Journal officiel
de l'Union européenne

FR
Série L

2024/1689 12.7.2024

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

## du 13 juin 2024

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

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

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

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

vu la proposition de la Commission européenne,

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

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

vu l'avis de la Banque centrale européenne ([2]),

vu l'avis du Comité des régions ([3]),

statuant conformément à la procédure législative ordinaire ([4]),

considérant ce qui suit:

(1) L'objectif du présent règlement est d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme, en particulier pour le développement, la mise sur le marché, la mise en service et l'utilisation de systèmes d'intelligence artificielle (ci-après dénommés «systèmes d'IA») dans l'Union, dans le respect des valeurs de l'Union, de promouvoir l'adoption de l'intelligence artificielle (IA) axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte des droits fondamentaux de l'Union européenne (ci-après dénommée «Charte»), y compris la démocratie, l'état de droit et la protection de l'environnement, de protéger contre les effets néfastes des systèmes d'IA dans l'Union, et de soutenir l'innovation. Le présent règlement garantit la libre circulation transfrontière 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 de systèmes d'IA, sauf autorisation expresse du présent règlement.

(2) Le présent règlement devrait être appliqué dans le respect des valeurs de l'Union consacrées dans la Charte, en facilitant la protection des personnes physiques, des entreprises, de la démocratie, de l'état de droit et de l'environnement, tout en stimulant l'innovation et l'emploi et en faisant de l'Union un acteur de premier plan dans l'adoption d'une IA digne de confiance.

(3) Les systèmes d'IA peuvent être facilement déployés dans un large éventail de secteurs de l'économie et dans de nombreux pans de la société, y compris transfrontières, et peuvent facilement circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales destinées à faire en sorte que l'IA soit digne de confiance et sûre et à ce qu'elle soit développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Le fait que les règles nationales divergent peut entraîner une fragmentation du marché intérieur et peut réduire la sécurité juridique pour les opérateurs qui développent, importent ou utilisent des systèmes d'IA. Il convient donc de garantir un niveau de protection cohérent et élevé dans toute l'Union afin de parvenir à une IA digne de confiance, et d'éviter les divergences qui entravent la libre circulation, l'innovation, le déploiement et l'adoption des systèmes d'IA et des produits et services connexes au sein du marché intérieur, en établissant des obligations uniformes pour les opérateurs et en garantissant la protection uniforme des raisons impérieuses d'intérêt général et des droits des citoyens dans l'ensemble du marché intérieur sur la base de l'article 114 du traité sur le fonctionnement de l'Union européenne. Dans la mesure où le présent règlement contient des règles spécifiques sur la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel, à savoir des restrictions portant sur l'utilisation de systèmes d'IA pour l'identification biométrique à distance à des fins répressives, sur l'utilisation de systèmes d'IA pour l'évaluation des risques liés à des personnes physiques à des fins répressives, et sur l'utilisation de systèmes d'IA de catégorisation biométrique à des fins répressives, il convient de fonder le présent règlement, pour ce qui est de ces règles spécifiques, sur l'article 16 du traité sur le fonctionnement de l'Union européenne. Compte tenu de ces règles spécifiques et du recours à l'article 16 du traité sur le fonctionnement de l'Union européenne, il convient de consulter le comité européen de la protection des données.

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

(5) Cependant, en fonction des circonstances concernant son application et son utilisation et du niveau de développement technologique, l'IA peut générer des risques et porter atteinte aux intérêts publics et aux droits fondamentaux protégés par le droit de l'Union. Le préjudice causé peut être matériel ou immatériel, y compris physique, psychologique, sociétal ou économique.

(6) Compte tenu de l'incidence majeure que l'IA peut avoir sur nos sociétés et de la nécessité de bâtir la confiance, l'IA et son cadre réglementaire doivent impérativement être élaborés dans le respect des valeurs de l'Union consacrées à l'article 2 du traité sur l'Union européenne, des droits et libertés fondamentaux prévus par les traités, et, conformément à l'article 6 du traité

sur l'Union européenne, de la Charte. Il est indispensable que l'IA soit une technologie axée sur l'humain. Elle devrait servir d'outil aux personnes, dans le but ultime d'accroître le bien-être des humains.

(7) Afin d'assurer un niveau cohérent et élevé de protection des intérêts publics en ce qui concerne la santé, la sécurité et les droits fondamentaux, il convient d'établir des règles communes pour les systèmes d'IA à haut risque. Ces règles devraient être conformes à la Charte, non discriminatoires et compatibles avec les engagements commerciaux internationaux de l'Union. Elles devraient également tenir compte de la déclaration européenne sur les droits et principes numériques pour la décennie numérique et des lignes directrices en matière d'éthique pour une IA digne de confiance rédigées par le groupe d'experts de haut niveau sur l'intelligence artificielle (ci-après dénommé «GEHN IA»).

(8) Un cadre juridique de l'Union établissant des règles harmonisées sur l'IA est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'IA dans le marché intérieur, tout en garantissant un niveau élevé de protection des intérêts publics, comme la santé et la sécurité, et de protection des droits fondamentaux, y compris la démocratie, l'état de droit et la protection de l'environnement, tels qu'ils sont reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, des règles régissant la mise sur le marché, la mise en service et l'utilisation de certains systèmes d'IA devraient être établies, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation des marchandises et des services. Ces règles devraient être claires et solides pour protéger les droits fondamentaux, soutenir de nouvelles solutions innovantes, permettre la mise en place d'un écosystème européen d'acteurs publics et privés créant des systèmes d'IA conformes aux valeurs de l'Union, et libérer le potentiel de la transformation numérique dans l'ensemble des régions de l'Union. En établissant ces règles, ainsi que des mesures en faveur de l'innovation mettant un accent particulier sur les petites et moyennes entreprises (PME), parmi lesquelles les jeunes pousses, le présent règlement contribue à la réalisation de l'objectif qui consiste à promouvoir l'approche européenne de l'IA axée sur l'humain et faire de l'UE un acteur mondial de premier plan dans le développement d'une IA sûre, fiable et éthique, ainsi que l'avait formulé le Conseil européen ([5]), et il garantit la protection de principes éthiques expressément demandée par le Parlement européen ([6]).

(9) Des règles harmonisées applicables à la mise sur le marché, à la mise en service et à l'utilisation de systèmes d'IA à haut risque devraient être établies conformément au règlement (CE) nº 765/2008 du Parlement européen et du Conseil ([7]), à la décision nº 768/2008/CE du Parlement européen et du Conseil ([8]) et au règlement (UE) 2019/1020 du Parlement européen et du Conseil ([9]) (ci-après dénommé «nouveau cadre législatif»). Les règles harmonisées énoncées dans le présent règlement devraient s'appliquer dans tous les secteurs et, conformément au nouveau cadre législatif, être sans préjudice du droit de l'Union en vigueur, en particulier en ce qui concerne la protection des données, la protection des consommateurs, les droits fondamentaux, l'emploi et la protection des travailleurs, et la sécurité des produits, que le présent règlement vient compléter. En conséquence, tous les droits et recours prévus par ce droit de l'Union pour les consommateurs et les autres personnes sur lesquelles les systèmes d'IA sont susceptibles d'avoir des incidences négatives, y compris en ce qui concerne la réparation de dommages éventuels conformément à la directive 85/374/CEE du Conseil ([10]), demeurent inchangés et pleinement applicables. En outre, dans le contexte de

l'emploi et de la protection des travailleurs, le présent règlement ne devrait donc pas avoir d'incidence sur le droit de l'Union en matière de politique sociale ni sur le droit national du travail, dans le respect du droit de l'Union, en ce qui concerne les conditions d'emploi et de travail, y compris la santé et la sécurité au travail et les relations entre employeurs et travailleurs. Par ailleurs, le présent règlement ne devrait pas porter atteinte à l'exercice des droits fondamentaux reconnus dans les États membres et au niveau de l'Union, notamment le droit ou la liberté de faire grève ou d'entreprendre d'autres actions prévues par les mécanismes de concertation sociale propres aux États membres, ainsi que le droit de négocier, de conclure et d'appliquer des conventions collectives ou de mener des actions collectives conformément au droit national. Le présent règlement ne devrait pas avoir d'incidence sur les dispositions visant à améliorer les conditions de travail dans le cadre du travail via une plateforme, établies dans la directive du Parlement européen et du Conseil relative à l'amélioration des conditions de travail dans le cadre du travail via une plateforme. De plus, le présent règlement vise à renforcer l'efficacité de ces droits et recours existants en établissant des exigences et des obligations spécifiques, y compris en ce qui concerne la transparence, la documentation technique et la tenue de registres des systèmes d'IA. Par ailleurs, les obligations imposées aux différents opérateurs intervenant dans la chaîne de valeur de l'IA en vertu du présent règlement devraient s'appliquer sans préjudice du droit national, dans le respect du droit de l'Union, ayant pour effet de limiter l'utilisation de certains systèmes d'IA lorsque ces législations ne relèvent pas du champ d'application du présent règlement ou poursuivent des objectifs légitimes d'intérêt public autres que ceux poursuivis par le présent règlement. Ainsi, le droit national du travail et les lois sur la protection des mineurs, à savoir des personnes âgées de moins de 18 ans, compte tenu de l'observation générale n° 25 (2021) de la CNUDE sur les droits de l'enfant en relation avec l'environnement numérique, dans la mesure où ils ne sont pas spécifiques aux systèmes d'IA et poursuivent d'autres objectifs légitimes d'intérêt public, ne devraient pas être affectés par le présent règlement.

