des risques connus et prévisibles associés à chaque système d'IA à haut risque ;

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

(c) l'évaluation d'autres risques éventuels sur la base de l'analyse des données recueillies dans le cadre 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), prennent dûment en considération les effets et les interactions possibles résultant de l'application combinée des exigences énoncées au présent chapitre 2. Elles tiennent compte de l'état de l'art 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 des 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 prévisibles. Ces risques résiduels sont communiqués à l'utilisateur.

Lors de l'identification des mesures de gestion des risques les plus appropriées, il convient de veiller aux points suivants :

(a) l'élimination ou la réduction des risques dans toute la mesure du possible par une conception et un développement adéquats ;

(b) le cas échéant, la mise en œuvre de mesures d'atténuation et de contrôle adéquates en ce qui concerne les risques qui ne peuvent être éliminés ;

(c) la fourniture d'une information adéquate 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, la formation des utilisateurs.

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 et de la formation attendues de l'utilisateur, ainsi que de l'environnement dans lequel le système est destiné à être utilisé.

5. Les systèmes d'IA à haut risque sont testés afin d'identifier les mesures de gestion des risques les plus appropriées. Les tests doivent garantir que les systèmes d'IA à haut risque fonctionnent de manière cohérente pour l'usage auquel ils sont destinés et qu'ils sont conformes aux exigences énoncées dans le présent chapitre.

6. Les procédures de test doivent permettre d'atteindre l'objectif visé par le 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, le cas échéant, à tout moment du processus de développement et, en tout état de cause, avant la mise sur le marché ou la mise en service. Les tests sont effectués par rapport à des paramètres et des seuils probabilistes définis au préalable et adaptés à l'objectif visé par le 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'examiner spécifiquement si le système d'IA à haut risque est susceptible d'être consulté par des enfants ou d'avoir un impact sur eux.

9. Pour les établissements de crédit régis 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 qui font appel à des techniques impliquant l'apprentissage de modèles avec des données sont développés sur la base d'ensembles de données d'apprentissage, de validation et d'essai qui répondent aux critères de qualité visés aux paragraphes 2 à 5.

2. Les ensembles de données de formation, de validation et d'essai sont soumis à des pratiques appropriées 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 pertinentes de traitement de 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 la pertinence des ensembles de données nécessaires ;

   (f) l'examen en vue d'éventuels biais ;

   (g) l'identification des éventuelles lacunes ou insuffisances des données, et la manière dont ces lacunes et insuffisances peuvent être traitées.

3. Les ensembles de données de formation, de validation et d'essai sont pertinents, représentatifs, exempts d'erreurs et complets. Ils présentent les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes sur lesquels le système d'IA à haut risque est destiné à être utilisé. Ces caractéristiques des ensembles de données peuvent être satisfaites au niveau des ensembles de données individuels ou d'une combinaison de ceux-ci.

4. Les ensembles de données de formation, de validation et d'essai tiennent compte, dans la mesure requise par l'objectif visé, des caractéristiques ou des éléments propres au cadre 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 pour assurer la surveillance, la détection et 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 à la réutilisation et à l'utilisation de mesures de sécurité et de préservation de la vie privée à la pointe de la technologie, telles que la pseudonymisation, ou le cryptage lorsque

l'anonymisation peut affecter de manière significative la finalité poursuivie.

6. Des pratiques appropriées 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'apprentissage 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 d'un système d'IA à haut risque doit être établie avant la mise sur le marché ou la mise en service de ce système et doit être tenue à jour.

   La documentation technique est établie de manière à démontrer que le système d'IA à haut risque est conforme aux exigences énoncées dans le présent chapitre et à fournir aux autorités compétentes nationales et aux organismes notifiés toutes les informations nécessaires pour évaluer la conformité du système d'IA à ces exigences. Il contient, au minimum, les éléments figurant 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 desdits actes juridiques.

3. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 pour modifier l'annexe IV si nécessaire afin de garantir que, compte tenu du progrès technique, la documentation technique fournit toutes les informations nécessaires pour évaluer la conformité du système aux exigences énoncées dans le présent chapitre.

Article 12
Tenue de registres

1. Les systèmes d'IA à haut risque doivent être conçus et développés avec des capacités permettant l'enregistrement automatique d'événements ("journaux") pendant le fonctionnement des systèmes d'IA à haut risque. Ces capacités d'enregistrement doivent être conformes aux normes reconnues ou aux spécifications communes.

2. Les capacités de journalisation doivent garantir un niveau de traçabilité du fonctionnement du système d'IA tout au long de son cycle de vie qui soit adapté à la finalité du système.

3. En particulier, les capacités de journalisation permettent de surveiller le fonctionnement du système d'IA à haut risque en ce qui concerne l'apparition de situations susceptibles d'amener le système d'IA à présenter un risque au sens de l'article 65, paragraphe 1, ou d'entraîner une modification substantielle, et de faciliter la surveillance après la mise sur le marché visée à l'article 61.

4. Pour les systèmes d'IA à haut risque visés à l'annexe III, paragraphe 1, point a), les capacités de journalisation fournissent au moins les éléments suivants :

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

   (b) la base de données de référence par rapport à laquelle les données d'entrée ont été vérifiées par le système ;

   (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, telle que visée à l'article 14, paragraphe 5.

Article 13
Transparence et fourniture d'informations aux utilisateurs

1. Les systèmes d'IA à haut risque sont conçus et développés de manière à ce que leur fonctionnement soit suffisamment transparent pour permettre aux utilisateurs d'interpréter les résultats du système et de les utiliser de manière appropriée. Un type et un degré de transparence appropriés sont assurés, en vue de respecter les obligations pertinentes de l'utilisateur et du fournisseur énoncées au chapitre 3 du présent titre.

2. Les systèmes d'IA à haut risque sont accompagnés d'un mode d'emploi dans un format numérique approprié ou autre, qui comprend des informations concises, complètes, correctes et claires qui sont pertinentes, accessibles et compréhensibles pour les utilisateurs.

3. Les informations visées au paragraphe 2 précisent :

(a) l'identité et les coordonnées du prestataire et, le cas échéant, de son représentant autorisé ;

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

(i) sa finalité ;

(ii) le niveau de précision, de robustesse et de cybersécurité visé à l'article 15 par rapport auquel le système d'IA à haut risque a été testé et validé et auquel on peut s'attendre, ainsi que toutes les circonstances connues et prévisibles qui peuvent avoir une incidence sur ce niveau attendu de précision, de robustesse et de cybersécurité ;

(iii) toute circonstance connue ou prévisible, liée à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisibles, pouvant entraîner des risques pour la santé et la sécurité ou les droits fondamentaux ;

(iv) ses performances à l'égard des personnes ou groupes de personnes sur lesquels le système est destiné à être utilisé ;

(v) le cas échéant, les spécifications des données d'entrée, ou toute autre information pertinente en termes d'ensembles de données d'entraînement, de validation et d'essai utilisés, en tenant compte de la finalité 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 surveillance humaine visées à l'article 14, y compris les mesures techniques mises en place pour faciliter l'interprétation des résultats des systèmes d'IA par les utilisateurs ;

(e) la durée de vie prévue du système d'IA à haut risque et toute mesure de maintenance et d'entretien nécessaire pour assurer le bon fonctionnement de ce système d'IA, y compris en ce qui concerne les mises à jour logicielles.

Article 14
Surveillance de l'homme

1. Les systèmes d'IA à haut risque sont conçus et développés, notamment à l'aide d'outils d'interface homme-machine appropriés, de manière à pouvoir être effectivement surveillés par des personnes physiques pendant la période d'utilisation du système d'IA.

2. La surveillance humaine 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 prévisibles, en particulier lorsque ces risques persistent malgré l'application des autres exigences énoncées dans le présent chapitre.

3. La surveillance humaine est assurée par l'une ou l'ensemble des mesures suivantes :

   (a) identifiés et intégrés, lorsque cela est techniquement possible, dans le système d'IA à haut risque par le fournisseur avant sa mise sur le marché ou sa mise en service ;

   (b) identifiés par le fournisseur avant la mise sur le marché ou la mise en service du système d'IA à haut risque et qui sont appropriés pour être mis en œuvre par l'utilisateur.

4. Les mesures visées au paragraphe 3 permettent aux personnes auxquelles la surveillance humaine est confiée de faire ce qui suit, en fonction des circonstances :

   (a) comprendre pleinement les capacités et les limites du système d'IA à haut risque et être en mesure de surveiller dûment son fonctionnement, de manière à pouvoir détecter les signes d'anomalies, de dysfonctionnements et de performances inattendues et y remédier dans les meilleurs délais ;

   (b) rester conscient de la tendance possible à se fier automatiquement ou à trop se fier au résultat produit 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 pour des décisions à prendre par des personnes physiques ;

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

   (d) être en mesure de décider, dans toute situation particulière, de ne pas utiliser le système d'IA à haut risque ou d'ignorer, d'annuler ou d'inverser les résultats du système d'IA à haut risque ;

   (e) être en mesure d'intervenir sur le fonctionnement du système d'IA à haut risque ou d'interrompre le système par un bouton "stop" ou une procédure similaire.

5. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 1 a), les mesures visées au paragraphe 3 sont de nature à garantir, en outre, qu'aucune action ou décision ne soit prise par l'utilisateur sur la base de l'identification résultant du système, à moins que celle-ci n'ait été vérifiée et confirmée par au moins deux personnes physiques.

Article 15
Précision, robustesse et cybersécurité

1. Les systèmes d'IA à haut risque sont conçus et développés de manière à atteindre,

compte tenu de leur finalité, un niveau de précision approprié,

la robustesse et la cybersécurité, et présentent des performances constantes à ces égards tout au long de leur cycle de vie.

2. Les niveaux de précision et les paramètres de précision pertinents des systèmes d'IA à haut risque sont déclarés dans les instructions d'utilisation qui les accompagnent.

3. Les systèmes d'IA à haut risque doivent être résilients en ce qui concerne les erreurs, les défauts ou les incohérences qui peuvent survenir au sein du système ou de l'environnement dans lequel le système fonctionne, notamment en raison de leur interaction avec des personnes physiques ou d'autres systèmes.

   La robustesse des systèmes d'IA à haut risque peut être obtenue par des solutions techniques de redondance, qui peuvent inclure des plans de sauvegarde ou de sécurité intégrée.

   Les systèmes d'IA à haut risque qui continuent d'apprendre après avoir été mis sur le marché ou mis en service sont développés de manière à garantir que les résultats éventuellement biaisés en raison des résultats utilisés comme données d'entrée pour des opérations futures ("boucles de rétroaction") sont dûment traités par des mesures d'atténuation appropriées.

4. Les systèmes d'IA à haut risque doivent être résilients face aux tentatives de tiers non autorisés de modifier leur utilisation ou leurs performances en exploitant les vulnérabilités du système.

   Les solutions techniques visant à assurer la cybersécurité des systèmes d'IA à haut risque doivent être adaptées aux circonstances et aux risques.

   Les solutions techniques visant à remédier aux vulnérabilités spécifiques de l'IA doivent inclure, le cas échéant, des mesures de prévention et de contrôle des attaques visant à manipuler l'ensemble de données d'entraînement ("empoisonnement des données"), des entrées conçues pour que le modèle commette une erreur ("exemples adverses") ou des défauts de modèle.

CHAPITRE 3

OBLIGATIONS DES FOURNISSEURS ET DES UTILISATEURS DE SYSTÈMES AI À HAUT RISQUE ET D'AUTRES PARTIES

Article 16
Obligations des fournisseurs de systèmes d'IA à haut risque

Les fournisseurs de systèmes d'IA à haut risque doivent :

(a) s'assurer que leurs systèmes d'IA à haut risque sont conformes aux exigences énoncées au chapitre 2 du présent titre ;

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

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

(d) lorsqu'ils sont sous leur contrôle, conservent les journaux générés automatiquement par leurs systèmes d'IA à haut risque ;

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

(f) se conformer aux obligations d'enregistrement visées à l'article 51 ;

(g) prendre 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) informer les autorités nationales compétentes des États membres dans lesquels elles ont mis le système d'IA à disposition ou l'ont mis en service et, le cas échéant, l'organisme notifié, de la non-conformité et des mesures correctives prises ;

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

(j) à la demande d'une autorité nationale compétente, démontrer 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 qui garantit le respect du présent règlement. Ce système est documenté de manière systématique et ordonnée sous la forme de politiques, de procédures et d'instructions écrites, et comprend au moins les aspects suivants :

(a) une stratégie de conformité réglementaire, y compris le respect des procédures d'évaluation de la conformité et des procédures de gestion des modifications du système d'IA à haut risque ;

(b) les techniques, procédures et actions systématiques à utiliser pour la conception, le contrôle de la conception et la vérification de la conception du système d'IA à haut risque ;

(c) les techniques, procédures et actions systématiques à utiliser pour le développement, le contrôle et l'assurance de la qualité du système d'IA à haut risque ;

(d) les procédures d'examen, de test et de validation à effectuer avant, pendant et après le développement du système d'IA à haut risque, et la fréquence à laquelle elles doivent être effectuées ;

(e) les spécifications techniques, y compris les normes, à appliquer et, lorsque les normes harmonisées pertinentes ne sont pas appliquées intégralement, les moyens à utiliser pour garantir que le système d'IA à haut risque est conforme aux exigences énoncées au chapitre 2 du présent titre ;

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

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

(h) l'établissement, la mise en œuvre et la maintenance d'un système de surveillance post-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) le traitement de la communication avec les autorités nationales compétentes, les autorités compétentes, y compris les autorités sectorielles, fournissant ou soutenant l'accès aux données, les organismes notifiés, les autres opérateurs, les clients ou les autres parties intéressées ;

(k) des systèmes et des procédures d'enregistrement de tous les documents et

informations pertinents ;

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

(m) un cadre de responsabilisation définissant les responsabilités de la direction et des autres membres du personnel en ce qui concerne tous les aspects énumérés dans ce paragraphe.

2. La mise en œuvre des aspects visés au paragraphe 1 est proportionnelle à la taille de l'organisation du prestataire.

3. Pour les prestataires qui sont des établissements de crédit régis par la directive 2013/36/UE, l'obligation de mettre en place un système de gestion de la qualité est réputée satisfaite par le respect des règles relatives aux dispositions, processus et mécanismes de gouvernance interne conformément à l'article 74 de ladite directive. Dans ce contexte, toute norme harmonisée visée à l'article 40 du présent règlement est prise en compte.

Article 18
Obligation d'établir une documentation technique

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

2. Les prestataires qui sont des établissements de crédit régis par la directive 2013/36/UE conservent la documentation technique dans le cadre de la documentation concernant la gouvernance interne, les dispositions, les processus et les mécanismes conformément à 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 pertinente, conformément à l'article 43, avant leur mise sur le marché ou leur mise en service. Lorsque la conformité des systèmes d'IA aux exigences énoncées au chapitre 2 du présent titre a été démontrée à la suite de cette évaluation de la conformité, 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 IA à haut risque visés à l'annexe III, point 5 b), qui sont mis sur le marché ou mis en service par des prestataires qui sont des établissements de crédit réglementés 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 conservent les journaux générés automatiquement par leurs systèmes d'IA à haut risque, dans la mesure où ces journaux sont sous leur contrôle en vertu d'un accord contractuel avec l'utilisateur ou d'une autre disposition légale. Les journaux sont conservés pendant une période appropriée compte tenu de la finalité du système d'IA à haut risque et des obligations légales applicables en vertu du droit de l'Union ou du droit national.

2. Les prestataires qui sont des établissements de crédit régis par la directive 2013/36/UE conservent les journaux générés automatiquement par leurs systèmes d'IA à haut risque dans le cadre de la documentation prévue aux articles 74 de ladite directive.

Article 21
Actions 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 mettre ce système en conformité, le retirer ou le rappeler, selon le cas. Ils en informent les distributeurs du système d'IA à haut risque en question et, le cas échéant, le mandataire et les importateurs.

Article 22
Obligation 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, ce dernier 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, notamment de la non-conformité et des mesures correctives prises.

Article 23
Coopération avec les autorités compétentes

Les fournisseurs de systèmes d'IA à haut risque fournissent à une autorité nationale compétente, à la demande de celle-ci, toutes les informations et tous les documents nécessaires pour démontrer la conformité du système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent titre, dans une langue officielle de l'Union déterminée par l'État membre concerné. Sur demande motivée d'une autorité nationale compétente, les fournisseurs donnent également accès à cette autorité aux journaux générés automatiquement par le système d'IA à haut risque, dans la mesure où ces journaux sont sous leur contrôle en vertu d'un accord contractuel avec l'utilisateur ou d'une autre disposition légale.

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 avec le produit fabriqué conformément à ces actes juridiques et sous le nom du fabricant du produit, le fabricant du produit assume la responsabilité de la conformité du système d'IA au présent règlement et, en ce qui concerne le système d'IA, a les mêmes obligations que celles imposées par le présent règlement au fournisseur.

Article 25
Représentants autorisés

1. Avant de mettre leurs systèmes à disposition sur le marché de l'Union, lorsqu'un importateur ne peut être identifié, les fournisseurs établis en dehors de l'Union désignent, par mandat écrit, un mandataire qui est établi dans l'Union.

2. Le mandataire exécute les tâches spécifiées dans le mandat reçu du prestataire. Le mandat habilite le mandataire à effectuer les tâches suivantes :

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

(b) fournir à une autorité nationale compétente, sur demande motivée, toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent titre, y compris l'accès aux journaux générés automatiquement par le système d'IA à haut risque dans la mesure où ces journaux sont sous le contrôle du fournisseur en vertu d'un accord contractuel avec l'utilisateur ou d'une autre disposition légale ;

(c) coopérer avec les autorités nationales compétentes, sur demande motivée, pour toute mesure prise par ces dernières en relation avec le 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 doivent s'assurer que :

(a) la procédure d'évaluation de la conformité appropriée a été effectuée par le fournisseur de ce système d'IA

(b) le prestataire 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 des instructions 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 pas ce système sur le marché tant que ce système d'IA n'a pas été mis 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, leur nom commercial ou leur marque déposée, ainsi que l'adresse à laquelle ils peuvent être contactés sur le système AI à haut risque ou, lorsque cela n'est pas possible, sur l'emballage ou la documentation d'accompagnement, selon le cas.

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

5. Les importateurs fournissent aux autorités nationales compétentes, sur demande motivée, toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent titre, dans une langue aisément compréhensible par cette autorité nationale compétente, y compris l'accès aux journaux générés automatiquement par le système d'IA à haut risque dans la mesure où ces journaux sont sous le contrôle du fournisseur en vertu d'un accord contractuel avec l'utilisateur ou d'une autre disposition légale. Ils doivent également coopérer avec ces autorités pour 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 des instructions 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 pas le système d'IA à haut risque à disposition sur le marché tant que ce système n'a pas été mis en conformité avec ces exigences. En outre, 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, à cet effet.

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

4. Un distributeur qui 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 prend les mesures correctives nécessaires pour mettre ce système en conformité avec ces exigences, le retirer ou le rappeler ou s'assure que le fournisseur, l'importateur ou tout opérateur concerné, selon le cas, prend 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, en fournissant des précisions, notamment, sur la non-conformité et sur toute action corrective entreprise.

5. Sur demande motivée d'une autorité nationale compétente, les distributeurs de systèmes d'IA à haut risque fournissent à cette autorité toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système à haut risque aux exigences énoncées au chapitre 2 du présent titre. Les distributeurs coopèrent également avec cette autorité nationale compétente pour toute mesure prise par cette autorité.

Article 28
Obligations des distributeurs, importateurs, utilisateurs ou tout autre tiers

1. Tout distributeur, importateur, utilisateur ou autre tiers est considéré comme un prestataire aux fins du présent règlement et est soumis aux obligations du prestataire en vertu de l'article 16, dans l'une des circonstances suivantes :

   (a) ils mettent sur le marché ou mettent en service un système d'IA à haut risque sous leur nom ou leur marque ;

   (b) ils modifient la finalité d'un système d'IA à haut risque déjà mis sur le marché ou mis en service ;

   (c) ils apportent 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 prestataire qui a initialement mis sur le marché ou mis en service le système d'IA à

haut risque n'est plus considéré comme un prestataire 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 instructions d'utilisation qui accompagnent les systèmes, conformément aux paragraphes 2 et 5.

2. Les obligations visées au paragraphe 1 sont sans préjudice des autres obligations de l'utilisateur en vertu du droit de l'Union ou du droit national et de la liberté de l'utilisateur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de surveillance humaine indiquées par le fournisseur.

3. Sans préjudice du paragraphe 1, dans la mesure où l'utilisateur exerce un contrôle sur les données d'entrée, il veille à ce que celles-ci soient pertinentes au regard de l'objectif visé par le système d'IA à haut risque.

4. Les utilisateurs surveillent le fonctionnement du système d'IA à haut risque sur la base des instructions d'utilisation. Lorsqu'ils ont des raisons de considérer que l'utilisation conforme au mode d'emploi peut conduire à ce 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 ont identifié un incident grave ou un dysfonctionnement au sens de l'article 62 et interrompent l'utilisation du système d'IA. Si l'utilisateur ne parvient pas à joindre le fournisseur, l'article 62 s'applique mutatis mutandis.

   Pour les utilisateurs qui sont des établissements de crédit réglementés par la directive 2013/36/UE, l'obligation de surveillance énoncée au premier alinéa est réputée satisfaite par le respect des règles relatives aux dispositions, processus et mécanismes de gouvernance interne conformément à l'article 74 de ladite directive.

5. Les utilisateurs de systèmes d'IA à haut risque conservent les journaux générés automatiquement par ce système d'IA à haut risque, dans la mesure où ces journaux sont sous leur contrôle. Les journaux sont conservés pendant une période appropriée compte tenu de la finalité du système d'IA à haut risque et des obligations légales applicables en vertu du droit de l'Union ou du droit national.

   Les utilisateurs qui sont des établissements de crédit réglementés par la directive 2013/36/UE conservent les journaux dans le cadre de la documentation relative aux dispositions, processus et mécanismes de gouvernance interne conformément à l'article 74 de ladite directive.

6. Les utilisateurs de systèmes d'IA à haut risque utilisent les informations fournies en vertu de l'article 13 pour se conformer à leur obligation de procéder à une analyse d'impact sur 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

Article 30
Autorités notifiantes

1. Chaque État membre désigne ou établit une autorité notifiante chargée de mettre en place et d'exécuter 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 un organisme national d'accréditation visé par le règlement (CE) n° 765/2008 comme autorité notifiante.

3. Les autorités de notification sont établies, organisées et fonctionnent 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 manière à ce que les décisions relatives à la notification des organismes d'évaluation de la conformité soient prises par des personnes compétentes différentes de celles qui ont effectué l'évaluation de ces organismes.

5. Les autorités notifiantes ne doivent pas proposer ou fournir des activités que les organismes d'évaluation de la conformité exercent ou des services de conseil sur une base commerciale ou concurrentielle.

6. Les autorités notifiantes préservent la confidentialité des informations qu'elles obtiennent.

7. Les autorités de notification doivent disposer 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 conformité soient effectuées de manière proportionnée, en évitant d'imposer des charges inutiles aux prestataires, et à ce que les organismes notifiés exercent leurs activités en tenant dûment compte de la taille d'une entreprise, du secteur dans lequel elle opère, de sa 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 lesquels l'organisme d'évaluation de la conformité se déclare compétent, ainsi que d'un certificat d'accréditation, lorsqu'il existe, délivré par un organisme national d'accréditation attestant que l'organisme d'évaluation de la conformité satisfait aux exigences définies à l'article 33. Tout document valide relatif aux 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 concerné ne peut fournir un certificat d'accréditation, il fournit 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. Pour les organismes notifiés qui sont désignés en vertu de toute autre législation d'harmonisation de l'Union, tous les documents et certificats liés à ces désignations peuvent être utilisés pour soutenir leur procédure de désignation en vertu 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 définies à l'article 33.

2. Les autorités de notification notifient la Commission et les autres États membres en utilisant l'outil de notification électronique développé 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 exercer les activités d'un organisme notifié que si aucune objection n'est soulevée par la Commission ou les autres États membres dans un délai d'un mois à compter d'une notification.