(10) Le droit fondamental à la protection des données à caractère personnel est garanti en particulier par les règlements (UE) 2016/679 ([11]) et (UE) 2018/1725 ([12]) du Parlement européen et du Conseil, ainsi que par la directive (UE) 2016/680 du Parlement européen et du Conseil ([13]). Par ailleurs, la directive 2002/58/CE du Parlement européen et du Conseil ([14]) protège la vie privée et la confidentialité des communications, y compris en prévoyant des conditions régissant le stockage de données à caractère personnel et non personnel dans des équipements terminaux ainsi que les conditions d'accès à ces données depuis ces équipements. Ces actes législatifs de l'Union servent de base à un traitement pérenne et responsable des données, y compris lorsque les ensembles de données contiennent un mélange de données à caractère personnel et de données à caractère non personnel. Le présent règlement n'entend pas modifier l'application du droit de l'Union régissant le traitement des données à caractère personnel, ni les tâches et les pouvoirs des autorités de contrôle indépendantes chargées de veiller au respect de ces ins truments. Il n'a pas non plus d'incidence sur les obligations des fournisseurs et des déployeurs de systèmes d'IA en leur qualité de responsables du traitement ou de sous-traitants découlant du droit de l'Union ou du droit national relatif à la protection des données à caractère personnel dans la mesure où la conception, le développement ou l'utilisation de systèmes d'IA implique le traitement de données à caractère personnel. Il convient également de préciser que les personnes concernées continuent de jouir de tous les droits et garanties qui leur sont conférés par le droit de l'Union, dont les droits liés à la prise de

décision individuelle entièrement automatisée, y compris le profilage. Des règles harmonisées concernant la mise sur le marché, la mise en service et l'utilisation des systèmes d'IA établies en vertu du présent règlement devraient faciliter la mise en œuvre effective des droits et autres voies de recours garantis par le droit de l'Union relatif à la protection des données à caractère personnel et d'autres droits fondamentaux, et permettre aux personnes concernées de faire valoir ces droits et autres voies de recours.

(11)Le présent règlement devrait être sans préjudice des dispositions relatives à la responsabilité des fournisseurs de services intermédiaires prévue dans le règlement (UE) 2022/2065 du Parlement européen et du Conseil ([15]).

(12)La notion de «système d'IA» figurant dans le présent règlement devrait être clairement définie et devrait être étroitement alignée sur les travaux des organisations internationales œuvrant dans le domaine de l'IA afin de garantir la sécurité juridique, et de faciliter la convergence internationale et une large acceptation, tout en offrant la souplesse nécessaire pour tenir compte des évolutions technologiques rapides dans ce domaine. En outre, la définition devrait être fondée sur les caractéristiques essentielles des systèmes d'IA qui la distinguent des systèmes logiciels ou des approches de programmation traditionnels plus simples, et ne devrait pas couvrir les systèmes fondés sur les règles définies uniquement par les personnes physiques pour exécuter automatiquement des opérations. Une caractéristique essentielle des systèmes d'IA est leur capacité d'inférence. Cette capacité d'inférence concerne le processus consistant à générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions, qui peuvent influencer l'environnement physique ou virtuel, et la capacité des systèmes d'IA à inférer des modèles ou des algorithmes, ou les deux, à partir d'entrées ou de données. Les techniques permettant l'inférence lors de la construction d'un système d'IA comprennent des approches d'apprentissage automatique qui apprennent à partir des données la manière d'atteindre certains objectifs, et des approches fondées sur la logique et les connaissances qui font des inférences à partir des connaissances encodées ou de la représentation symbolique de la tâche à résoudre. La capacité d'un système d'IA à faire des inférences va au-delà du traitement de données de base en ce qu'elle permet l'apprentissage, le raisonnement ou la modélisation. Le terme «fondé sur des machines» renvoie au fait que les systèmes d'IA tournent sur des machines. La référence à des objectifs explicites ou implicites souligne que les systèmes d'IA peuvent fonctionner selon des objectifs explicites définis ou des objectifs implicites. Les objectifs du système d'IA peuvent être différents de la destination du système d'IA dans un contexte spécifique. Aux fins du présent règlement, les environnements devraient s'entendre comme étant les contextes dans lesquels les systèmes d'IA fonctionnent, tandis que les sorties générées par le système d'IA correspondent à différentes fonctions exécutées par les systèmes d'IA et consistent en des prévisions, du contenu, des recommandations ou des décisions. Les systèmes d'IA sont conçus pour fonctionner à différents niveaux d'autonomie, ce qui signifie qu'ils bénéficient d'un certain degré d'indépendance dans leur action par rapport à une ingérence humaine et de capacités à fonctionner sans intervention humaine. La faculté d'adaptation dont un système d'IA pourrait faire preuve après son déploiement est liée à des capacités d'auto-apprentissage, qui permettent au système d'évoluer en cours d'utilisation. Les systèmes d'IA peuvent être utilisés seuls ou en tant que composant d'un produit, que le système soit physiquement incorporé dans le produit (intégré) ou qu'il serve la fonctionnalité du produit sans y être incorporé (non intégré).

(13)Il convient d'interpréter la notion de «déployeur» visée dans le présent règlement comme désignant toute personne physique ou morale, y compris une autorité publique, une agence ou un autre organisme, utilisant sous sa propre autorité un système d'IA, sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel. En fonction du type de système d'IA, l'utilisation du système peut concerner des personnes autres que le déployeur.

(14)Il convient d'interpréter la notion de «données biométriques» utilisée dans le présent règlement à la lumière de la notion de données biométriques au sens de l'article 4, point 14), du règlement (UE) 2016/679, de l'article 3, point 18), du règlement (UE) 2018/1725, et de l'article 3, point 13), de la directive (UE) 2016/680. Des données biométriques peuvent permettre l'authentification, l'identification ou la catégorisation des personnes physiques, ainsi que la reconnaissance de leurs émotions.

(15)La notion d'«identification biométrique» visée dans le présent règlement devrait être définie comme la reconnaissance automatisée de caractéristiques physiques, physiologiques et comportementales d'une personne, telles que le visage, les mouvements oculaires, la forme du corps, la voix, la prosodie, la démarche, la posture, le rythme cardiaque, la pression sanguine, l'odeur et la frappe au clavier, aux fins d'établir l'identité d'une personne par comparaison des données biométriques de cette personne avec les données biométriques de personnes stockées dans une base de données de référence, que la personne ait donné son approbation ou non. En sont exclus les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, ce qui inclut l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux.

(16)La notion de «catégorisation biométrique» visée dans le présent règlement devrait être définie comme le classement de personnes physiques dans certaines catégories sur la base de leurs données biométriques. Ces catégories spécifiques peuvent concerner des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits liés au comportement ou à la personnalité, la langue, la religion, l'appartenance à une minorité nationale ou encore l'orientation sexuelle ou politique. Cela n'inclut pas les systèmes de catégorisation biométrique qui sont une caractéristique purement accessoire intrinsèquement liée à un autre service commercial, ce qui signifie que cette caractéristique ne peut, pour des raisons techniques objectives, être utilisée sans le service principal, et l'intégration de cette caractéristique ou fonctionnalité n'est pas un moyen de contourner l'applicabilité des règles du présent règlement. Ainsi, les filtres de catégorisation des caractéristiques faciales ou corporelles qui sont utilisés sur les places de marché en ligne pourraient correspondre à ce type de caractéristique accessoire, étant donné qu'ils ne peuvent être utilisés qu'en lien avec le service principal, qui consiste à vendre un produit en permettant au consommateur d'afficher un aperçu du produit porté par lui-même et de l'aider à prendre une décision d'achat. Les filtres utilisés sur les services de réseaux sociaux en ligne qui classent par catégorie les caractéristiques faciales ou corporelles afin de permettre aux utilisateurs d'ajouter ou de modifier des images ou des vidéos pourraient également être considérés comme des fonctionnalités accessoires, étant donné que ce type de filtre ne peut pas être utilisé sans le service principal des services de réseau social consistant à partager des contenus en ligne.

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

(18)La notion de «système de reconnaissance des émotions» visée dans le présent règlement devrait être définie comme un système d'IA servant à identifier les émotions ou les intentions de personnes physiques ou à faire des déductions quant à leurs émotions ou intentions, sur la base de leurs données biométriques. Cette notion renvoie à des émotions ou des intentions telles que le bonheur, la tristesse, la colère, la surprise, le dégoût, la gêne, l'excitation, la honte, le mépris, la satisfaction et l'amusement. Cette notion ne recouvre pas les états physiques, tels que la douleur ou la fatigue, qui comprennent, par exemple, des systèmes utilisés pour déceler l'état de fatigue des pilotes ou des conducteurs professionnels aux fins de la prévention des accidents. Elle ne recouvre pas non plus la simple détection d'expressions, de gestes ou de mouvements dont l'apparence est immédiate, à moins que ceux-ci ne soient utilisés pour identifier ou déduire des émotions. Ces expressions peuvent être des expressions faciales toutes simples telles qu'un froncement de sourcils ou un sourire, ou des gestes tels qu'un mouvement de mains, de bras ou de tête, ou encore des caractéristiques de la voix d'une personne, comme le fait de parler fort ou de chuchoter.

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

(20)Afin de tirer le meilleur parti des systèmes d'IA tout en protégeant les droits fondamentaux, la santé et la sécurité et de permettre un contrôle démocratique, il convient que les fournisseurs, les déployeurs et les personnes concernées acquièrent, dans le cadre de la maîtrise de l'IA, les notions nécessaires pour prendre des décisions éclairées concernant les systèmes d'IA. Ces notions peuvent varier en fonction du contexte et peuvent recouvrir le faire de comprendre l'application correcte des éléments techniques au cours de la phase de développement du système d'IA, les mesures à appliquer pendant son utilisation, les moyens appropriés d'interpréter les sorties du système d'IA et, dans le cas des personnes concernées, les connaissances nécessaires pour comprendre comment les décisions prises avec l'aide de l'IA auront une incidence sur elles. Dans le cadre de l'application du présent règlement, la maîtrise de l'IA devrait fournir à tous les acteurs pertinents de la chaîne de valeur de l'IA les connaissances nécessaires pour en garantir le respect approprié et la mise en application correcte. En outre, la mise en œuvre à grande échelle de mesures relatives à la maîtrise de l'IA et l'introduction d'actions de suivi appropriées pourraient contribuer à améliorer les conditions de travail et, à terme, soutenir la consolidation et une trajectoire d'innovation d'une IA digne

de confiance dans l'Union. Le Comité européen de l'intelligence artificielle (ci-après dénommé «Comité IA») devrait soutenir la Commission afin de promouvoir les outils de maîtrise de l'IA, la sensibilisation du public et la compréhension des avantages, des risques, des garanties, des droits et des obligations liés à l'utilisation des systèmes d'IA. En coopération avec les parties prenantes concernées, la Commission et les États membres devraient faciliter l'élaboration de codes de conduite volontaires au service de la maîtrise de l'IA chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA.

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

(22) Compte tenu de leur nature numérique, certains systèmes d'IA devraient relever du présent règlement même lorsqu'ils ne sont pas mis sur le marché, mis en service, ou utilisés dans l'Union. Cela devrait notamment être le cas lorsqu'un opérateur établi dans l'Union confie à un opérateur externe établi dans un pays tiers la tâche d'exécuter certains services ayant trait à une activité devant être réalisée par un système d'IA qui serait considéré comme étant à haut risque. Dans ces circonstances, le système d'IA utilisé dans un pays tiers par l'opérateur pourrait traiter des données légalement collectées et transférées depuis l'Union, et fournir à l'opérateur contractant établi dans l'Union les sorties dudit système d'IA provenant de ce traitement, sans que ce système d'IA soit mis sur le marché, mis en service ou utilisé dans l'Union. Afin d'éviter le contournement des règles du présent règlement et d'assurer une protection efficace des personnes physiques situées dans l'Union, le présent règlement devrait également s'appliquer aux fournisseurs et aux déployeurs de systèmes d'IA qui sont établis dans un pays tiers, dans la mesure les sorties produites par ces systèmes sont destinées à être utilisées dans l'Union. Néanmoins, pour tenir compte des dispositions existantes et des besoins particuliers de coopération future avec les partenaires étrangers avec lesquels des informations et des preuves sont échangées, le présent règlement ne devrait pas s'appliquer aux autorités publiques d'un pays tiers ni aux organisations internationales lorsqu'elles agissent dans le cadre d'accords de coopération ou d'accords internationaux conclus au niveau de l'Union ou au niveau national pour la coopération des services répressifs et judiciaires avec l'Union ou avec les États membres, à condition que le pays tiers concerné ou les organisations internationales concernées fournissent des garanties adéquates en ce qui concerne la protection des libertés et droits fondamentaux des personnes. Le cas échéant, cela peut couvrir les activités des entités chargées par les pays tiers d'exécuter des tâches spécifiques à l'appui de cette coopération policière et judiciaire. De tels cadres de coopération ou 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'Union, des pays tiers et des organisations internationales. Les autorités compétentes pour la surveillance des autorités répressives et judiciaires au titre du présent règlement devraient évaluer si ces cadres de coopération ou accords internationaux comportent des garanties adéquates en ce qui concerne la protection des libertés et droits fondamentaux des personnes. Les autorités nationales bénéficiaires et les institutions, organes et organismes de l'Union qui utilisent ces sorties dans l'Union demeurent responsables de veiller à ce que leur utilisation soit conforme au droit de l'Union. Lors de la révision de ces

accords internationaux ou de la conclusion de nouveaux accords à l'avenir, les parties contractantes devraient tout mettre en œuvre pour aligner ces accords sur les exigences du présent règlement.

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

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

(25) Le présent règlement devrait soutenir l'innovation et respecter la liberté scientifique et ne devrait pas compromettre les activités de recherche et de développement. Il est donc nécessaire d'exclure de son champ d'application les systèmes et modèles d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques. En outre, il est nécessaire de veiller à ce que le présent règlement n'affecte pas autrement les activités de

recherche et de développement scientifiques relatives aux systèmes ou modèles d'IA avant leur mise sur le marché ou leur mise en service. En ce qui concerne les activités de recherche, d'essai et de développement axées sur les produits, relatives aux systèmes ou modèles d'IA, les dispositions du présent règlement ne devraient pas non plus s'appliquer avant la mise en service ou la mise sur le marché de ces systèmes et modèles. Cette exclusion est sans préjudice de l'obligation de se conformer au présent règlement lorsqu'un système d'IA relevant du champ d'application du présent règlement est mis sur le marché ou mis en service à la suite de cette activité de recherche et de développement, et sans préjudice de l'application des dispositions relatives aux bacs à sable réglementaires de l'IA et aux essais en conditions réelles. En outre, sans préjudice de l'exclusion des systèmes d'IA spécifiquement développés et mis en service aux seules fins de la recherche et du développement scientifiques, tout autre système d'IA susceptible d'être utilisé pour mener une activité de recherche et de développement devrait rester soumis aux dispositions du présent règlement. En tout état de cause, toute activité de recherche et de développement devrait être menée conformément à des normes éthiques et professionnelles reconnues en matière de recherche scientifique et dans le respect du droit de l'Union applicable.

(26) 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 inacceptables en matière d'IA, de fixer des exigences pour les systèmes d'IA à haut risque et des obligations pour les opérateurs concernés, ainsi que de fixer des obligations de transparence pour certains systèmes d'IA.

(27) Si l'approche fondée sur les risques constitue la base d'un ensemble proportionné et efficace de règles contraignantes, il importe de rappeler les lignes directrices en matière d'éthique pour une IA digne de confiance, élaborées en 2019 par le GEHN IA indépendant constitué par la Commission. Dans ces lignes directrices, le GEHN IA a élaboré sept principes éthiques non contraignants pour l'IA, qui sont destinés à contribuer à faire en sorte que l'IA soit digne de confiance et saine sur le plan éthique. Il s'agit des sept principes suivants: action humaine et contrôle humain; robustesse technique et sécurité; respect de la vie privée et gouvernance des données; transparence; diversité, non-discrimination et équité; bien-être sociétal et environnemental; et responsabilité. Sans préjudice des exigences juridiquement contraignantes du présent règlement et de toute autre disposition législative de l'Union applicable, ces lignes directrices contribuent à la conception d'une IA cohérente, fiable et axée sur l'humain, conformément à la Charte et aux valeurs sur lesquelles l'Union est fondée. Conformément aux lignes directrices du GEHN IA, «action humaine et contrôle humain» renvoient au fait que les systèmes d'IA sont développés et utilisés comme un outil au service des personnes, qui respecte la dignité humaine et l'autonomie de l'individu, et qui fonctionne de manière à pouvoir être contrôlé et supervisé par des êtres humains.«Robustesse technique et sécurité» renvoient au fait que les systèmes d'IA sont développés et utilisés de manière à ce qu'ils soient techniquement robustes en cas de problème et résilients aux tentatives visant à en corrompre l'utilisation ou les performances afin de permettre à des tiers d'en faire une utilisation abusive, et à réduire le plus possible les atteintes involontaires. «Respect de la vie privée et gouvernance des données» renvoient au fait que les systèmes d'IA sont développés et utilisés conformément aux règles en matière de respect de la vie privée et de protection des données,

dans le cadre d'un traitement de données répondant à des normes élevées en matière de qualité et d'intégrité. «Transparence» renvoie au fait que les systèmes d'IA sont développés et utilisés de manière à permettre une traçabilité et une explicabilité appropriées, faisant en sorte que les personnes réalisent qu'elles communiquent ou interagissent avec un système d'IA, que les déployeurs soient dûment informés des capacités et des limites de ce système d'IA et que les personnes concernées soient informées de leurs droits. «Diversité, non-discrimination et équité» renvoient au fait que les systèmes d'IA sont développés et utilisés de manière à inclure des acteurs divers et à promouvoir l'égalité d'accès, l'égalité de genre et la diversité culturelle, tout en évitant les effets discriminatoires et les biais injustes, qui sont interdits par le droit de l'Union ou le droit national. «Bien-être sociétal et environnemental» renvoie au fait que les systèmes d'IA sont développés et utilisés d'une manière durable et respectueuse de l'environnement, mais aussi de manière à ce que tous les êtres humains en profitent, tout en surveillant et en évaluant les effets à long terme sur l'individu, la société et la démocratie. Ces principes devraient se retrouver, autant que possible, dans la conception et l'utilisation des modèles d'IA. Ils devraient en tout état de cause servir de base à l'élaboration de codes de conduite au titre du présent règlement. Toutes les parties prenantes, y compris l'industrie, le monde universitaire, la société civile et les organismes de normalisation, sont encouragées à tenir compte, ainsi qu'il convient, des principes éthiques pour l'élaboration de bonnes pratiques et de normes volontaires.

(28) Si l'IA peut être utilisée à de nombreuses fins positives, elle peut aussi être utilisée à mauvais escient et fournir des outils nouveaux et puissants à l'appui de pratiques de manipulation, d'exploitation et de contrôle social. De telles pratiques sont particulièrement néfastes et abusives et devraient être interdites, car elles sont contraires aux valeurs de l'Union relatives au respect de la dignité humaine, à la liberté, à l'égalité, à la démocratie et à l'état de droit, ainsi qu'aux droits fondamentaux consacrés dans la Charte, y compris le droit à la non-discrimination, le droit à la protection des données et à la vie privée et les droits de l'enfant.

(29) Des techniques de manipulation fondées sur l'IA peuvent être utilisées pour persuader des personnes d'adopter des comportements indésirables ou pour les tromper en les poussant à prendre des décisions d'une manière qui met à mal et compromet leur autonomie, leur libre arbitre et leur liberté de choix. La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA ayant pour objectif ou pour effet d'altérer substantiellement les comportements humains, avec le risque de causer des dommages importants, en particulier d'avoir des incidences suffisamment importantes sur la santé physique ou psychologique ou sur les intérêts financiers, sont particulièrement dangereuses et devraient dès lors être interdites. Ces systèmes d'IA font intervenir des composants subliminaux, tels que des stimuli sonores, visuels ou vidéo que l'individu ne peut percevoir, étant donné que ces stimuli échappent à la perception humaine, ou d'autres techniques manipulatrices ou trompeuses qui mettent à mal ou altèrent l'autonomie de la personne, son libre arbitre ou sa liberté de choix de telle sorte que l'individu n'est pas conscient de ces techniques ou, à supposer qu'il le soit, sans qu'il puisse échapper à la duperie ni opposer une résistance ou un contrôle auxdites techniques. Cela pourrait être facilité, par exemple, par des interfaces cerveau-machine ou par la réalité virtuelle étant donné qu'elles permettent d'avoir plus de contrôle sur les stimuli qui sont présentés aux personnes, dans la mesure où elles peuvent en altérer sensiblement le comportement d'une manière très nocive. En outre, des systèmes d'IA peuvent également exploiter les vulnérabilités d'une personne ou d'un groupe particulier de personnes en raison