5. Les autorités notifiantes informent la Commission et les autres États membres de toute modification ultérieure pertinente de 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 satisfont aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de processus qui sont nécessaires à l'accomplissement de leurs tâches.

3. La structure organisationnelle, la répartition des responsabilités, la structure hiérarchique et le fonctionnement des organismes notifiés sont tels qu'ils garantissent la confiance dans l'exécution et les résultats des activités d'évaluation de la conformité menées par les organismes notifiés.

4. Les organismes notifiés sont indépendants du fournisseur d'un système d'IA à haut risque pour lequel ils effectuent des 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 est évalué, ainsi que de tout concurrent du fournisseur.

5. Les organismes notifiés sont organisés et fonctionnent de manière à garantir l'indépendance, l'objectivité et l'impartialité de leurs activités. Les organismes notifiés documentent et mettent en œuvre une structure et des procédures visant à garantir l'impartialité et à promouvoir et appliquer les principes d'impartialité dans l'ensemble de leur organisation, de leur personnel et de leurs activités d'évaluation.

6. Les organismes notifiés disposent de procédures documentées garantissant 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 qui entrent en leur possession lors de l'exécution des activités d'évaluation de la conformité, sauf lorsque la divulgation est requise par la loi. Le personnel des organismes notifiés est tenu au secret professionnel pour toutes les informations obtenues dans l'exécution de leurs tâches au titre du présent règlement, sauf à l'égard des autorités notifiantes de l'État membre dans lequel leurs activités sont exercées.

7. Les organismes notifiés disposent de procédures pour l'exécution des activités qui tiennent dûment compte de la taille de l'entreprise, du secteur dans lequel elle opère, de sa structure, du degré de complexité du système d'IA en question.

8. Les organismes notifiés souscrivent une assurance responsabilité civile appropriée pour leurs activités d'évaluation de la conformité, sauf si la responsabilité est assumée par l'État membre concerné conformément au droit national ou si cet État membre est directement responsable de l'évaluation de la conformité.

9. Les organismes notifiés doivent être capables d'accomplir toutes les tâches qui leur

incombent en vertu du présent règlement avec la plus grande intégrité professionnelle et les compétences requises.

compétence dans le domaine spécifique, que ces tâches soient effectuées par les organismes notifiés eux-mêmes ou en leur nom et sous leur responsabilité.

10. Les organismes notifiés disposent de compétences internes suffisantes pour être en mesure d'évaluer efficacement les tâches effectuées par des parties externes en leur nom. À cette fin, à tout moment et pour chaque procédure d'évaluation de la conformité et chaque type de système d'IA à haut risque pour lesquels ils ont été désignés, l'organisme notifié dispose en permanence d'un personnel administratif, technique et scientifique suffisant qui possède une expérience et des connaissances relatives aux technologies d'intelligence artificielle, aux données et à l'informatique pertinentes, ainsi qu'aux exigences énoncées au chapitre 2 du présent titre.

11. Les organismes notifiés participent aux activités de coordination visées à l'article 38. Ils participent également directement ou sont représentés dans les organisations européennes de normalisation, ou veillent à être informés et à se tenir à jour en ce qui concerne les normes pertinentes.

12. Les organismes notifiés mettent à disposition et soumettent sur demande toute la documentation pertinente, y compris la documentation des fournisseurs, à l'autorité notifiante visée à l'article 30 pour lui permettre de mener ses activités d'évaluation, de désignation, de notification, de contrôle et de surveillance et pour faciliter l'évaluation décrite dans le présent chapitre.

Article 34
Filiales et sous-traitance des organismes notifiés

1. Lorsqu'un organisme notifié sous-traite des tâches spécifiques liées à l'évaluation de la conformité ou a recours à une filiale, il s'assure que le sous-traitant ou la filiale satisfait aux exigences définies à l'article 33 et en informe l'autorité notifiante.

2. Les organismes notifiés assument l'entière responsabilité des tâches effectuées par les sous-traitants ou les filiales, quel que soit le lieu où ils sont établis.

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

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 les travaux qu'ils ont effectués en vertu du présent règlement.

Article 35
Numéros d'identification et listes des organismes notifiés désignés en vertu du présent règlement

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

2. La Commission met à la disposition du public la liste des organismes notifiés au titre du présent règlement, y compris les numéros d'identification qui leur ont été attribués et les activités pour lesquelles ils ont été notifiés. La Commission veille à ce que la liste soit tenue à jour.

Article 36
Modifications des notifications

1. Lorsqu'une autorité notifiante a des soupçons ou a été informée qu'un organisme notifié ne répond plus aux exigences prévues à l'article 33, ou qu'il ne remplit pas ses obligations, cette autorité enquête sans délai avec la plus grande diligence. Dans ce contexte, elle informe l'organisme notifié concerné des objections soulevées et lui donne la possibilité de faire connaître son point de vue. Si l'autorité notifiante arrive à la conclusion que l'enquête menée par l'organisme notifié ne répond plus aux exigences énoncées à l'article 33 ou qu'il ne remplit pas ses obligations, elle restreint, suspend ou retire la notification, selon le cas, en fonction de la gravité du manquement. Il en informe aussi immédiatement la Commission et les autres États membres.

2. En cas de restriction, de suspension ou de retrait de la notification, ou lorsque l'organisme notifié a cessé son activité, l'autorité notifiante prend les mesures appropriées pour que les dossiers de cet organisme notifié soient soit repris par un autre organisme notifié, soit tenus à la disposition des autorités notifiantes responsables à leur demande.

Article 37
Contestation de la compétence des organismes notifiés

1. La Commission enquête, si nécessaire, sur tous les cas où il y a des raisons de douter qu'un organisme notifié respecte les exigences énoncées à l'article 33.

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

3. La Commission veille à ce que toutes les informations confidentielles obtenues au cours de ses enquêtes en vertu du présent article soient traitées de manière confidentielle.

4. Lorsque la Commission constate qu'un organisme notifié ne satisfait pas ou ne satisfait plus aux exigences prévues à l'article 33, elle adopte une décision motivée demandant à l'État membre notifiant de prendre les mesures correctives nécessaires, y compris le retrait de la notification si nécessaire. Cet acte d'exécution est adopté conformément à la procédure d'examen visée à l'article 74, paragraphe 2.

Article 38
Coordination des organismes notifiés

1. La Commission veille à ce que, en ce qui concerne les domaines couverts par le présent règlement, une coordination et une coopération appropriées entre les organismes notifiés actifs dans les procédures d'évaluation de la conformité des systèmes d'IA en vertu du présent règlement soient mises en place et fonctionnent correctement sous la forme 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 des pays tiers

Les organismes d'évaluation de la conformité établis en vertu du droit d'un pays tiers avec lequel l'Union a conclu un accord peuvent être autorisés à exercer les activités des organismes notifiés en vertu du présent règlement.

CHAPITRE 5

NORMES, ÉVALUATION DE LA CONFORMITÉ, CERTIFICATS, ENREGISTREMENT

Article 40
Normes harmonisées

Les systèmes d'IA à haut risque qui sont conformes à des normes harmonisées ou à des parties de celles-ci dont les références ont été publiées au Journal officiel de l'Union européenne sont présumés conformes aux exigences énoncées au chapitre 2 du présent titre, dans la mesure où ces normes couvrent ces exigences.

Article 41
Spécifications communes

1. Lorsque les normes harmonisées visées à l'article 40 n'existent pas ou lorsque la Commission estime que les normes harmonisées pertinentes sont insuffisantes ou qu'il est nécessaire de répondre à des préoccupations spécifiques 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. La Commission, lors de l'élaboration du cahier des charges commun visé au paragraphe 1, recueille l'avis des organismes ou groupes d'experts compétents établis en vertu du droit sectoriel de l'Union applicable.
3. Les systèmes d'IA à haut risque qui sont conformes aux spécifications communes visées au paragraphe 1 sont présumés être conformes aux exigences énoncées au chapitre 2 du présent titre, dans la mesure où ces spécifications communes couvrent ces exigences.
4. Lorsque les prestataires ne se conforment pas aux spécifications communes visées au paragraphe 1, ils justifient dûment qu'ils ont adopté des solutions techniques au moins équivalentes à celles-ci.

Article 42
Présomption de conformité à certaines exigences

1. Compte tenu de leur finalité, les systèmes d'IA à haut risque qui ont été formés et testés sur des données concernant le cadre 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 système de cybersécurité conformément au règlement (UE) 2019/881 du Parlement européen et du Conseil63 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 le certificat de cybersécurité ou la déclaration de conformité ou des parties de ceux-ci couvrent ces exigences.

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 aux 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, le fournisseur 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 aux exigences énoncées au chapitre 2 du présent titre, le prestataire 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 ne sont pas disponibles, le prestataire suit la procédure d'évaluation de la conformité définie 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 services répressifs, les services d'immigration ou d'asile ainsi que par 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, fait office d'organisme notifié.

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 2 à 8, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI, qui ne prévoit pas l'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 pertinente, comme l'exigent ces actes juridiques. Les exigences énoncées au chapitre 2 du présent titre s'appliquent à ces systèmes.

63 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification en matière de cybersécurité des technologies de l'information et des communications et abrogeant le règlement (UE) n° 526/2013 (loi

sur la cybersécurité) (JO L 151 du 7.6.2019, p. 1).

les systèmes d'IA à haut risque et font partie de cette évaluation. Les points 4.3, 4.4, 4.5 et le point 4.6, cinquième alinéa, de l'annexe VII 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 aux exigences énoncées au chapitre 2 du présent titre, à condition que la conformité de ces organismes notifiés aux exigences énoncées à l'article 33, paragraphes 4, 9 et 10, ait été évaluée dans le cadre de la procédure de notification prévue par ces actes juridiques.

Lorsque les actes juridiques énumérés à l'annexe II, section A, permettent au fabricant du produit de se soustraire à une évaluation de la conformité par une tierce partie, à condition que ce fabricant ait appliqué toutes les normes harmonisées couvrant toutes les exigences pertinentes, ce fabricant ne peut faire usage de cette option que s'il a également appliqué des normes harmonisées ou, le cas échéant, des 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 doivent faire l'objet d'une nouvelle procédure d'évaluation de la conformité chaque fois qu'ils sont substantiellement modifiés, que le système modifié soit destiné à être distribué ou qu'il continue à être utilisé par l'utilisateur actuel.

   Pour les systèmes d'IA à haut risque qui continuent d'apprendre après avoir été mis sur le marché ou mis en service, les changements apportés au système d'IA à haut risque et à ses performances qui ont été prédéterminés par le fournisseur au moment de l'évaluation initiale de la conformité et qui 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 afin d'introduire des éléments des procédures d'évaluation de la conformité qui deviennent nécessaires à la lumière du progrès technique.

6. La Commission est habilitée à adopter des actes délégués pour 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 la procédure d'évaluation de la conformité visée à l'annexe VII ou à des parties de celle-ci. 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 pour la santé et la sécurité et la protection des droits fondamentaux que présentent ces systèmes, ainsi que de la disponibilité de capacités et de ressources adéquates parmi les organismes notifiés.

Article 44
Certificats

1. Les certificats délivrés par les organismes notifiés conformément à l'annexe VII sont rédigés dans une langue officielle de l'Union déterminée par l'État membre dans lequel l'organisme notifié est établi ou dans une langue officielle de l'Union acceptée par l'organisme notifié.

2. Les certificats sont valables pour la période qu'ils indiquent, qui ne doit pas dépasser cinq ans. Sur demande du fournisseur, la validité d'un certificat peut être prolongée pour des périodes supplémentaires, chacune ne dépassant pas cinq ans, sur la base

d'une réévaluation conformément aux 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 prend en compte le principe de

proportionnalité, suspendre ou retirer le certificat délivré ou imposer toute restriction à celui-ci, à moins que le respect de ces exigences ne soit assuré par des mesures correctives appropriées prises par le fournisseur du système dans un délai approprié fixé 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 accessible aux parties ayant un intérêt légitime dans cette décision.