de leur âge, d'un handicap au sens de la directive (UE) 2019/882 du Parlement européen et du Conseil ([16]), ou d'une situation sociale ou économique spécifique susceptible de rendre ces personnes plus vulnérables à l'exploitation, telles que les personnes vivant dans une extrême pauvreté ou appartenant à des minorités ethniques ou religieuses. De tels systèmes d'IA peuvent être mis sur le marché, mis en service ou utilisés avec pour objectif ou pour effet d'altérer substantiellement le comportement d'une personne d'une manière qui cause ou est raisonnablement susceptible de causer un préjudice important à cette personne ou à une autre personne ou à des groupes de personnes, y compris des dommages susceptibles de s'accumuler au fil du temps, et il y a lieu, par conséquent, de les interdire. Il peut s'avérer impossible de présumer l'existence d'une intention d'altérer le comportement lorsque cette altération résulte de facteurs externes au système d'IA qui échappent au contrôle du fournisseur ou du déployeur, à savoir de facteurs qui ne peuvent être raisonnablement prévisibles, et partant, ne peuvent être atténués par le fournisseur ou le déployeur du système d'IA. En tout état de cause, il n'est pas nécessaire que le fournisseur ou le déployeur ait l'intention de causer un préjudice important, du moment que ce préjudice résulte de pratiques de manipulation ou d'exploitation reposant sur l'IA. Les interdictions de telles pratiques en matière d'IA complètent les dispositions de la directive 2005/29/CE du Parlement européen et du Conseil ([17]), notamment concernant le fait que les pratiques commerciales déloyales entraînant des préjudices économiques ou financiers pour les consommateurs sont interdites en toutes circonstances, qu'elles soient mises en place au moyen de systèmes d'IA ou autrement. Les interdictions des pratiques de manipulation et d'exploitation prévues par le présent règlement ne devraient pas affecter les pratiques licites dans le cadre de traitements médicaux tels que le traitement psychologique d'une maladie mentale ou la rééducation physique, lorsque ces pratiques sont effectuées conformément à la législation applicable et aux normes médicales, comme le consentement explicite des personnes ou de leurs représentants légaux. En outre, les pratiques commerciales courantes et légitimes, par exemple dans le domaine de la publicité, qui respectent le droit applicable ne devraient pas, en soi, être considérées comme constituant des pratiques de manipulation préjudiciables reposant sur l'IA.

(30) Il y a lieu d'interdire les systèmes de catégorisation biométrique fondés sur les données biométriques des personnes physiques, comme le visage ou les empreintes digitales, utilisés pour arriver à des déductions ou des inférences concernant les opinions politiques d'un individu, son affiliation à une organisation syndicale, ses convictions religieuses ou philosophiques, sa race, sa vie sexuelle ou son orientation sexuelle. Cette interdiction ne devrait pas couvrir l'étiquetage, le filtrage ou la catégorisation licites des ensembles de données biométriques acquis dans le respect du droit de l'Union ou du droit national en fonction de données biométriques, comme le tri des images en fonction de la couleur des cheveux ou de celle des yeux, qui peuvent par exemple être utilisés dans le domaine répressif.

(31) Les systèmes d'IA permettant la notation sociale des personnes physiques par des acteurs publics ou privés peuvent conduire à des résultats discriminatoires et à l'exclusion de certains groupes. Ils peuvent porter atteinte au droit à la dignité et à la non-discrimination et sont contraires aux valeurs d'égalité et de justice. Ces systèmes d'IA évaluent ou classent les personnes physiques ou les groupes de personnes physiques en fonction de plusieurs points de données liées à leur comportement social dans divers contextes ou de caractéristiques personnelles ou de personnalité connues, déduites ou prédites pendant un certain temps. La

note sociale obtenue à partir de ces systèmes d'IA peut conduire au traitement préjudiciable ou défavorable de personnes physiques ou de groupes entiers dans des contextes sociaux qui sont dissociés du contexte dans lequel les données ont été initialement générées ou collectées, ou à un traitement préjudiciable disproportionné ou injustifié au regard de la gravité de leur comportement social. Il y a donc lieu d'interdire les systèmes d'IA impliquant de telles pratiques de notation inacceptables et produisant de tels effets préjudiciables ou défavorables. Cette interdiction ne devrait pas avoir d'incidence sur les évaluations licites des personnes physiques qui sont pratiquées dans un but précis, dans le respect du droit de l'Union et du droit national.

(32) 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 particulièrement intrusive pour les droits et les libertés des personnes concernées, dans la mesure où elle peut toucher la vie privée d'une grande partie de la population, susciter un sentiment de surveillance constante et dissuader indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux. Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Ce risque de résultats biaisés et d'effets discriminatoires est particulièrement significatif en ce qui concerne l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. En outre, du fait de l'immédiateté des effets et des possibilités limitées d'effectuer des vérifications ou des corrections supplémentaires, l'utilisation de systèmes fonctionnant en temps réel engendre des risques accrus pour les droits et les libertés des personnes concernées dans le cadre d'activités répressives ou affectées par celles-ci.

(33) L'utilisation de ces systèmes à des fins répressives devrait donc être interdite, sauf dans des situations précisément répertoriées et rigoureusement définies, dans lesquelles l'utilisation se limite au strict nécessaire à la réalisation d'objectifs d'intérêt général dont l'importance l'emporte sur les risques encourus. Ces situations comprennent la recherche de certaines victimes d'actes criminels, y compris de personnes disparues; certaines menaces pour la vie ou la sécurité physique des personnes physiques, ou des menaces d'attaque terroriste; et la localisation ou l'identification des auteurs ou des suspects des infractions pénales énumérées dans une annexe du présent règlement, lorsque ces infractions pénales sont passibles, dans l'État membre concerné, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins quatre ans et telles qu'elles sont définies dans le droit dudit État membre. Le seuil fixé pour la peine ou la mesure de sûreté privative de liberté prévue par le droit national contribue à garantir que l'infraction soit suffisamment grave pour justifier l'utilisation de systèmes d'identification biométrique à distance «en temps réel». En outre, la liste des infractions pénales figurant en annexe du présent règlement sont basées sur les 32 infractions pénales énumérées dans la décision-cadre 2002/584/JAI du Conseil ([18]), compte tenu du fait que certaines de ces infractions sont, en pratique, susceptibles d'être plus pertinentes que d'autres, dans le sens où le recours à l'identification biométrique à distance «en temps réel» pourrait, vraisemblablement, être nécessaire et proportionné, à des degrés très divers, pour les mesures pratiques de localisation ou d'identification d'un auteur ou d'un suspect de l'une des différentes infractions pénales répertoriées, eu égard également aux différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des éventuelles conséquences négatives. Une menace imminente pour la vie ou pour la sécurité

physique des personnes physiques pourrait également résulter d'une grave perturbation d'une infrastructure critique, au sens de l'article 2, point 4), de la directive (UE) 2022/2557 du Parlement européen et du Conseil ([19]), lorsque l'arrêt ou la destruction de cette infrastructure critique entraînerait une menace imminente pour la vie ou la sécurité physique d'une personne, notamment en portant gravement atteinte à la fourniture de produits de base à la population ou à l'exercice de la fonction essentielle de l'État. Par ailleurs, le présent règlement devrait préserver la capacité des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile d'effectuer des contrôles d'identité en présence de la personne concernée conformément aux conditions prévues par le droit de l'Union et le droit national pour ces contrôles. En particulier, les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile devraient pouvoir utiliser des systèmes d'information, conformément au droit de l'Union ou au droit national, pour identifier une personne qui, lors d'un contrôle d'identité, soit refuse d'être identifiée, soit n'est pas en mesure de décliner son identité ou de la prouver, sans qu'il leur soit fait obligation par le présent règlement d'obtenir une autorisation préalable. Il peut s'agir, par exemple, d'une personne impliquée dans une infraction, qui ne veut pas ou ne peut pas divulguer son identité aux autorités répressives en raison d'un accident ou de son état de santé.

(34) Afin de s'assurer que ces systèmes soient utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune des situations précisément répertoriées et rigoureusement définies, certains éléments devraient être pris en considération, notamment en ce qui concerne la nature de la situation donnant lieu à la demande et les conséquences de l'utilisation pour les droits et les libertés de toutes les personnes concernées, ainsi que les garanties et les conditions associées à l'utilisation. En outre, l'utilisation, à des fins répressives, de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public ne devrait être déployée que pour confirmer l'identité de la personne spécifiquement ciblée et elle devrait être limitée au strict nécessaire dans le temps, ainsi que du point de vue de la portée géographique et personnelle, eu égard en particulier aux preuves ou aux indications concernant les menaces, les victimes ou les auteurs. L'utilisation du système d'identification biométrique à distance en temps réel dans des espaces accessibles au public ne devrait être autorisée que si l'autorité répressive compétente a réalisé une analyse d'impact sur les droits fondamentaux et, sauf disposition contraire du présent règlement, a enregistré le système dans la base de données prévue par le présent règlement. La base de données de référence des personnes devrait être appropriée pour chaque cas d'utilisation dans chacune des situations mentionnées ci-dessus.

(35) Toute utilisation d'un système d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives devrait être subordonnée à l'autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre dont la décision est contraignante. Cette autorisation devrait en principe être obtenue avant l'utilisation du système d'IA en vue d'identifier une ou plusieurs personnes. Des exceptions à cette règle devraient être autorisées dans des situations dûment justifiées en raison du caractère urgent, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est de nature à rendre effectivement et objectivement impossible l'obtention d'une autorisation avant de commencer à utiliser le système d'IA. Dans de telles situations d'urgence, l'utilisation du système d'IA devrait être limitée au strict nécessaire et assortie de

garanties et de conditions appropriées, telles qu'elles sont déterminées dans le droit national et spécifiées dans le contexte de chaque cas d'utilisation urgente par les autorités répressives elles-mêmes. En outre, l'autorité répressive devrait, dans ce genre de situation, solliciter une telle autorisation tout en indiquant les raisons pour lesquelles elle n'a pas été en mesure de le faire plus tôt, sans retard injustifié et au plus tard dans un délai de 24 heures. Lorsqu'une demande d'autorisation est rejetée, l'utilisation de systèmes d'identification biométrique en temps réel liés à cette autorisation devrait cesser immédiatement et toutes les données relatives à cette utilisation devraient être mises au rebut et supprimées. Ces données comprennent les données d'entrée directement acquises par un système d'IA au cours de l'utilisation de ce système, ainsi que les résultats et sorties de l'utilisation liée à cette autorisation. Cela ne devrait pas comprendre les entrées qui sont légalement acquises dans le respect d'un autre droit national ou du droit de l'Union. En tout état de cause, aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne devrait être prise sur la seule base des sorties du système d'identification biométrique à distance.