Article 46
Obligations d'information des organismes notifiés

1. Les organismes notifiés informent l'autorité notifiante des éléments suivants :

   (a) tout certificat d'évaluation de la documentation technique de l'Union, tout supplément à ces certificats, tout agrément de système de gestion de la qualité délivré conformément aux exigences de l'annexe VII ;

   (b) tout refus, restriction, suspension ou retrait d'un certificat d'évaluation de la documentation technique de l'Union ou d'un agrément de système de gestion de la qualité délivré conformément aux exigences de l'annexe VII ;

   (c) toute circonstance affectant la portée ou les conditions de la notification ;

   (d) toute demande d'information qu'ils ont 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 effectuées dans le cadre de leur notification et toute autre activité effectuée, y compris les activités transfrontalières et la sous-traitance.

2. Chaque organisme notifié informe les autres organismes notifiés :

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

   (b) des certificats d'évaluation de la documentation technique de l'UE ou de leurs suppléments qu'elle a refusés, retirés, suspendus ou soumis à d'autres restrictions, et, sur demande, des certificats et/ou de leurs suppléments qu'elle a délivrés.

3. Chaque organisme notifié fournit aux autres organismes notifiés exerçant des activités similaires d'évaluation de la conformité couvrant les mêmes technologies d'intelligence artificielle des informations pertinentes sur les questions relatives aux résultats négatifs et, sur demande, positifs de l'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 autoriser la mise sur le marché ou la mise en service de systèmes d'IA spécifiques à haut risque sur le territoire de l'État membre concerné, pour des raisons exceptionnelles de sécurité publique ou de protection de la vie et de la santé des personnes, de protection de l'environnement et de protection des actifs industriels et infrastructurels essentiels. Cette autorisation est accordée pour une durée limitée, le temps que les mesures de

conformité nécessaires soient prises.

les procédures d'évaluation sont en cours, et prend fin une fois ces procédures achevées. L'achèvement de ces procédures est entrepris sans retard excessif.

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 est conforme 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 en vertu du paragraphe 1.

3. Lorsque, dans les quinze jours civils suivant la réception des informations visées au paragraphe 2, aucune objection n'a été soulevée par un État membre ou la Commission à l'égard 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. Lorsque, dans les 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 lorsque la Commission considère que l'autorisation est contraire au droit de l'Union ou que la conclusion des États membres concernant la conformité du système visée au paragraphe 2 n'est pas fondée, la Commission entre sans délai en consultation avec l'État membre concerné ; le ou les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Au vu de ces éléments, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre concerné et à l'opérateur ou aux opérateurs concernés.

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

6. Par dérogation aux paragraphes 1 à 5, pour les systèmes IA à haut risque destinés à être utilisés comme composants de sécurité de dispositifs, ou qui sont eux-mêmes des dispositifs, couverts par le règlement (UE) 2017/745 et le règlement (UE) 2017/746, l'article 59 du règlement (UE) 2017/745 et l'article 54 du règlement (UE) 2017/746 s'appliquent également en ce qui concerne la dérogation à l'évaluation de la conformité aux exigences énoncées au chapitre 2 du présent titre.

Article 48
Déclaration de conformité de l'UE

1. Le fournisseur établit une déclaration écrite de conformité UE pour chaque système d'IA et la tient à la disposition des autorités nationales compétentes pendant 10 ans après la mise sur le marché ou la mise en service du système d'IA. La déclaration de conformité de l'UE doit identifier le système d'IA pour lequel elle a été établie. Une copie de la déclaration de conformité de l'UE est remise sur demande aux autorités compétentes nationales concernées.

2. La déclaration UE de conformité indique 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 figurant à l'annexe V et est traduite dans une ou plusieurs langues officielles de l'Union exigées par le ou les États membres dans lesquels le système d'IA à haut risque est mis à disposition.

3. Lorsque les systèmes d'IA à haut risque sont soumis à une autre législation d'harmonisation de l'Union qui exige également une déclaration de conformité de l'UE, une seule déclaration de conformité de l'UE est établie pour toutes les législations de l'Union applicables à l'IA.

système d'IA à haut risque. La déclaration contient toutes les informations nécessaires à l'identification de la législation d'harmonisation de l'Union à laquelle la déclaration se rapporte.

4. En établissant la déclaration UE de conformité, le prestataire assume la responsabilité du respect des exigences énoncées au chapitre 2 du présent titre. Le prestataire 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 aux fins de la mise à jour du contenu de la déclaration UE de conformité figurant à l'annexe V, afin d'introduire les éléments qui deviennent nécessaires à la lumière du progrès technique.

Article 49
Marquage de conformité CE

1. Le marquage CE est apposé de manière visible, lisible et indélébile pour les systèmes d'IA à haut risque. Lorsque cela n'est pas possible ou ne se justifie pas en raison de la nature du système d'IA à haut risque, il est apposé sur l'emballage ou sur la documentation d'accompagnement, selon le cas.

2. Le marquage CE visé au paragraphe 1 du présent article est soumis aux principes généraux énoncés à l'article 30 du règlement (CE) n° 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 définies à l'article 43. Le numéro d'identification est également indiqué dans tout matériel promotionnel qui mentionne que le système d'IA à haut risque satisfait aux exigences du marquage CE.

Article 50
Conservation des documents

Le fournisseur tient à la disposition des autorités nationales compétentes, pendant une période se terminant dix ans après la mise sur le marché ou la mise en service du système d'IA :

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

(b) la documentation relative au système de gestion de la qualité visée 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 de conformité de l'UE 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

LES OBLIGATIONS DE TRANSPARENCE POUR CERTAINS SYSTÈMES DE L'AI

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, à moins que cela ne soit évident d'après les circonstances et le contexte d'utilisation. Cette obligation ne s'applique pas aux systèmes d'IA autorisés par la loi à détecter, prévenir, enquêter et poursuivre des infractions pénales, sauf si ces systèmes sont mis à la disposition du public pour signaler une infraction pénale.

2. Les utilisateurs d'un système de reconnaissance des émotions ou d'un système de catégorisation biométrique doivent informer du fonctionnement du système les personnes physiques qui y sont exposées. Cette obligation ne s'applique pas aux systèmes d'IA utilisés pour la catégorisation biométrique, qui sont autorisés par la loi pour détecter, prévenir et enquêter sur des infractions pénales.

3. Les utilisateurs d'un système d'IA qui génère ou manipule un contenu image, audio ou vidéo ressemblant sensiblement à des personnes, des objets, des lieux ou d'autres entités ou événements existants et qui donnerait à une personne l'impression d'être authentique ou véridique ("deep fake"), doivent indiquer que le contenu a été généré ou manipulé artificiellement.

   Toutefois, le premier alinéa ne s'applique pas lorsque l'utilisation est autorisée par la loi pour la détection, la prévention, la recherche et la poursuite d'infractions pénales 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'affectent pas les exigences et obligations énoncées au titre III du présent règlement.

TITRE V

MESURES EN FAVEUR DE L'INNOVATION

Article 53
Bacs à sable réglementaires pour l'IA

1. Les bacs à sable réglementaires de l'IA établis par une ou plusieurs autorités compétentes des États membres ou par le Contrôleur européen de la protection des données fournissent un environnement contrôlé qui facilite le développement, l'essai et la validation de systèmes d'IA innovants pendant une période limitée avant leur mise sur le marché ou leur mise en service conformément à un plan spécifique. Cela se fait sous la supervision et l'orientation directes des autorités compétentes en vue d'assurer le respect des exigences du présent règlement et, le cas échéant, des autres législations de l'Union et des États membres supervisées 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 d'une autre manière de la compétence de surveillance d'autres autorités nationales ou autorités compétentes fournissant ou soutenant l'accès aux données,

les autorités nationales chargées de la protection des données et les autres autorités nationales sont associées au fonctionnement du bac à sable réglementaire de l'IA.

3. Les bacs à sable réglementaires de l'IA n'affectent pas les pouvoirs de surveillance et de correction des autorités compétentes. Tout risque significatif pour la santé, la sécurité et les droits fondamentaux identifié au cours du développement et de l'essai de ces systèmes entraîne une atténuation immédiate et, à défaut, la suspension du processus de développement et d'essai jusqu'à ce que cette atténuation ait lieu.

4. Les participants au bac à sable réglementaire de l'IA demeurent responsables, en vertu de la législation de l'Union et des États membres en matière de responsabilité, de tout préjudice infligé à des tiers à la suite 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 en matière d'IA coordonnent leurs activités et coopèrent dans le cadre du Conseil européen de l'intelligence artificielle. Elles soumettent au conseil 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 tirés et les recommandations sur leur mise en place et, le cas échéant, sur l'application du présent règlement et des autres textes législatifs de l'Union supervisés au sein du bac à sable.

6. Les modalités et les conditions de fonctionnement des bacs à sable réglementaires en matière d'IA, y compris les critères d'éligibilité et la procédure de candidature, 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 conformément à la procédure d'examen visée à l'article 74, paragraphe 2.

Article 54

Traitement ultérieur des données à caractère personnel pour le développement de certains systèmes d'IA dans l'intérêt public dans le bac à sable réglementaire de l'IA.

1. Dans le bac à sable réglementaire de l'IA, les données à caractère personnel légalement collectées à d'autres fins sont traitées aux fins de développer et de tester certains systèmes d'IA innovants dans le bac à sable dans les conditions suivantes :

   (a) les systèmes d'IA innovants sont développés pour sauvegarder un intérêt public substantiel dans un ou plusieurs des domaines suivants :

      (i) la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la protection contre les menaces à la sécurité publique et leur prévention, 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 au respect d'une ou plusieurs des exigences visées au titre III, chapitre 2, lorsque ces exigences ne peuvent pas être efficacement satisfaites par le traitement de données anonymes, synthétiques ou d'autres données non personnelles ;

(c) il existe des mécanismes de contrôle efficaces permettant de déterminer si des risques élevés pour les droits fondamentaux des personnes concernées peuvent survenir au cours de l'expérimentation du bac à sable, ainsi qu'un mécanisme de réponse permettant d'atténuer rapidement ces risques et, le cas échéant, d'arrêter le traitement ;

(d) toutes les données à caractère personnel à traiter dans le cadre du bac à sable se trouvent dans un environnement de traitement des données fonctionnellement distinct, isolé et protégé, sous le contrôle des participants, et seules les personnes autorisées ont accès à ces données ;

(e) les données personnelles traitées ne sont pas transmises, transférées ou autrement accessibles à d'autres parties ;

(f) tout traitement de données à caractère personnel dans le cadre du bac à sable n'entraîne pas de mesures ou de décisions affectant les personnes concernées ;

(g) toutes 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 pris fin ou que les données à caractère personnel ont atteint la fin de leur période de conservation ;

(h) les journaux du traitement des données à caractère personnel dans le cadre du bac à sable sont conservés pendant toute la durée de la participation au bac à sable et un an après sa fin, uniquement aux fins et aussi longtemps que nécessaire pour remplir les obligations en matière de responsabilité et de documentation en vertu du présent article ou d'une autre application de la législation de l'Union ou des États membres ;

(i) Une description complète et détaillée du processus et du raisonnement qui sous-tend la formation, les tests et la validation du système d'IA est conservée avec les résultats des tests dans la documentation technique de l'annexe IV ;

(j) un bref résumé du projet d'IA développé dans le bac à sable, de ses objectifs et des résultats attendus, 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 d'autres fins que celles explicitement mentionnées dans cette législation.

Article 55
Mesures pour les fournisseurs et les utilisateurs à petite échelle

1. Les États membres entreprennent les actions suivantes :

(a) fournir 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) organiser des activités spécifiques de sensibilisation à l'application du présent règlement, adaptées aux besoins des fournisseurs et des utilisateurs à petite échelle ;

(c) le cas échéant, établir un canal de communication spécifique avec les fournisseurs et utilisateurs à petite échelle et les autres innovateurs afin de fournir des conseils et de répondre aux questions concernant la mise en œuvre du présent règlement.

2. Les intérêts et les besoins spécifiques des petits prestataires sont pris en compte lors de la fixation des redevances pour l'évaluation de la conformité au titre de l'article 43,

en réduisant ces redevances proportionnellement à leur taille et à l'importance de leur marché.