(36)Afin de s'acquitter de leurs tâches conformément aux exigences énoncées dans le présent règlement ainsi que dans les règles nationales, l'autorité de surveillance du marché concernée et l'autorité nationale chargée de la protection des données devraient être informées de chaque utilisation du système d'identification biométrique en temps réel. Les autorités de surveillance du marché et les autorités nationales chargées de la protection des données auxquelles une notification a été adressée devraient présenter à la Commission un rapport annuel sur l'utilisation des systèmes d'identification biométrique en temps réel.

(37)En outre, il convient de prévoir, dans le cadre exhaustif établi par le présent règlement, qu'une telle utilisation sur le territoire d'un État membre conformément au présent règlement ne devrait être possible que dans le cas et dans la mesure où l'État membre concerné a décidé de prévoir expressément la possibilité d'autoriser une telle utilisation dans des règles détaillées de son droit national. Par conséquent, les États membres restent libres, en vertu du présent règlement, de ne pas prévoir une telle possibilité, ou de prévoir une telle possibilité uniquement pour certains objectifs parmi ceux susceptibles de justifier l'utilisation autorisée définis dans le présent règlement. Ces règles nationales devraient être notifiées à la Commission dans les 30 jours suivant leur adoption.

(38)L'utilisation de systèmes d'IA pour l'identification biométrique à distance en temps réel de personnes physiques dans des espaces accessibles au public à des fins répressives passe nécessairement par le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, et qui sont fondées sur l'article 16 du traité sur le fonctionnement de l'Union européenne, devraient s'appliquer en tant que lex specialis pour ce qui est des règles sur le traitement des données biométriques figurant à l'article 10 de la directive (UE) 2016/680, réglementant ainsi de manière exhaustive cette utilisation et le traitement des données biométriques qui en résulte. Par conséquent, une telle utilisation et un tel traitement ne devraient être possibles que dans la mesure où ils sont compatibles avec le cadre fixé par le présent règlement, sans qu'il soit possible pour les autorités compétentes, lorsqu'elles agissent à des fins répressives en dehors de ce cadre, d'utiliser ces systèmes et de traiter ces données pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement ne vise pas à fournir la base juridique pour le traitement des données à caractère personnel en vertu de l'article 8 de la

directive (UE) 2016/680. Cependant, l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins autres que répressives, y compris par les autorités compétentes, ne devrait pas être couverte par le cadre spécifique concernant l'utilisation à des fins répressives établi par le présent règlement. L'utilisation à des fins autres que répressives ne devrait donc pas être subordonnée à l'exigence d'une autorisation au titre du présent règlement et des règles détaillées du droit national applicable susceptibles de donner effet à cette autorisation.

(39) Tout traitement de données biométriques et d'autres données à caractère personnel mobilisées lors de l'utilisation de systèmes d'IA pour l'identification biométrique, qui n'est pas lié à l'utilisation de systèmes d'identification biométrique à distance en temps réel dans des espaces accessibles au public à des fins répressives, réglementée par le présent règlement, devrait rester conforme à toutes les exigences découlant de l'article 10 de la directive (UE) 2016/680. À des fins autres que répressives, l'article 9, paragraphe 1, du règlement (UE) 2016/679 et l'article 10, paragraphe 1, du règlement (UE) 2018/1725 interdisent le traitement de données biométriques sous réserve d'exceptions limitées prévues dans ces articles. En application de l'article 9, paragraphe 1, du règlement (UE) 2016/679, l'utilisation de l'identification biométrique à distance à des fins autres que répressives a déjà fait l'objet de décisions d'interdiction prises par les autorités nationales chargées de la protection des données.

(40) 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, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande n'est pas liée par les règles fixées à l'article 5, paragraphe 1, premier alinéa, point g), dans la mesure où il s'applique à l'utilisation de systèmes de catégorisation biométrique pour des activités dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, à l'article 5, paragraphe 1, premier alinéa, point d), dans la mesure où il s'applique à l'utilisation de systèmes d'IA couverts par cette disposition, à l'article 5, paragraphe 1, premier alinéa, point h), à l'article 5, paragraphes 2 à 6, et l'article 26, paragraphe 10, du présent règlement et adoptées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne concernant le traitement de données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne, lorsque l'Irlande n'est pas liée par les règles qui régissent des formes de coopération judiciaire en matière pénale ou de coopération policière dans le cadre desquelles les dispositions fixées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne doivent être respectées.

(41) Conformément aux articles 2 et 2 *bis* du protocole n° 22 sur la position du Danemark, annexé au traité l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'est pas lié par les règles fixées à l'article 5, paragraphe 1, premier alinéa, point g), dans la mesure où il s'applique à l'utilisation de systèmes de catégorisation biométrique pour des activités dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, à l'article 5, paragraphe 1, premier alinéa, point d), dans la mesure où il s'applique à l'utilisation de systèmes d'IA couverts par cette disposition, à l'article 5, paragraphe 1, premier alinéa, point h), à l'article 5, paragraphes 2 à 6, et à l'article 26,

paragraphe 10, du présent règlement et adoptées sur la base de l'article 16 du traité sur le fonctionnement de l'Union européenne, ni soumis à leur application, lorsqu'elles concernent le traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du chapitre 4 ou du chapitre 5 du titre V de la troisième partie du traité sur le fonctionnement de l'Union européenne.

(42) Conformément à la présomption d'innocence, les personnes physiques dans l'Union devraient toujours être jugées sur leur comportement réel. Une personne physique ne devrait jamais être jugée sur la base d'un comportement prédit par l'IA uniquement sur la base de son profilage, de ses traits de personnalité ou de ses caractéristiques, telles que la nationalité, le lieu de naissance, le lieu de résidence, le nombre d'enfants, le niveau d'endettement ou le type de voiture, sans qu'il existe un motif raisonnable de soupçonner que cette personne est impliquée dans une activité criminelle sur la base de faits objectifs vérifiables et sans évaluation humaine de ceux-ci. Par conséquent, il convient d'interdire les évaluations des risques effectuées en ce qui concerne des personnes physiques dans le but d'évaluer la probabilité que ces dernières commettent une infraction ou de prévoir la survenance d'une infraction pénale, réelle ou potentielle, sur la seule base du profilage de ces personnes physiques ou de l'évaluation de leurs traits de personnalité et caractéristiques. En tout état de cause, cette interdiction ne vise ni ne concerne l'analyse des risques non fondée sur le profilage des personnes ou sur les traits de personnalité et les caractéristiques des individus, tels que les systèmes d'IA utilisant l'analyse des risques pour évaluer la probabilité de fraude financière de la part d'entreprises sur la base de transactions suspectes ou d'outils d'analyse des risques permettant de prédire la probabilité de la localisation de stupéfiants ou de marchandises illicites par les autorités douanières, par exemple sur la base de voies de trafic connues.

(43) Il y a lieu d'interdire la mise sur le marché, la mise en service à cette fin spécifique ou l'utilisation de systèmes d'IA qui créent ou développent des bases de données de reconnaissance faciale par le moissonnage non ciblé d'images faciales provenant de l'internet ou de la vidéosurveillance, parce que cette pratique ne fait qu'accentuer le sentiment de surveillance de masse et peut entraîner des violations flagrantes des droits fondamentaux, y compris du droit au respect de la vie privée.

(44) La base scientifique des systèmes d'IA visant à identifier ou à inférer les émotions suscite de vives inquiétudes, d'autant plus que l'expression des émotions varie considérablement d'une culture et d'une situation à l'autre, comme d'ailleurs chez un même individu. Les principaux défauts de ces systèmes sont, entre autres, leur fiabilité limitée, leur manque de précision et leur généralisabilité limitée. Par conséquent, les systèmes d'IA qui identifient ou déduisent les émotions ou les intentions de personnes physiques sur la base de leurs données biométriques peuvent conduire à des résultats discriminatoires et peuvent être intrusifs pour les droits et libertés des personnes concernées. Si l'on considère le déséquilibre de pouvoir qui existe dans le cadre du travail ou de l'enseignement, combiné au caractère intrusif de ces systèmes, ces derniers risqueraient de déboucher sur le traitement préjudiciable ou défavorable de certaines personnes physiques ou de groupes entiers de personnes physiques. Par conséquent, il convient d'interdire la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA destinés à être utilisés pour déterminer l'état émotionnel de personnes physiques dans des situations liées au lieu de travail et à l'enseignement. Cette interdiction ne devrait pas porter sur les

systèmes d'IA mis sur le marché strictement pour des raisons médicales ou de sécurité, tels que les systèmes destinés à un usage thérapeutique.

(45)Le présent règlement devrait être sans effet sur les pratiques interdites par le droit de l'Union, notamment en vertu du droit de la protection des données, de la lutte contre la discrimination, de la protection des consommateurs et de la concurrence.

(46)Les systèmes d'IA à haut risque ne devraient être mis sur le marché de l'Union, mis en service ou utilisés que s'ils satisfont à certaines exigences obligatoires. Ces exigences devraient garantir que les systèmes d'IA à haut risque disponibles dans l'Union ou dont les sorties sont utilisées d'une autre manière dans l'Union ne présentent pas de risques inacceptables pour d'importants intérêts publics de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union. Sur la base du nouveau cadre législatif, que la Commission a détaillé dans sa communication présentant le «"Guide bleu" relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022» ([20]), la règle générale est que plus d'un acte juridique de la législation d'harmonisation de l'Union, comme les règlements (UE) 2017/745 ([21]) et (UE) 2017/746 ([22]) du Parlement européen et du Conseil ou la directive 2006/42/CE du Parlement européen et du Conseil ([23]), peuvent s'appliquer à un produit dès lors que la mise à disposition ou la mise en service ne peut avoir lieu que lorsque le produit est conforme à l'ensemble de la législation d'harmonisation de l'Union applicable. Dans un souci de cohérence, et afin d'éviter des charges administratives ou des coûts inutiles, les fournisseurs d'un produit contenant un ou plusieurs systèmes d'IA à haut risque, auxquels s'appliquent les exigences du présent règlement et de la législation d'harmonisation de l'Union dont la liste figure en annexe du présent règlement, devraient disposer d'une certaine souplesse en ce qui concerne les décisions opérationnelles à prendre quant à la manière de garantir de façon optimale qu'un produit contenant un ou plusieurs systèmes d'IA est conforme à l'ensemble des exigences applicables de la législation d'harmonisation de l'Union. Les systèmes d'IA désignés comme étant à haut risque devraient être limités aux systèmes qui ont une incidence préjudiciable substantielle sur la santé, la sécurité et les droits fondamentaux des citoyens dans l'Union et une telle limitation devrait réduire au minimum toute éventuelle restriction au commerce international.

(47)Les systèmes d'IA pourraient avoir un impact négatif sur la santé et la sécurité des citoyens, en particulier lorsque ces systèmes sont utilisés en tant que composants de sécurité de produits. Conformément aux objectifs de la législation d'harmonisation de l'Union visant à faciliter la libre circulation des produits sur le marché intérieur et à garantir que seuls des produits sûrs et conformes à d'autres égards soient mis sur le marché, il est important de dûment prévenir et atténuer les risques pour la sécurité susceptibles d'être créés par un produit dans son ensemble en raison de ses composants numériques, y compris les systèmes d'IA. Par exemple, des robots de plus en plus autonomes, que ce soit dans le secteur de l'industrie manufacturière ou des services de soins et d'aide à autrui, devraient pouvoir opérer et remplir leurs fonctions en toute sécurité dans des environnements complexes. De même, dans le secteur de la santé, où les enjeux pour la vie et la santé sont particulièrement importants, les systèmes de diagnostic de plus en plus sophistiqués et les systèmes soutenant les décisions humaines devraient être fiables et précis.

(48)L'ampleur de l'incidence négative du système d'IA sur les droits fondamentaux protégés par la Charte est un critère particulièrement pertinent lorsqu'il s'agit de classer un système d'IA en tant que système à haut risque. Ces droits comprennent le droit à la dignité humaine, le respect

de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'expression et d'information, la liberté de réunion et d'association, le droit à la non-discrimination, le droit à l'éducation, la protection des consommateurs, les droits des travailleurs, les droits des personnes handicapées, l'égalité de genre, les droits de propriété intellectuelle, le droit à un recours effectif et à accéder à un tribunal impartial, les droits de la défense et la présomption d'innocence, et le droit à une bonne administration. En plus de ces droits, il est important de souligner le fait que les enfants bénéficient de droits spécifiques consacrés à l'article 24 de la Charte et dans la convention des Nations unies relative aux droits de l'enfant (et précisés dans l'observation générale n° 25 de la CNUDE en ce qui concerne l'environnement numérique), et que ces deux textes considèrent la prise en compte des vulnérabilités des enfants et la fourniture d'une protection et de soins appropriés comme nécessaires au bien-être de l'enfant. Le droit fondamental à un niveau élevé de protection de l'environnement, consacré dans la Charte et mis en œuvre dans les politiques de l'Union, devrait également être pris en considération lors de l'évaluation de la gravité du préjudice qu'un système d'IA peut causer, notamment en ce qui concerne les conséquences pour la santé et la sécurité des personnes.

(49) En ce qui concerne les systèmes d'IA à haut risque constituant des composants de sécurité de produits ou de systèmes, ou qui sont eux-mêmes des produits ou des systèmes entrant dans le champ d'application du règlement (CE) n° 300/2008 du Parlement européen et du Conseil ([24]), du règlement (UE) n° 167/2013 du Parlement européen et du Conseil ([25]), du règlement (UE) n° 168/2013 du Parlement européen et du Conseil ([26]), de la directive 2014/90/UE du Parlement européen et du Conseil ([27]), de la directive (UE) 2016/797 du Parlement européen et du Conseil ([28]), du règlement (UE) 2018/858 du Parlement européen et du Conseil ([29]), du règlement (UE) 2018/1139 du Parlement européen et du Conseil ([30]) ou du règlement (UE) 2019/2144 du Parlement européen et du Conseil ([31]), il convient de modifier ces actes pour veiller à ce que la Commission tienne compte, sur la base des spécificités techniques et réglementaires de chaque secteur, et sans interférer avec les mécanismes et les autorités de gouvernance, d'évaluation de la conformité et de contrôle de l'application déjà en place en vertu de ces règlements, des exigences obligatoires applicables aux systèmes d'IA à haut risque définis dans le présent règlement lors de l'adoption d'actes délégués ou d'actes d'exécution pertinents sur la base de ces actes.

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

(51) La classification d'un système d'IA comme étant à haut risque en application du présent règlement ne devrait pas nécessairement signifier que le produit utilisant le système d'IA en

tant que composant de sécurité, ou que le système d'IA lui-même en tant que produit, est considéré comme étant à haut risque selon les critères établis dans la législation d'harmonisation de l'Union correspondante qui s'applique au produit en question. Tel est notamment le cas pour le règlement (UE) 2017/745 et le règlement (UE) 2017/746, dans le cadre desquels une évaluation de la conformité par un tiers est prévue pour les produits à risque moyen et les produits à haut risque.

(52)En ce qui concerne les systèmes d'IA autonomes, à savoir les systèmes d'IA à haut risque autres que ceux qui constituent des composants de sécurité de produits ou qui sont eux-mêmes des produits, il convient de les classer comme étant à haut risque si, au vu de leur destination, ils présentent un risque élevé de causer un préjudice à la santé, à la sécurité ou aux droits fondamentaux des citoyens, en tenant compte à la fois de la gravité et de la probabilité du préjudice éventuel, et s'ils sont utilisés dans un certain nombre de domaines spécifiquement prédéfinis dans le présent règlement. La définition de ces systèmes est fondée sur la même méthode et les mêmes critères que ceux également envisagés pour toute modification ultérieure de la liste des systèmes d'IA à haut risque que la Commission devrait être habilitée à adopter, au moyen d'actes délégués, afin de tenir compte du rythme rapide de l'évolution technologique, ainsi que des changements potentiels dans l'utilisation des systèmes d'IA.

(53)Il importe également de préciser qu'il peut exister des cas spécifiques dans lesquels les systèmes d'IA visés dans des domaines prédéfinis spécifiés dans le présent règlement ne présentent pas un risque important d'atteinte aux intérêts juridiques protégés dans ces domaines parce qu'ils n'ont pas d'incidence substantielle sur la prise de décision ou ne causent pas de préjudice important à ces intérêts. Aux fins du présent règlement, il convient d'entendre par système d'IA qui n'a pas d'incidence substantielle sur le résultat de la prise de décision un système d'IA qui n'a pas d'incidence sur la substance et, partant, sur le résultat de la prise de décision, qu'elle soit humaine ou automatisée. Dans les cas où une ou plusieurs des conditions ci-après sont remplies, il pourrait s'agir d'un système d'IA qui n'a pas d'incidence substantielle sur le résultat de la prise de décision. La première de ces conditions devrait être que le système d'IA est destiné à accomplir une tâche procédurale étroite, comme transformer des données non structurées en données structurées, classer les documents entrants par catégories ou détecter les doublons parmi un grand nombre d'applications. Ces tâches sont par nature si étroites et limitées qu'elles ne présentent que des risques limités, qui ne sont pas exacerbés par une utilisation d'un système d'IA dans un contexte répertorié parmi les utilisations à haut risque dans la liste figurant en annexe du présent règlement. La deuxième condition devrait être que la tâche effectuée par le système d'IA est destinée à améliorer le résultat d'une activité humaine préalablement réalisée, susceptible d'être utile aux fins des utilisations à haut risque énumérées dans une annexe du présent règlement. Compte tenu de ces caractéristiques, le système d'IA n'ajoute qu'une couche supplémentaire à une activité humaine, ce qui présente par conséquent un risque réduit. Cette condition s'appliquerait par exemple aux systèmes d'IA destinés à améliorer la façon dont un document est rédigé, pour lui donner un ton professionnel ou un style académique ou pour l'adapter à un message de marque défini. La troisième condition devrait être que le système d'IA est destiné à détecter les constantes en matière de prise de décision ou les écarts par rapport aux constantes habituelles antérieures. Le risque serait réduit parce que l'utilisation du système d'IA intervient après la réalisation d'une évaluation humaine et n'est pas destinée à se substituer à celle-ci ni à l'influencer, sans examen humain approprié. Il s'agit par exemple des systèmes d'IA qui,

compte tenu de certaines constantes habituelles observées chez un enseignant au niveau de la notation, peuvent être utilisés pour vérifier a posteriori si l'enseignant s'est éventuellement écarté de ces constantes, de manière à signaler d'éventuelles incohérences ou anomalies. La quatrième condition devrait être que le système d'IA est destiné à exécuter une tâche qui n'est qu'un acte préparatoire à une évaluation pertinente aux fins des systèmes d'IA repris dans la liste figurant dans une annexe du présent règlement et, partant, la probabilité que les sorties produites par le système présentent un risque pour l'évaluation postérieure est très faible. Cette condition s'applique, entre autres, aux solutions intelligentes de traitement des fichiers, qui comprennent diverses fonctions telles que l'indexation, la recherche, le traitement de texte et le traitement de la parole ou le fait de relier des données à d'autres sources de données, ou aux systèmes d'IA utilisés pour la traduction de documents initiaux. En tout état de cause, les systèmes d'IA utilisés dans des cas d'utilisation à haut risque énumérés dans une annexe du présent règlement devraient être considérés comme présentant des risques importants de préjudice pour la santé, la sécurité ou les droits fondamentaux si le système d'IA implique un profilage au sens de l'article 4, point 4), du règlement (UE) 2016/679, de l'article 3, point 4), de la directive (UE) 2016/680 et de l'article 3, point 5), du règlement (UE) 2018/1725. Afin de garantir la traçabilité et la transparence, un fournisseur qui considère qu'un système d'IA n'est pas à haut risque sur la base des conditions susvisées devrait documenter l'évaluation avant la mise sur le marché ou la mise en service de ce système et fournir cette documentation aux autorités nationales compétentes sur demande. Ce fournisseur devrait être tenu d'enregistrer le système d'IA dans la base de données de l'UE établie en vertu du présent règlement. En vue de fournir des orientations supplémentaires pour la mise en œuvre pratique des critères en fonction desquels des systèmes d'IA répertoriés dans la liste figurant dans une annexe du présent règlement sont, à titre exceptionnel, des systèmes qui ne sont pas à haut risque, la Commission devrait, après consultation du Comité IA, fournir des lignes directrices précisant cette mise en œuvre pratique, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.