CONSEIL EUROPÉEN DE L'INTELLIGENCE ARTIFICIELLE

Article 56
Création du Conseil européen de l'intelligence artificielle

1. Un "Conseil européen de l'intelligence artificielle" (le "Conseil") est créé.

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

   (a) contribuer à une coopération efficace des autorités nationales de surveillance et de la Commission en ce qui concerne les questions couvertes par le présent règlement ;

   (b) coordonner et contribuer aux orientations et analyses de la Commission, des autorités nationales de surveillance et des autres autorités compétentes sur les questions émergentes dans le marché intérieur en ce qui concerne les sujets couverts par le présent règlement ;

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

Article 57
Structure du conseil d'administration

1. Le conseil d'administration est composé des autorités de contrôle nationales, qui sont représentées par le chef ou un fonctionnaire de haut niveau équivalent de cette autorité, et du contrôleur européen de la protection des données. D'autres autorités nationales peuvent être invitées aux réunions, lorsque les questions abordées présentent un intérêt pour elles.

2. Le conseil d'administration adopte son règlement intérieur à la majorité simple de ses membres, après approbation de la Commission. Le règlement intérieur contient également les aspects opérationnels liés à l'exécution des tâches du conseil d'administration énumérées à l'article 58. Le conseil d'administration peut, le cas échéant, créer des sous-groupes chargés d'examiner des questions spécifiques.

3. Le conseil d'administration est présidé par la Commission. La Commission convoque les réunions et prépare l'ordre du jour, conformément aux tâches confiées au conseil d'administration en vertu du présent règlement et à son règlement intérieur. La Commission fournit un soutien administratif et analytique aux activités du conseil d'administration en application du présent règlement.

4. Le conseil peut inviter des experts externes et des observateurs à assister à ses réunions et peut procéder à 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 conseil et d'autres organes, organismes, agences et groupes consultatifs de l'Union.

Article 58
Tâches du Conseil

Lorsqu'il fournit des conseils et une assistance à la Commission dans le cadre de l'article 56, paragraphe 2, le conseil d'administration doit notamment

(a) recueillir et partager l'expertise et les meilleures pratiques entre les États membres ;

(b) contribuer à l'uniformisation des pratiques administratives dans les États membres, y compris pour le fonctionnement des bacs à sable réglementaires visés à l'article 53 ;

(c) émettre 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 concernant les 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 concernant la fixation des amendes administratives visées à l'article 71.

CHAPITRE 2

LES AUTORITÉS NATIONALES COMPÉTENTES

Article 59
Désignation des autorités nationales compétentes

1. Des autorités nationales compétentes sont établies ou désignées par chaque État membre afin 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 nationale de surveillance parmi les autorités nationales compétentes. L'autorité nationale de surveillance fait office d'autorité de notification et d'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 informent la Commission de leur(s) désignation(s) et, le cas échéant, des raisons pour lesquelles ils ont désigné plus d'une autorité.

4. Les États membres veillent à ce que les autorités nationales compétentes disposent de ressources financières et humaines suffisantes pour remplir les tâches qui leur incombent en vertu du présent règlement. En particulier, les autorités compétentes nationales disposent en permanence d'un nombre suffisant de personnel dont les compétences et l'expertise comprennent une compréhension approfondie des technologies d'intelligence artificielle, des données et de l'informatique, des droits fondamentaux, des risques pour la santé et la sécurité et une connaissance des normes et des exigences légales existantes.

5. Les États membres font rapport à la Commission sur une base annuelle sur l'état des ressources financières et humaines des autorités nationales compétentes, en évaluant leur adéquation. La Commission transmet ces informations au conseil d'administration pour discussion et recommandations éventuelles.

6. La Commission facilite l'échange 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 fournisseurs à petite échelle. Lorsque les autorités nationales compétentes ont l'intention de fournir des orientations et des conseils concernant un système d'IA dans des domaines couverts par une autre législation de l'Union, les autorités nationales compétentes en vertu de cette législation 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 pour leur contrôle.

TITRE VII

BASE DE DONNÉES DE L'UE POUR LES SYSTÈMES AUTONOMES À HAUT RISQUE DE L'AI

Article 60
Base de données de l'UE pour les systèmes autonomes d'IA à haut risque

1. La Commission, en collaboration avec les États membres, crée et gère une base de données de l'UE contenant les informations visées au paragraphe 2 concernant 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. La Commission leur apporte un soutien technique et administratif.

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 elles sont nécessaires à la collecte et au traitement des informations conformément au présent règlement. Ces informations comprennent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et qui ont l'autorité légale pour représenter le fournisseur.

5. La Commission est le contrôleur de la base de données de l'UE. Elle assure également aux fournisseurs un soutien technique et administratif adéquat.

TITRE VIII

SUIVI POST-MARCHÉ, PARTAGE D'INFORMATIONS, SURVEILLANCE DU MARCHÉ

CHAPITRE 1

SURVEILLANCE POST-COMMERCIALISATION

Article 61
Surveillance post-commercialisation par les fournisseurs et plan de surveillance post-commercialisation pour les systèmes d'IA à haut risque

1. Les fournisseurs établissent et documentent un système de surveillance post-

commercialisation d'une manière qui est proportionnée à la nature des technologies d'intelligence artificielle et aux risques du système d'IA à haut risque.

2. Le système de surveillance après commercialisation recueille, documente et analyse de manière active et systématique les données pertinentes fournies par les utilisateurs ou recueillies par d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur durée de vie, et permet au fournisseur d'évaluer la conformité continue des systèmes d'IA aux exigences énoncées au titre III, chapitre 2.

3. Le système de surveillance après commercialisation est fondé 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 couverts par les 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 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.

CHAPITRE 2

LE PARTAGE D'INFORMATIONS SUR LES INCIDENTS ET LES DYSFONCTIONNEMENTS

Article 62
Signalement des incidents graves et des dysfonctionnements

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union signalent tout incident grave ou tout dysfonctionnement de ces systèmes qui constitue une violation des obligations prévues par le droit de l'Union visant à protéger les droits fondamentaux aux autorités de surveillance du marché des États membres où cet incident ou cette violation s'est produit.

Cette notification est effectuée immédiatement après que le prestataire a établi un lien de causalité entre le système d'IA et l'incident ou le dysfonctionnement ou la probabilité raisonnable d'un tel lien, et, en tout état de cause, au plus tard 15 jours après que le prestataire a eu connaissance de l'incident grave ou du dysfonctionnement.

2. Lorsqu'elle reçoit une notification relative à une violation des obligations prévues par le droit de l'Union et destinées à protéger les droits fondamentaux, l'autorité de surveillance du marché en 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 douze 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 prestataires 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, couverts par le règlement (UE) 2017/745 et le règlement (UE) 2017/746, la notification des incidents graves ou des dysfonctionnements est limitée à ceux qui constituent une violation des obligations prévues par le droit de l'Union visant à protéger les droits fondamentaux.

CHAPITRE 3

APPLICATION

DE LA LOI

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 couverts par le présent règlement. Toutefois, aux fins de l'application effective du présent règlement :

   (a) toute référence à un opérateur économique au titre 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 relevant du règlement (UE) 2019/1020 s'entend comme incluant tous les systèmes d'IA entrant dans le champ d'application du présent règlement.

2. L'autorité nationale de surveillance fait régulièrement rapport à la Commission sur les résultats des activités pertinentes de surveillance du marché. L'autorité nationale de surveillance signale sans délai à la Commission et aux autorités nationales de la concurrence concernées toute information identifiée au cours 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, liés à des 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 désignées en vertu de ces actes juridiques.

4. Pour les systèmes d'IA mis sur le marché, mis en service ou utilisés par des institutions financières régies par la législation de l'Union sur les services financiers, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité compétente chargée de la surveillance financière de ces institutions en vertu de cette législation.

5. Pour les systèmes d'IA énumérés au point 1 a) dans la mesure où les systèmes sont utilisés à des fins répressives, les points 6 et 7 de l'annexe III, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités compétentes de contrôle de la protection des données en vertu de la directive (UE) 2016/680, ou du règlement 2016/679, soit les autorités nationales compétentes contrôlant les activités des services répressifs, d'immigration ou d'asile mettant en service ou utilisant 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 agit en tant qu'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 qui supervisent l'application de la législation d'harmonisation de l'Union énumérée à l'annexe II ou d'autres législations de l'Union qui pourraient 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. Accès aux données et à la documentation dans le cadre de leurs activités, les autorités de surveillance du marché se voient accorder un accès complet aux ensembles de données de formation, de validation et d'essai utilisés par le fournisseur, y compris par le biais d'interfaces de programmation d'applications ("API") ou d'autres moyens et outils techniques appropriés permettant 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 se voient accorder l'accès au code source du système d'IA.

3. Les autorités ou organismes publics nationaux qui surveillent ou font respecter les obligations découlant du droit de l'Union et protégeant les droits fondamentaux en rapport avec l'utilisation des systèmes d'IA à haut risque visés à l'annexe III sont habilités à demander et à consulter toute documentation créée ou conservée en vertu du présent règlement lorsque l'accès à cette documentation est nécessaire à l'exercice des compétences relevant de leur mandat dans les limites de leur juridiction. L'autorité ou l'organisme public compétent informe l'autorité de surveillance du marché de l'État membre concerné de toute demande de ce type.

4. Au plus tard trois 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 nationale de surveillance. Les États membres notifient cette liste à la Commission et à tous les autres États membres et la tiennent à jour.

5. Lorsque la documentation visée au paragraphe 3 est insuffisante pour déterminer si une violation des obligations découlant du droit de l'Union et visant à protéger les droits fondamentaux a eu lieu, l'autorité ou l'organisme public visé au paragraphe 3 peut demander de manière motivée à l'autorité de surveillance du marché d'organiser un test du système d'IA à haut risque par des moyens techniques. L'autorité de surveillance du marché organise le test en associant étroitement l'autorité ou l'organisme public demandeur dans un délai raisonnable suivant la demande.

6. Toute information et tout document obtenus par les autorités ou organismes publics nationaux visés au paragraphe 3 en application des dispositions du présent article sont traités dans le respect des obligations de confidentialité énoncées à l'article 70.

Article 65
Procédure de traitement des systèmes d'IA présentant un risque au niveau national

1. Les systèmes d'IA présentant un risque s'entendent comme un produit présentant un risque défini à l'article 3, point 19 du règlement (UE) 2019/1020 dans la mesure où il s'agit de risques pour la santé ou la sécurité ou pour 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 tel que visé au paragraphe 1, elle procède à une évaluation du système d'IA concerné en ce qui concerne sa conformité à toutes les exigences et obligations prévues par le présent règlement. Lorsque des risques pour la protection des droits fondamentaux sont présents, l'autorité de surveillance du marché informe également les autorités ou organismes publics nationaux compétents visés à l'article 64, paragraphe 3. Les opérateurs concernés

coopèrent, si nécessaire, avec l'autorité de surveillance du marché.

les autorités de surveillance 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 les obligations prévues par le présent règlement, elle demande sans délai à l'opérateur concerné de prendre toutes les mesures correctives appropriées pour mettre le système d'IA en conformité, de le retirer du marché ou de le rappeler dans un délai raisonnable, proportionné à la nature du risque, selon ce qu'elle peut prescrire.

L'autorité de surveillance du marché informe l'organisme notifié concerné en conséquence. L'article 18 du règlement (UE) 2019/1020 s'applique aux mesures visées au deuxième alinéa.

3. Lorsque l'autorité de surveillance du marché estime que la non-conformité ne se limite pas à son territoire national, elle informe la Commission et les autres États membres des résultats de l'évaluation et des mesures qu'elle a demandé à l'opérateur de prendre.

4. L'opérateur s'assure que toutes les mesures correctives appropriées sont prises à l'égard de tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché dans toute l'Union.

5. Lorsque l'exploitant d'un système d'IA ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2, l'autorité de surveillance du marché prend toutes les mesures provisoires appropriées pour interdire ou restreindre la mise à disposition du système d'IA sur son marché national, pour retirer le produit de ce marché ou pour le rappeler. Cette autorité informe sans délai la Commission et les autres États membres de ces mesures.