(54) Étant donné que les données biométriques constituent une catégorie particulière de données à caractère personnel, il convient de classer comme étant à haut risque plusieurs cas d'utilisation critique des systèmes biométriques, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables. Les inexactitudes techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Le risque de tels résultats biaisés et d'effets discriminatoires est particulièrement important en ce qui concerne l'âge, l'appartenance ethnique, la race, le sexe ou le handicap. Il convient par conséquent de classer les systèmes d'identification biométrique à distance comme étant à haut risque compte tenu des risques qu'ils présentent. Sont exclus de cette classification les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique, parmi lesquelles l'authentification, dont la seule finalité est de confirmer qu'une personne physique donnée est bien celle qu'elle prétend être et de confirmer l'identité d'une personne physique dans le seul but d'avoir accès à un service, de déverrouiller un dispositif ou de disposer d'un accès sécurisé à des locaux. En outre, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés pour la catégorisation biométrique en fonction d'attributs ou de caractéristiques sensibles protégés en vertu de l'article 9, paragraphe 1, du règlement (UE) 2016/679 sur la base de données biométriques, dans la mesure où ils ne sont pas interdits par le

présent règlement, et les systèmes de reconnaissance des émotions qui ne sont pas interdits en vertu du présent règlement. Les systèmes biométriques destinés à être utilisés uniquement dans le but de permettre la cybersécurité et les mesures de protection des données à caractère personnel ne devraient pas être considérés comme des systèmes d'IA à haut risque.

(55) En ce qui concerne la gestion et l'exploitation des infrastructures critiques, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans le cadre de la gestion et de l'exploitation des infrastructures numériques critiques visées à l'annexe, point 8, de la directive (UE) 2022/2557, du trafic routier et de l'approvisionnement en eau, gaz, électricité et chauffage, car leur défaillance ou leur mauvais fonctionnement peut mettre en danger la vie et la santé de personnes à grande échelle et entraîner des perturbations importantes dans le déroulement normal des activités sociales et économiques. Les composants de sécurité des infrastructures critiques, y compris des infrastructures numériques critiques, sont des systèmes utilisés pour protéger directement l'intégrité physique des infrastructures critiques ou la santé et la sécurité des personnes et des biens, mais qui ne sont pas nécessaires au fonctionnement du système. La défaillance ou le mauvais fonctionnement de ces composants pourrait directement entraîner des risques pour l'intégrité physique des infrastructures critiques et, partant, des risques pour la santé et la sécurité des personnes et des biens. Les composants destinés à être utilisés uniquement à des fins de cybersécurité ne devraient pas être considérés comme des composants de sécurité. Les systèmes de surveillance de la pression de l'eau ou les systèmes de commande des alarmes incendie dans les centres d'informatique en nuage sont des exemples de composants de sécurité de ces infrastructures critiques.

(56) Le déploiement de systèmes d'IA dans l'éducation est important pour promouvoir une éducation et une formation numériques de qualité et pour permettre à tous les apprenants et enseignants d'acquérir et de partager les aptitudes et compétences numériques nécessaires, y compris l'éducation aux médias, ainsi que l'esprit critique, pour participer activement à l'économie, à la société et aux processus démocratiques. Toutefois, les systèmes d'IA utilisés dans l'éducation ou la formation professionnelle, en particulier pour déterminer l'accès ou l'admission, pour affecter des personnes à des établissements ou programmes d'enseignement et de formation professionnelle à tous les niveaux, pour évaluer les acquis d'apprentissage des personnes, pour évaluer le niveau d'enseignement approprié d'une personne et influencer substantiellement le niveau d'enseignement et de formation dont bénéficiera cette personne ou auquel elle pourra avoir accès ou pour surveiller les étudiants au cours des épreuves et détecter les comportements interdits dans ce cadre devraient être classés comme étant à haut risque, car ils peuvent déterminer le parcours éducatif et professionnel d'une personne et peut par conséquent avoir une incidence sur la capacité de cette personne à assurer sa propre subsistance. Lorsqu'ils sont mal conçus et utilisés, ces systèmes peuvent être particulièrement intrusifs et mener à des violations du droit à l'éducation et à la formation ainsi que du droit à ne pas subir de discriminations, et perpétuer des schémas historiques de discrimination, par exemple à l'encontre des femmes, de certains groupes d'âge, des personnes handicapées ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle.

(57) Les systèmes d'IA utilisés pour des questions liées à l'emploi, à la gestion de la main-d'œuvre et à l'accès à l'emploi indépendant, en particulier pour le recrutement et la sélection de

personnes, pour la prise de décisions affectant les conditions des relations professionnelles, ainsi que la promotion et la résiliation des relations professionnelles contractuelles, pour l'attribution de tâches fondée sur le comportement individuel, les traits de personnalité ou les caractéristiques personnelles et pour le suivi ou l'évaluation des personnes dans le cadre de relations professionnelles contractuelles, devraient également être classés comme étant à haut risque car ces systèmes peuvent avoir une incidence considérable sur les perspectives de carrière et les moyens de subsistance de ces personnes ainsi que sur les droits des travailleurs. Les relations professionnelles contractuelles en question devraient concerner également, de manière significative, celles qui lient les employés et les personnes qui fournissent des services sur des plateformes telles que celles visées dans le programme de travail de la Commission pour 2021. Tout au long du processus de recrutement et lors de l'évaluation, de la promotion ou du maintien des personnes dans des relations professionnelles contractuelles, les systèmes d'IA peuvent perpétuer des schémas historiques de discrimination, par exemple à l'égard des femmes, de certains groupes d'âge et des personnes handicapées, ou de certaines personnes en raison de leur origine raciale ou ethnique ou de leur orientation sexuelle. Les systèmes d'IA utilisés pour surveiller les performances et le comportement de ces personnes peuvent aussi porter atteinte à leurs droits fondamentaux à la protection des données et à la vie privée.

(58) Un autre domaine dans lequel l'utilisation des systèmes d'IA mérite une attention particulière est l'accès et le droit à certains services et prestations essentiels, publics et privés, devant permettre aux personnes de participer pleinement à la société ou d'améliorer leur niveau de vie. En particulier, les personnes physiques qui demandent à bénéficier ou bénéficient de prestations et services essentiels d'aide publique de la part des pouvoirs publics, à savoir des services de soins de santé, des prestations de sécurité sociale, des services sociaux fournissant une protection dans des cas tels que la maternité, la maladie, les accidents du travail, la dépendance ou la vieillesse et la perte d'emploi et l'aide sociale et au logement, sont généralement tributaires de ces prestations et services et se trouvent dans une situation vulnérable par rapport aux autorités compétentes. Lorsqu'ils sont utilisés pour déterminer si ces prestations et services devraient être accordés, refusés, réduits, révoqués ou récupérés par les autorités, y compris pour déterminer si les bénéficiaires y ont légitimement droit, les systèmes d'IA peuvent avoir une grande incidence sur les moyens de subsistance des personnes et porter atteinte à leurs droits fondamentaux, tels que le droit à la protection sociale, à la non-discrimination, à la dignité humaine ou à un recours effectif, et devraient donc être classés comme étant à haut risque. Néanmoins, le présent règlement ne devrait pas entraver la mise en place et l'utilisation, dans l'administration publique, d'approches innovantes qui bénéficieraient d'une utilisation plus large de systèmes d'IA conformes et sûrs, à condition que ces systèmes n'entraînent pas de risque élevé pour les personnes physiques et morales. En outre, les systèmes d'IA utilisés pour évaluer la note de crédit ou la solvabilité des personnes physiques devraient être classés en tant que systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes à des ressources financières ou à des services essentiels tels que le logement, l'électricité et les services de télécommunication. Les systèmes d'IA utilisés à ces fins peuvent conduire à la discrimination entre personnes ou groupes et perpétuer des schémas historiques de discrimination, tels que ceux fondés sur les origines raciales ou ethniques, le sexe, les handicaps, l'âge ou l'orientation sexuelle, ou peuvent créer de nouvelles formes d'incidences discriminatoires. Toutefois, les systèmes d'IA prévus par le droit de l'Union aux fins de détecter les fraudes dans l'offre de services financiers et à des fins prudentielles pour

calculer les besoins en fonds propres des établissements de crédit et des compagnies d'assurance ne devraient pas être considérés comme étant à haut risque au titre du présent règlement. Par ailleurs, les systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-santé et vie peuvent avoir une incidence significative sur les moyens de subsistance de ces personnes et, s'ils ne sont pas dûment conçus, développés et utilisés, peuvent porter atteinte à leurs droits fondamentaux et entraîner de graves conséquences pour leur vie et leur santé, y compris l'exclusion financière et la discrimination. Enfin, les systèmes d'IA utilisés pour évaluer et hiérarchiser les appels d'urgence émis par des personnes physiques ou pour envoyer des services d'intervention d'urgence ou établir des priorités dans l'envoi de tels services, y compris la police, les pompiers et les secours, ainsi que dans l'utilisation des systèmes de tri des patients admis dans les services de santé d'urgence, devraient aussi être classés comme étant à haut risque car ils prennent des décisions dans des situations très critiques pour la vie, la santé et les biens des personnes.