6. Les informations visées au paragraphe 5 comprennent tous les détails disponibles, notamment les données nécessaires à l'identification du système d'IA non conforme, l'origine du système d'IA, la nature de la non-conformité alléguée et le risque encouru, la nature et la durée des mesures nationales prises et les arguments avancés par l'opérateur concerné. En particulier, les autorités de surveillance du marché indiquent si la non-conformité est due à un ou plusieurs des éléments suivants :

   (a) un manquement du système d'IA aux exigences énoncées au titre III, chapitre 2 ;

   (b) les lacunes des normes harmonisées ou des 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 engagé la procédure informent sans délai la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent concernant la non-conformité du système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans un délai de trois mois à compter de la réception des informations visées au paragraphe 5, aucune objection n'a été soulevée par un État membre ou la Commission à l'égard d'une mesure provisoire prise par un État membre, cette mesure est réputée justifiée. Ceci 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 des mesures restrictives appropriées soient prises à l'égard du produit concerné, telles que le retrait du produit de leur marché, sans délai.

Article 66
Procédure de sauvegarde syndicale

1. Lorsque, dans un délai de trois mois à compter de la réception de la notification visée à l'article 65, paragraphe 5, des objections sont soulevées par un État membre à l'encontre d'une mesure prise par un autre État membre, ou lorsque la Commission considère que la mesure est contraire au droit de l'Union, la Commission entre sans délai en consultation avec l'État membre et le ou les opérateurs concernés et évalue la mesure nationale. Sur la base des résultats de cette évaluation, la Commission décide si la mesure nationale est justifiée ou non dans les 9 mois suivant la notification visée à l'article 65, paragraphe 5, et notifie cette décision à l'État membre concerné.

2. Si la mesure nationale est considérée comme justifiée, tous les États membres prennent les mesures nécessaires pour que le système d'IA non conforme soit retiré de leur marché et en informent la Commission. Si la mesure nationale est considérée comme injustifiée, l'État membre concerné retire la mesure.

3. Lorsque la mesure nationale est considérée comme justifiée et que la non-conformité du système d'IA est attribuée à des lacunes dans les normes harmonisées ou les spécifications communes visées aux articles 40 et 41 du présent règlement, la Commission applique la procédure prévue à l'article 11 du règlement (UE) n° 1025/2012.

Article 67
Systèmes d'IA conformes qui présentent un risque

1. Lorsque, après avoir effectué une évaluation au titre de l'article 65, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un système d'IA soit conforme au présent règlement, il présente un risque pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux ou pour d'autres aspects de la protection de l'intérêt public, il exige de l'opérateur concerné qu'il prenne toutes les mesures appropriées pour faire en sorte que le système d'IA concerné, lorsqu'il est mis sur le marché ou mis en service, ne présente plus ce risque, qu'il retire le système d'IA du marché ou qu'il le rappelle dans un délai raisonnable, proportionné à la nature du risque, qu'il peut prescrire.

2. Le fournisseur ou les autres opérateurs concernés veillent à ce que des mesures correctives soient prises à l'égard de 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 visé au paragraphe 1.

3. L'État membre informe immédiatement la Commission et les autres États membres. Ces informations comprennent tous les détails disponibles, en particulier les données nécessaires à l'identification du système d'IA concerné, l'origine et la chaîne d'approvisionnement du système d'IA, la nature du risque encouru ainsi que la nature et la durée des mesures nationales prises.

4. La Commission entame sans délai des consultations avec les États membres et l'opérateur concerné et évalue les mesures nationales prises. Sur la base

des résultats de cette évaluation, la Commission décide si la mesure est justifiée ou non et, le cas échéant, propose des mesures appropriées.

5. La Commission adresse 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 suivantes, elle demande au prestataire concerné de mettre fin 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 de conformité de l'UE n'a pas été établie ;

   (d) la déclaration de conformité de l'UE n'a pas été rédigée correctement ;

   (e) le numéro d'identification de l'organisme notifié, qui est impliqué dans la procédure d'évaluation de la conformité, le cas échéant, n'a pas été apposé ;

2. Si la non-conformité visée au paragraphe 1 persiste, l'État membre concerné prend toutes les mesures appropriées pour restreindre ou interdire la mise à disposition sur le marché du système d'IA à haut risque ou veiller à ce qu'il soit rappelé ou retiré du marché.

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 de solutions techniques qui constituent des moyens appropriés d'assurer le respect de ces exigences compte tenu de la finalité des systèmes.

2. La Commission et le Conseil 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 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, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de 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 des utilisateurs et de toute partie prenante intéressée et de leurs organisations représentatives. Les codes de conduite peuvent couvrir un ou plusieurs systèmes d'IA en tenant compte de la similitude de la finalité des systèmes concernés.

4. La Commission et le Conseil tiennent compte des intérêts et des besoins spécifiques des petits prestataires et des jeunes entreprises lorsqu'ils encouragent et facilitent l'élaboration de codes de conduite.

Article 70
Confidentialité

1. Les autorités compétentes nationales et les organismes notifiés participant à l'application du présent règlement respectent la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et de leurs activités de manière à protéger, notamment :

   (a) les droits de propriété intellectuelle, et les informations commerciales confidentielles ou les secrets commerciaux d'une personne physique ou morale, y compris le code source, à l'exception des cas visés à l'article 5 de la directive 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets commerciaux) contre leur acquisition, leur utilisation et leur divulgation illicites s'appliquent.

   (b) la mise en œuvre effective du présent règlement, notamment à des fins d'inspection, d'enquête ou d'audit ;(c) les intérêts publics et de sécurité nationale ;

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

2. Sans préjudice du paragraphe 1, les informations échangées sur une base confidentielle entre les autorités compétentes nationales et entre les autorités compétentes nationales et la Commission ne sont pas divulguées sans consultation préalable de l'autorité compétente nationale d'origine 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 services répressifs, les services d'immigration ou les services d'asile, lorsque cette divulgation mettrait en péril des intérêts publics et de sécurité nationale.

   Lorsque les services répressifs, les services d'immigration ou les services d'asile sont les fournisseurs des 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, accéder immédiatement à la documentation ou en obtenir une copie. Seul le personnel de l'autorité de surveillance du marché détenant le niveau d'habilitation de sécurité approprié est autorisé à accéder à cette documentation ou à en obtenir une copie.

3. Les paragraphes 1 et 2 n'affectent pas les droits et obligations de la Commission, des États membres et des organismes notifiés en matière d'échange d'informations et de diffusion des alertes, ni les obligations des parties concernées de fournir des informations 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 réglementaires de pays tiers avec lesquels ils ont conclu des accords de confidentialité bilatéraux ou multilatéraux garantissant un niveau de confidentialité adéquat.

Article 71
Pénalités

1. Dans le respect des conditions fixées par le présent règlement, les États membres déterminent le régime des sanctions, y compris les amendes administratives, applicables aux violations du présent règlement et prennent toutes les mesures nécessaires pour assurer leur mise en œuvre correcte et effective. Les sanctions prévues sont effectives, proportionnées et dissuasives. Elles tiennent compte en particulier des intérêts des petits prestataires et des entreprises en démarrage, ainsi que de leur viabilité économique.

2. Les États membres notifient à la Commission ces règles et ces mesures et lui communiquent, sans délai, toute modification ultérieure les concernant.

3. Les infractions suivantes sont passibles d'amendes administratives pouvant aller jusqu'à 30 000 000 EUR ou, si le contrevenant est une entreprise, jusqu'à 6 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

   (a) le non-respect de l'interdiction des pratiques d'intelligence artificielle visées à l'article 5 ;

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

4. Le non-respect par le système d'IA de toute exigence ou obligation prévue par le présent règlement, autre que celles prévues aux articles 5 et 10, est passible d'amendes administratives pouvant aller jusqu'à 20 000 000 EUR ou, si le contrevenant est une entreprise, jusqu'à
4 % de son chiffre d'affaires annuel mondial total pour l'exercice précédent, le chiffre le plus élevé étant retenu.

5. La fourniture d'informations incorrectes, incomplètes ou trompeuses aux organismes notifiés et aux autorités nationales compétentes en réponse à une demande est passible d'amendes administratives pouvant aller jusqu'à 10 000 000 EUR ou, si le contrevenant est une entreprise, jusqu'à 2 % de son chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

6. Pour décider du montant de l'amende administrative dans chaque cas individuel, toutes les circonstances pertinentes de la situation spécifique sont prises en compte 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) si des amendes administratives ont déjà été appliquées 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 fixe des règles sur la question de savoir si et dans quelle mesure des amendes administratives peuvent être imposées aux autorités et organismes publics établis dans cet État membre.

8. Selon le système juridique des États membres, le régime des amendes administratives peut être appliqué de telle sorte que les amendes soient imposées par les juridictions nationales compétentes ou par d'autres instances applicables dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

Article 72

Amendes administratives infligées 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 qui relèvent du champ d'application du présent règlement. Lorsqu'il décide d'imposer ou non une amende administrative et qu'il décide du montant de l'amende administrative dans chaque cas individuel, toutes les circonstances pertinentes de la situation spécifique sont prises en compte 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 avec le contrôleur européen de la protection des données en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs, y compris le respect de toute mesure précédemment ordonnée par le contrôleur européen de la protection des données à l'encontre de l'institution, de l'agence ou de l'organe de l'Union concerné par le même sujet ;

   (c) toute infraction antérieure similaire commise par l'institution, l'agence ou l'organe de l'Union ;

2. Les infractions suivantes sont passibles d'amendes administratives pouvant aller jusqu'à 500 000 EUR :

   (a) le non-respect de l'interdiction des pratiques d'intelligence artificielle visées à l'article 5 ;

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

3. Le non-respect par le système d'IA de toute exigence ou obligation prévue par le présent règlement, autre que celles prévues aux articles 5 et 10, est passible d'amendes administratives 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, l'agence ou l'organe de l'Union qui fait l'objet de la procédure menée par le contrôleur européen de la protection des données l'occasion d'être entendu sur la question de l'éventuelle violation. Le contrôleur européen de la protection des données ne fonde ses décisions que sur des éléments et des circonstances sur lesquels les parties concernées ont pu formuler des observations. Les plaignants, s'il y en a, sont associés étroitement à la procédure.

5. Les droits de la défense des parties concernées sont pleinement respectés dans la procédure. Elles ont le droit d'accéder au dossier du contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des particuliers ou des entreprises à ce que leurs données personnelles ou leurs secrets d'affaires soient protégés.

6. Les fonds collectés par l'imposition d'amendes dans le cadre du présent article constituent les recettes du budget général de l'Union.

TITRE XI

DÉLÉGATION DE POUVOIR ET PROCÉDURE DE DÉLÉGATION DE POUVOIR

Article 73

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués est conféré à la Commission dans les conditions prévues par le 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 compter de [l'*entrée en vigueur du 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 par le Conseil. Une décision de révocation met fin à la délégation de pouvoir précisée dans cette décision. Elle prend effet le jour suivant celui de sa publication au *Journal officiel de l'Union européenne* ou à une date ultérieure qui y est précisée. Elle n'affecte pas la validité des actes délégués déjà en vigueur.

4. Dès 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 aucune objection n'a été exprimée par le Parlement européen ou le Conseil 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 qu'ils ne s'y opposeront pas. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 74
Procédure du comité

1. La Commission est assistée par un comité. Ce comité est un comité au sens du règlement (UE) n° 182/2011.

2. Dans le cas où il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

Article 75
Modification du règlement (CE) n° 300/2008

À l'article 4, paragraphe 3, du règlement (CE) n° 300/2008, l'alinéa suivant est ajouté :

"Lors de l'adoption des mesures détaillées relatives aux spécifications techniques et aux procédures d'approbation et d'utilisation des équipements de sécurité concernant les systèmes d'intelligence artificielle au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, les exigences énoncées au chapitre 2, titre III, dudit règlement sont prises en compte."

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

Article 76
Modification du règlement (UE) n° 167/2013

À l'article 17, paragraphe 5, du règlement (UE) n° 167/2013, l'alinéa suivant est ajouté :

" Lors de l'adoption d'actes délégués en vertu du premier alinéa concernant des 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*, les exigences énoncées au titre III, chapitre 2, de ce règlement sont prises en compte.

_____

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

Article 77
Modification du règlement (UE) n° 168/2013

À l'article 22, paragraphe 5, du règlement (UE) n° 168/2013, l'alinéa suivant est ajouté :

" Lors de l'adoption d'actes délégués en vertu du premier alinéa concernant des 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*, les exigences énoncées au titre III, chapitre 2, de ce règlement sont prises en compte.

_____

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 en vertu du paragraphe 1 et d'actes d'exécution en vertu du paragraphe 11 concernant 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*, les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte.

_____

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 en vertu du paragraphe 3 concernant des 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 *, les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte.

_____

* 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 concernant 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*, les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte.

_____

* 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 concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle], les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte. "

(3) À l'article 43, l'alinéa suivant est ajouté :

" 4) Lors de l'adoption d'actes d'exécution conformément au paragraphe 1 concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle], les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte. "

(4) À l'article 47, l'alinéa suivant est ajouté :

“3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle], les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte. "

(5) À l'article 57, l'alinéa suivant est ajouté :

"Lors de l'adoption de ces actes d'exécution concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle], les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte."

(6) À l'article 58, l'alinéa suivant est ajouté :

“3. Lors de l'adoption d'actes délégués en vertu des paragraphes 1 et 2 concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle] , les exigences énoncées au titre III, chapitre 2, de ce règlement sont prises en compte.".

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 des actes d'exécution conformément au paragraphe 2, concernant 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*, les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte.

_____

* 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 TI 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 *[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 un changement significatif de la conception ou de la finalité du ou des systèmes d'IA concernés.

   Les exigences énoncées dans le présent règlement sont prises en compte, le cas échéant, dans l'évaluation de chaque système d'information à grande échelle établi par les actes juridiques énumérés à l'annexe IX, qui doit être effectuée comme prévu dans 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 partir de cette date, ces systèmes font l'objet de modifications importantes dans leur conception ou leur destination.

Article 84
Évaluation et révision

1. La Commission évalue la nécessité de modifier la liste de l'annexe III une fois par an après l'entrée en vigueur du présent règlement.

2. Au plus tard [*trois ans après la date d'application du présent règlement visée à l'article 85, paragraphe 2*] et ensuite tous les quatre ans, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement. Ces rapports sont rendus publics.

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

   (a) l'état des ressources financières et humaines des autorités nationales compétentes afin d'accomplir efficacement les tâches qui leur sont confiées en vertu du présent règlement ;

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

4. Dans les [*trois ans suivant 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 visant 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 Conseil, les États membres et les autorités nationales compétentes fournissent à la Commission des informations sur sa demande.

6. Dans le cadre des évaluations et des réexamens visés aux paragraphes 1 à 4, la Commission tient compte des positions et des conclusions du Conseil, du Parlement européen, du Conseil et d'autres organismes ou sources pertinents.

7. La Commission présente, si nécessaire, des propositions appropriées pour 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 s'applique à partir de [24 mois après l'entrée en vigueur du règlement].

3. Par dérogation au paragraphe 2 :

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

(b) L'article 71 est applicable à partir de [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,

Par le Parlement européenPar le Conseil
Le présidentLe président

ÉTAT FINANCIER LÉGISLATIF

1. CADRE CADRE DE LA PROPOSITION/INITIATIVE

1.1. Titre de la proposition/initiative

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

1.3. La proposition/initiative concerne :

1.4. Objectif(s)

1.4.1. Objectif(s) général(aux)

1.4.2. Objectif(s) spécifique(s)

1.4.3. Résultat(s) attendu(s) et impact

1.4.4. Indicateurs de performance

1.5. Motifs de la proposition/initiative

1.5.1. Exigence(s) à satisfaire à court ou à long terme, y compris un calendrier détaillé pour le déploiement de la mise en œuvre de l'initiative.

1.5.2. Valeur ajoutée de l'intervention de l'Union (elle peut résulter de différents facteurs, par exemple des gains de coordination, de la sécurité juridique, d'une plus grande efficacité ou de complémentarités). Aux fins du présent point, la "valeur ajoutée de l'intervention de l'Union" est la valeur résultant de l'intervention de l'Union qui s'ajoute à la valeur qui aurait été créée par les États membres seuls.

1.5.3. Les leçons tirées d'expériences similaires dans le passé

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

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

1.6. Durée et impact financier de la proposition/initiative

1.7. Mode(s) de gestion prévu(s)

2. MESURES DE GESTION

2.1. Règles de suivi et de rapport

2.2. Système de gestion et de contrôle

2.2.1. Justification du ou des modes de gestion, du ou des mécanismes de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposés.

2.2.2. Informations concernant les risques identifiés et 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 (ratio "coûts des contrôles ÷ valeur des fonds gérés"), et évaluation des niveaux attendus de risque d'erreur (au moment du paiement et de la clôture).

2.3. Mesures visant à prévenir la fraude et les irrégularités

3. ESTIMATION DE L'IMPACT FINANCIER DE LA PROPOSITION OU DE L'INITIATIVE

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

3.2. Estimation de l'incidence financière de la proposition sur les crédits

3.2.1. *Résumé de l'impact estimé sur les crédits opérationnels*

3.2.2. *Produit estimé financé par des crédits opérationnels*

3.2.3. *Résumé de l'impact estimé sur les crédits administratifs*

3.2.4. *Compatibilité avec le cadre financier pluriannuel actuel*

3.2.5. *Contributions de tiers*

3.3. Impact estimé sur les recettes

ÉTAT FINANCIER LÉGISLATIF

1. CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE CADRE DE LA PROPOSITION L'INITIATIVE DE LA PROPOSITION L'INITIATIVE

1.1. Titre de la proposition/initiative

Règlement du Parlement européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle (loi sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union

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

Réseaux de communication, contenu et technologie ;

Marché intérieur, industrie, entrepreneuriat et PME ;

L'impact budgétaire concerne les nouvelles tâches confiées à la Commission, y compris le soutien au Conseil de l'IA de l'UE ;

Activité : Façonner l'avenir numérique de l'Europe.

1.3. La proposition/initiative concerne :

X **une nouvelle action**

☐ **une nouvelle action faisant suite à un projet pilote/une action préparatoire64**

☐ **l'extension d'une action existante**

☐ **une action redirigée vers une nouvelle action**

1.4. Objectif(s)

1.4.1. Objectif(s) général(aux)

L'objectif général de l'intervention est d'assurer le bon fonctionnement du marché unique en créant les conditions nécessaires 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 n° 1

Fixer des exigences spécifiques aux systèmes d'IA et des obligations pour tous les acteurs de la chaîne de valeur afin de garantir que les systèmes d'IA mis sur le marché et utilisés sont sûrs et respectent la législation existante sur les droits fondamentaux et les valeurs de l'Union ;

Objectif spécifique n° 2

Garantir la sécurité juridique pour faciliter l'investissement et l'innovation dans l'IA en précisant les exigences essentielles, les obligations, ainsi que les procédures de conformité et de respect des règles qui doivent être suivies pour placer ou utiliser un système d'IA sur le marché de l'Union ;

Objectif spécifique n° 3

Renforcer la gouvernance et l'application effective de la législation existante en

64Comme visé à l'article 54, paragraphe 2, point a) ou b), du règlement financier.

les procédures de post-suivi et la répartition des tâches de gouvernance et de supervision entre les niveaux national et européen ;

Objectif spécifique n° 4

Faciliter le développement d'un marché unique pour les applications d'IA légales, sûres et dignes de confiance et prévenir la fragmentation du marché en prenant des mesures au niveau de l'UE pour fixer des exigences minimales pour que les systèmes d'IA puissent être placés et utilisés sur le marché de l'Union dans le respect de la législation existante sur les droits fondamentaux et la sécurité.

1.4.3. Résultat(s) attendu(s) et impact

Spécifiez les effets que la proposition/initiative devrait avoir sur les bénéficiaires/groupes ciblés.

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

Les utilisateurs d'IA devraient bénéficier de la certitude juridique que les systèmes d'IA à haut risque qu'ils achètent sont conformes aux lois et aux valeurs européennes.

Les consommateurs devraient en bénéficier en réduisant le risque de violation de leur

1.4.4. Indicateurs de performance

Précisez les indicateurs de suivi de la mise en œuvre de la proposition/initiative.

Indicateur 1

Nombre d'incidents graves ou de performances d'IA qui constituent un incident grave ou une violation des obligations en matière de droits fondamentaux (semestriel) par domaines d'application et calculé a) en termes absolus, b) en tant que part des applications déployées et c) en tant que part des citoyens concernés.

Indicateur 2

a) Investissement total en IA dans l'UE (annuel)

b) Investissement total en IA par État membre (annuel)

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

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

a) et b) seront calculés sur la base de sources officielles et comparés à des estimations privées.

c) et d) seront collectés par des enquêtes régulières de l'entreprise.

1.5. Motifs de la proposition/initiative

1.5.1. Exigence(s) à satisfaire à court ou à long terme, y compris un calendrier détaillé pour le déploiement de 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 devront avoir nommé les autorités existantes et/ou établi de nouvelles autorités exécutant les tâches définies dans la législation plus tôt, et le conseil européen de l'IA devra être mis en place et efficace. 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 de développer la base de données, de sorte que son développement soit

1.5.2. Valeur ajoutée de l'intervention de l'Union (elle peut résulter de différents facteurs, par exemple des gains de coordination, de la sécurité juridique, d'une plus grande efficacité ou de complémentarités). Aux fins du présent point, la "valeur ajoutée de l'intervention de l'Union" est la valeur résultant de l'intervention de l'Union qui s'ajoute à la valeur qui aurait été créée par les États membres seuls.

L'émergence d'un cadre disparate de règles nationales potentiellement divergentes entravera la fourniture continue de systèmes d'IA dans l'ensemble de l'UE et ne

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 dynamiser le marché intérieur et offre un grand potentiel pour donner à l'industrie européenne un avantage concurrentiel sur la scène mondiale et des économies d'échelle qui ne peuvent être réalisées par les États membres seuls.

1.5.3. Les leçons tirées d'expériences similaires dans le passé

La directive 2000/31/CE sur le commerce électronique fournit le cadre de base pour le fonctionnement du marché unique et la surveillance des services numériques et établit une structure de base pour un mécanisme général de coopération entre les États membres, couvrant en principe toutes les exigences applicables aux services numériques. L'évaluation de la directive a mis en évidence des lacunes dans plusieurs aspects de ce mécanisme de coopération, notamment 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 conduit au fil des ans à un manque de confiance entre les États membres pour répondre aux préoccupations concernant les fournisseurs offrant des services numériques transfrontaliers. L'évaluation de la directive a montré la nécessité de définir un ensemble différencié de règles et d'exigences au niveau européen. C'est pourquoi la mise en œuvre des obligations spécifiques prévues par le présent règlement nécessiterait un mécanisme de coopération spécifique au niveau de l'UE, avec une

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

Le règlement établissant des règles harmonisées en matière d'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 fourni par la législation existante. Pour cette raison, une nouvelle fonction de réglementation et de coordination nationale et européenne doit être établie avec cette proposition.

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

En outre, en augmentant la confiance dans l'IA et en encourageant ainsi les investissements dans le développement et l'adoption de l'IA, elle complète l'Europe numérique, pour laquelle la promotion de la diffusion de l'IA est l'une des cinq

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

Le personnel sera redéployé. Les autres coûts seront pris en charge par l'enveloppe DEP. étant donné que l'objectif de ce règlement - garantir une IA digne de confiance - contribue directement à un objectif clé de l'Europe numérique - accélérer le développement et le déploiement de l'IA en Europe.

1.6. Durée et impact financier de la proposition/initiative

☐ **durée limitée**

– en vigueur du [JJ/MM]AAAA au [JJ/MM]AAAA

– Incidence financière de YYYY à YYYY pour les crédits d'engagement et de YYYY à YYYY pour les crédits de paiement.

X **durée illimitée**

– Mise en œuvre avec une période de démarrage d'un/deux (tbc) ans,

– suivi d'un fonctionnement à pleine échelle.

1.7. Mode(s) de gestion prévu(s)65

X **Gestion directe** par la Commission

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

– par les agences exécutives

☐ **Gestion partagée** avec les États membres

☐ **Gestion indirecte** en confiant les tâches d'exécution du budget à :

– les pays tiers ou les organismes qu'ils ont désignés ;

– les organisations internationales et leurs agences (à préciser) ;

– la BEI et le Fonds européen d'investissement ;

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

– les organismes de droit public ;

– les organismes de droit privé chargés d'une mission de service public dans la mesure où ils offrent des garanties financières suffisantes ;

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

– les personnes chargées de la mise en œuvre des actions spécifiques de la PESC conformément au titre V du TUE, et identifiées dans l'acte de base correspondant.

– *Si plus d'un mode de gestion est indiqué, veuillez fournir des détails dans la section "Commentaires".*

Commentaires

65Les détails des modes de gestion et 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. Règles de suivi et de rapport

Précisez la fréquence et les conditions.

Le règlement sera réexaminé et évalué cinq ans après son entrée en vigueur. La Commission fera rapport sur les résultats de l'évaluation au Parlement européen, au Conseil et au Comité économique et social européen.

2.2. Système(s) de gestion et de contrôle

2.2.1. Justification du ou des modes de gestion, du ou des mécanismes de mise en œuvre du financement, des modalités de paiement et de la stratégie de contrôle proposés.

Le règlement établit une nouvelle politique en matière de règles harmonisées pour la fourniture de systèmes d'intelligence artificielle dans le marché intérieur tout en assurant le respect de la sécurité et des droits fondamentaux. Ces nouvelles règles exigent un mécanisme de cohérence pour l'application transfrontalière des obligations découlant de ce règlement, sous la forme d'un nouveau groupe consultatif coordonnant les activités des autorités nationales.

Afin de faire face à ces nouvelles tâches, il est nécessaire de doter les services de la Commission de ressources appropriées. On estime que l'application du nouveau règlement nécessitera 10 ETP à régime (5 ETP pour le soutien aux activités de la Commission et 5 ETP pour le Contrôleur européen de la protection des données agissant en tant qu'organe de notification des systèmes d'IA déployés par un organe de

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

Afin de garantir que les membres du conseil d'administration aient la possibilité d'effectuer des analyses en connaissance de cause sur la base d'éléments factuels, il est prévu que le conseil d'administration soit soutenu par la structure administrative de la Commission et qu'un groupe d'experts soit créé pour apporter une expertise

2.2.3. Estimation et justification du rapport coût-efficacité des contrôles (ratio "coûts des contrôles ÷ valeur des fonds gérés"), et évaluation des niveaux attendus de risque d'erreur (au moment du paiement et de la clôture).

Pour les dépenses de réunion, étant donné la faible valeur par transaction (par exemple, le remboursement des frais de voyage d'un délégué pour une réunion), les procédures de contrôle standard semblent suffisantes. En ce qui concerne le développement de la base de données, l'attribution des contrats fait l'objet d'un système de contrôle interne fort au sein de la DG CNECT grâce à des activités d'achat centralisées.

2.3. Mesures visant à prévenir la fraude et les irrégularités

Précisez les mesures de prévention et de protection existantes ou envisagées, par exemple celles de la stratégie anti-fraude.

Les mesures existantes de prévention de la fraude applicables à la Commission couvriront les crédits supplémentaires nécessaires pour le présent règlement.

3. ESTIMATION DE L'IMPACT FINANCIER DE LA PROPOSITION OU 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.

Intitulé du cadre financier pluriannuel	Ligne budgétaire	Type de dépenses	Contribution			
	Numéro	Diff./Non-diff. [66]	de l'AELE pays [67]	des pays candidats [68]	de pays tiers	au sens de l'article 21, paragraphe 2, point b), du règlement financier.
7	20 02 06 Dépenses administratives	Non-diff.	NON	NON	NON	NON
1	02 04 03 DEP Intelligence Artificielle	Diff.	OUI	NON	NON	NON
1	02 01 30 01 Dépenses d'appui au programme Digital Europe	Non-diff.	OUI	NON	NON	NON

3.2. Estimation de l'incidence financière de la proposition sur les crédits

3.2.1. Résumé de l'impact estimé sur les dépenses des crédits opérationnels

– La proposition/initiative ne nécessite pas l'utilisation de crédits opérationnels

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

Millions d'euros (à trois décimales près)

66 Diff. = Crédits dissociés / Non-diff. = Crédits non dissociés.

67 AELE : Association européenne de libre-échange.

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

Intitulé du cadre financier pluriannuel	1	

DG : CNECT				Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **202769**	**TOTAL**	
• Crédits opérationnels											
Ligne budgétaire70 02 04 03		Engagements	(1a)		1.000						**1.000**
		Paiements	(2a)		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 des programmes spécifiques71											
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**

69Indicatif et dépendant de la disponibilité du budget.

70Selon la nomenclature budgétaire officielle.

71 Assistance technique et/ou administrative et dépenses à l'appui de la mise en œuvre des programmes et/ou 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 pour les programmes spécifiques		(6)		**0.240**	**0.240**	**0.240**	**0.240**	**0.240**		**1.200**
TOTAL des crédits sous 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 plus d'une rubrique est concernée par la proposition / initiative, répétez la section ci-dessus :

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

Intitulé du cadre financier pluriannuel	7	Dépenses administratives

Cette section doit être remplie en utilisant les "données budgétaires de nature administrative" qui seront introduites en premier lieu dans l'annexeà la fichefinancière législative (annexe V du règlement intérieur), qui est téléchargée dans DECIDE à des fins de consultation interservices.

Millions d'euros (à trois décimales près)

		Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**Après 202772**	**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	**Appropriations**	**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	**Appropriations**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**0.760**	**3.800**
	(Total des engagements = Total des paiements)	1.530	1.530	1.530	1.530	1.530	1.530	**7.650**

Millions d'euros (à trois décimales près)

		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**

72Tous les chiffres de cette colonne sont indicatifs et soumis à la poursuite des programmes et à la disponibilité des crédits.

sous les TITRES 1 à 7 du cadre financier pluriannuel	Paiements		2.370	1.870	1.870	1.870	1.870	**9.850**

3.2.2. Produit estimé financé par des crédits opérationnels

Crédits d'engagement en millions d'euros (à trois décimales près)

Indiquer les objectifs et les résultats			Année **2022**		Année **2023**		Année **2024**		Année **2025**		Année **2026**		Année **2027**		Après **202773**		**TOTAL**	
	OUTPUTS																	
	Type	Coût moyen	No	Coût	No	Coût	No	Coût	No	Coût	No	Coût	No	Coût	No	Coût	Total No	Coût total
OBJECTIF SPÉCIFIQUE Non [174]...																		
Base de données					1	1.000	1		1		1		1		1	0.100	1	1.000
Réunions- Sortie					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 pour l'objectif spécifique n° 1																		
OBJECTIF SPÉCIFIQUE n° 2 ...																		
- Sortie																		
Sous-total pour l'objectif spécifique n° 2																		
TOTALS					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 de cette colonne sont indicatifs et soumis à la poursuite des programmes et à la disponibilité des crédits.

[74]Comme décrit au point 1.4.2. Objectif(s) spécifique(s)...".

3.2.3. Résumé de l'impact estimé sur les crédits administratifs

– La proposition/initiative ne nécessite pas l'utilisation de crédits de nature administrative

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

Millions d'euros (à trois décimales près)

	Année **2022**	Année **2023**	Année **2024**	Année **2025**	Année **2026**	Année **2027**	**Annuellement 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**
Total partiel RUBRIQUE 7 du cadre financier pluriannuel		1.530	1.530	1.530	1.530	1.530	**1.530**	**7.650**
Extérieur HEADING 776 **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**

Les crédits nécessaires pour les ressources humaines et les autres dépenses de nature administrative seront couverts par des crédits de la DG déjà affectés à la gestion de l'action et/ou ayant fait l'objet d'un redéploiement au sein de la DG, ainsi que, le cas échéant, par toute dotation supplémentaire qui pourrait être accordée à la DG gestionnaire dans le cadre de la procédure annuelle d'allocation et compte tenu des contraintes budgétaires.

75 Tous les chiffres de cette colonne sont indicatifs et soumis à la poursuite des programmes et à la disponibilité des crédits.

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

3.2.3.1. Estimation des besoins en ressources humaines

– La proposition/initiative ne nécessite pas l'utilisation de ressources humaines.

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

Estimation à exprimer en unités d'équivalent temps plein

.		Année **2023**	Année **2024**	Année **2025**	**2026**	**2027**	**Après 2027**[77]	
• **Postes du tableau des effectifs (fonctionnaires et agents temporaires)**								
20 01 02 01 (Siège et bureaux de représentation de la Commission)		10	10	10	10	10	10	
20 01 02 03 (Délégations)								
01 01 01 01 (Recherche indirecte)								
01 01 01 11 (Recherche directe)								
Autres lignes budgétaires (précisez)								
• **Personnel externe (en unité d'équivalent 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							
	- dans Délégations							
01 01 01 02 (AC, END, INT - Recherche indirecte)								
01 01 01 12 (AC, END, INT - Recherche directe)								
Autres lignes budgétaires (précisez)								
TOTAL		**10**	**10**	**10**	**10**	**10**	**10**	

XX est le domaine politique ou le titre budgétaire concerné.

Les ressources humaines nécessaires seront couvertes par le personnel de la DG déjà affecté à la gestion de l'action et/ou redéployé au sein de la DG, ainsi que, le cas échéant, par toute allocation supplémentaire qui pourrait être accordée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et compte tenu des contraintes budgétaires.

Le CEPD devrait fournir la moitié des ressources nécessaires.

Description des tâches à effectuer :

Fonctionnaires et agents temporaires	La préparation d'un total de 13 à 16 réunions, la rédaction de rapports, la poursuite du travail politique, par exemple en ce qui concerne les modifications futures de la liste des demandes d'IA à haut risque, et le maintien des relations avec les autorités des États membres nécessiteront quatre AD ETP et un AST ETP. Pour les systèmes d'IA développés par les institutions européennes, le Contrôleur européen de la protection des données est responsable. Sur la base de l'expérience passée, on peut estimer que 5 AD FTE sont nécessaires pour remplir les responsabilités du CEPD en vertu du projet de législation.

[77] Tous les chiffres de cette colonne sont indicatifs et soumis à la poursuite des programmes et à la disponibilité des crédits.

[78] AC = Personnel contractuel ; AL = Personnel local ; END = Expert national détaché ; INT = Personnel d'agence ; JPD = Les professionnels juniors dans les délégations.

[79] Sous-plafond pour le personnel externe couvert par des crédits opérationnels (anciennes lignes "BA").

Personnel externe	

3.2.4. Compatibilité avec le cadre financier pluriannuel actuel

La proposition/initiative :

– X peuvent être entièrement financés par redéploiement dans le cadre de la rubrique correspondante 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 l'utilisation des instruments spéciaux tels que définis dans le règlement CFP.

Expliquez ce qui est nécessaire, en précisant les rubriques et les lignes budgétaires concernées, les montants correspondants et les instruments qu'il est proposé d'utiliser.

– nécessite une révision du CFP.

Expliquez ce qui est nécessaire, en précisant les rubriques et les lignes budgétaires concernées et les montants correspondants.

3.2.5. Contributions de tiers

La proposition/initiative :

– X ne prévoit pas de cofinancement par des tiers

– prévoit le cofinancement par des tiers estimé ci-dessous :

Crédits en millions d'euros (à trois décimales près)

	Année **N80**	Année **N+1**	Année **N+2**	Année **N+3**	Indiquez autant d'années que nécessaire pour montrer la durée de l'impact (voir point 1.6).			Total
Précisez l'organisme de cofinancement								
TOTAL des crédits cofinancés								

80L 'année N est l'année de début de la mise en œuvre de la proposition/initiative. Veuillez remplacer "N" par la première année prévue de mise en œuvre (par exemple : 2021). Il en va de même pour les années suivantes.

3.3. Impact estimé sur les recettes

– La proposition/initiative a l'impact financier suivant :

– La proposition/initiative a l'impact financier suivant :

– sur les autres revenus

– sur les autres revenus

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

Millions d'euros (à trois décimales près)

Ligne de recettes du budget :	Crédits disponibles pour l'exercice en cours	Impact de la proposition/initiative81						
		Année **N**	Année **N+1**	Année **N+2**	Année **N+3**	Indiquez autant d'années que nécessaire pour montrer la durée de l'impact (voir point 1.6).		
Article								

Pour les recettes affectées, préciser la ou les lignes de dépenses budgétaires concernées.

Autres remarques (par exemple, méthode/formule utilisée pour calculer l'impact sur les recettes ou toute autre information).

81En ce qui concerne les ressources propres traditionnelles (droits de douane, cotisations sucre), les montants

indiqués doivent être des montants nets, c'est-à-dire des montants bruts après déduction de 20 % pour les frais de perception.