(59) Compte tenu du rôle et de la responsabilité des autorités répressives, les actions menées par celles-ci qui supposent certaines utilisations de systèmes d'IA sont caractérisées par un degré important de déséquilibre des forces et peuvent conduire à la surveillance, à l'arrestation ou à la privation de la liberté d'une personne physique ainsi qu'à d'autres conséquences négatives sur des droits fondamentaux garantis par la Charte. En particulier, si le système d'IA n'est pas entraîné avec des données de haute qualité, ne répond pas aux exigences voulues en termes de performance, d'exactitude ou de robustesse, ou n'est pas correctement conçu et testé avant d'être mis sur le marché ou mis en service, il risque de traiter des personnes de manière discriminatoire ou, plus généralement, incorrecte ou injuste. En outre, l'exercice de droits fondamentaux procéduraux importants, tels que le droit à un recours effectif et à accéder à un tribunal impartial, ainsi que les droits de la défense et la présomption d'innocence, pourrait être entravé, en particulier lorsque ces systèmes d'IA ne sont pas suffisamment transparents, explicables et documentés. Il convient donc de classer comme étant à haut risque, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, un certain nombre de systèmes d'IA destinés à être utilisés dans un contexte répressif où l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter des conséquences négatives, conserver la confiance du public et garantir que des comptes soient rendus et que des recours puissent être exercés. Compte tenu de la nature des activités et des risques y afférents, ces systèmes d'IA à haut risque devraient inclure en particulier les systèmes d'IA destinés à être utilisés par les autorités répressives ou pour leur compte ou par les institutions, organes et organismes de l'Union pour aider les autorités répressives à évaluer le risque qu'une personne physique ne devienne victime d'infractions pénales, tels que les polygraphes et instruments similaires, à évaluer la fiabilité des preuves dans le cadre d'enquêtes ou de poursuites relatives à des infractions pénales, et, dans la mesure où cela n'est pas interdit par le présent règlement, à évaluer le risque d'infraction ou de récidive d'une personne physique non seulement sur la base du profilage de personnes physiques, mais aussi sur la base de l'évaluation des traits de personnalité, des caractéristiques ou des antécédents judiciaires de personnes physiques ou de groupes, à des fins de profilage dans le cadre de la détection d'infractions pénales, d'enquêtes et de poursuites en la matière. Les systèmes d'IA spécifiquement destinés à être utilisés pour des procédures administratives par les autorités fiscales et douanières ainsi que par les cellules de renseignement financier effectuant des

tâches administratives d'analyse d'informations dans le cadre de la législation de l'Union relative à la lutte contre le blanchiment des capitaux ne devraient pas être classés comme des systèmes d'IA à haut risque utilisés par les autorités répressives à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. L'utilisation des outils d'IA par les autorités répressives et d'autres autorités pertinentes ne devrait pas devenir un facteur d'inégalité ou d'exclusion. Les conséquences de l'utilisation des outils d'IA sur les droits de la défense des suspects ne devraient pas être ignorées, en particulier la difficulté d'obtenir des informations utiles sur le fonctionnement de ces outils et, partant, la difficulté de saisir la justice pour contester leurs résultats, en particulier pour les personnes physiques faisant l'objet d'une enquête.

(60) Les systèmes d'IA utilisés dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières touchent des personnes qui se trouvent souvent dans une situation particulièrement vulnérable et qui sont tributaires du résultat des actions des autorités publiques compétentes. L'exactitude, la nature non discriminatoire et la transparence des systèmes d'IA utilisés dans ces contextes sont donc particulièrement importantes pour garantir le respect des droits fondamentaux des personnes concernées, en particulier leurs droits à la libre circulation, à la non-discrimination, à la protection de la vie privée et des données à caractère personnel, à une protection internationale et à une bonne administration. Il convient donc de classer comme étant à haut risque, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, les systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou pour leur compte ou par les institutions, organes et organismes de l'Union chargés de tâches dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières, tels que les polygraphes et instruments similaires, pour évaluer certains risques présentés par des personnes physiques entrant sur le territoire d'un État membre ou demandant un visa ou l'asile, et pour aider les autorités publiques compétentes à procéder à l'examen, y compris l'évaluation connexe de la fiabilité des éléments de preuve, des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, aux fins de détecter, de reconnaître ou d'identifier des personnes physiques dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, à l'exception de la vérification des documents de voyage. Les systèmes d'IA utilisés dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières couverts par le présent règlement devraient être conformes aux exigences procédurales pertinentes fixées par le règlement (CE) nº 810/2009 du Parlement européen et du Conseil ([32]), la directive 2013/32/UE du Parlement européen et du Conseil ([33]) et tout autre acte législatif pertinent de l'Union. Les systèmes d'IA ne devraient en aucun cas être utilisés par les États membres ou les institutions, organes ou organismes de l'Union dans les domaines de la migration, de l'asile et de la gestion des contrôles aux frontières comme moyen de contourner les obligations internationales qui leur incombent en vertu de la convention des Nations unies relative au statut des réfugiés, signée à Genève le 28 juillet 1951, telle que modifiée par le protocole du 31 janvier 1967. Ils ne devraient pas non plus être utilisés pour enfreindre de quelque manière que ce soit le principe de non-refoulement ou pour refuser des voies d'accès légales sûres et effectives au territoire de l'Union, y compris le droit à la protection internationale.

(61)Certains systèmes d'IA destinés à être utilisés pour l'administration de la justice et les processus démocratiques devraient être classés comme étant à haut risque, compte tenu de leur incidence potentiellement significative sur la démocratie, l'état de droit, les libertés individuelles ainsi que le droit à un recours effectif et à accéder à un tribunal impartial. En particulier, pour faire face aux risques de biais, d'erreurs et d'opacité, il convient de classer comme étant à haut risque les systèmes d'IA destinés à être utilisés par une autorité judiciaire ou pour le compte de celle-ci pour aider les autorités judiciaires à rechercher et à interpréter les faits et la loi, et à appliquer la loi à un ensemble concret de faits. Les systèmes d'IA destinés à être utilisés par des organismes de règlement extrajudiciaire des litiges à ces fins devraient également être considérés comme étant à haut risque lorsque les résultats des procédures de règlement extrajudiciaire des litiges produisent des effets juridiques pour les parties. L'utilisation d'outils d'IA peut soutenir le pouvoir de décision des juges ou l'indépendance judiciaire, mais ne devrait pas les remplacer, car la décision finale doit rester une activité humaine. La classification des systèmes d'IA comme étant à haut risque ne devrait cependant pas s'étendre aux systèmes d'IA destinés à être utilisés pour des activités administratives purement accessoires qui n'ont aucune incidence sur l'administration réelle de la justice dans des cas individuels, telles que l'anonymisation ou la pseudonymisation de décisions judiciaires, de documents ou de données, la communication entre membres du personnel ou les tâches administratives.

(62)Sans préjudice des règles prévues dans le règlement (UE) 2024/900 du Parlement européen et du Conseil ([34]), et afin de faire face aux risques d'ingérence extérieure indue dans le droit de vote consacré à l'article 39 de la Charte et d'effets négatifs sur la démocratie et l'état de droit, les systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums devraient être classés comme étant à haut risque, à l'exception des systèmes d'IA dont les sorties ne touchent pas directement les personnes physiques, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques d'un point de vue administratif et logistique.

(63)Le fait qu'un système d'IA soit classé comme étant à haut risque au titre du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système est licite au titre d'autres actes législatifs de l'Union ou au titre du droit national compatible avec le droit de l'Union, concernant notamment la protection des données à caractère personnel ou l'utilisation de polygraphes et d'instruments similaires ou d'autres systèmes d'analyse de l'état émotionnel des personnes physiques. Toute utilisation de ce type devrait continuer à être subordonnée aux exigences applicables découlant de la Charte et des actes applicables du droit dérivé de l'Union et du droit national. Le présent règlement ne saurait être considéré comme constituant un fondement juridique pour le traitement des données à caractère personnel, y compris des catégories particulières de données à caractère personnel, le cas échéant, sauf disposition contraire expresse du présent règlement.

(64)Afin d'atténuer les risques liés aux systèmes d'IA à haut risque mis sur le marché ou mis en service et de garantir un niveau élevé de fiabilité, certaines exigences obligatoires devraient s'appliquer aux systèmes d'IA à haut risque, en tenant compte de la destination du système d'IA et du contexte de son utilisation et en fonction du système de gestion des risques à mettre en place par le fournisseur. Les mesures adoptées par les fournisseurs pour se conformer aux

exigences obligatoires du présent règlement devraient tenir compte de l'état de la technique généralement reconnu en matière d'IA, et être proportionnées et effectives pour atteindre les objectifs du présent règlement. Reposant sur le nouveau cadre législatif, tel que précisé dans la communication de la Commission intitulée «"Guide bleu" relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022», la règle générale est que plus d'un acte juridique de la législation d'harmonisation de l'Union peuvent être applicables à un produit donné, étant donné que la mise à disposition ou la mise en service ne peut avoir lieu que si le produit est conforme à l'ensemble de la législation d'harmonisation de l'Union applicable. Les dangers des systèmes d'IA couverts par les exigences du présent règlement concernent des aspects différents de ceux qui sont énoncés dans la législation d'harmonisation existante de l'Union, et, par conséquent, les exigences du présent règlement compléteraient l'ensemble existant de la législation d'harmonisation de l'Union. Par exemple, les machines ou les dispositifs médicaux incorporant un système d'IA peuvent présenter des risques qui ne sont pas couverts par les exigences essentielles en matière de santé et de sécurité énoncées dans la législation harmonisée pertinente de l'Union, étant donné que cette législation sectorielle ne traite pas des risques spécifiques aux systèmes d'IA. Cela implique d'appliquer conjointement et de manière complémentaire les divers actes législatifs. Dans un souci de cohérence, et afin d'éviter une charge administrative et des coûts inutiles, les fournisseurs d'un produit contenant un ou plusieurs systèmes d'IA à haut risque, auxquels s'appliquent les exigences du présent règlement ainsi que les exigences de la législation d'harmonisation de l'Union reposant sur le nouveau cadre législatif et dont la liste figure dans une annexe du présent règlement, devraient disposer d'une certaine souplesse en ce qui concerne les décisions opérationnelles à prendre quant à la manière de garantir de façon optimale qu'un produit contenant un ou plusieurs systèmes d'IA est conforme à l'ensemble des exigences applicables de cette législation harmonisée de l'Union. Cette souplesse pourrait signifier, par exemple, que le fournisseur décide d'intégrer une partie des processus d'essai et de déclaration nécessaires, ainsi que des informations et de la documentation requises en vertu du présent règlement dans la documentation et les procédures existantes requises en vertu de la législation d'harmonisation de l'Union en vigueur reposant sur le nouveau cadre législatif et dont la liste figure en annexe du présent règlement. Cela ne devrait en aucun cas porter atteinte à l'obligation qu'a le fournisseur de se conformer à toutes les exigences applicables.

(65) Le système de gestion des risques devrait consister en un processus itératif continu planifié et se dérouler sur l'ensemble du cycle de vie d'un système d'IA à haut risque. Ce processus devrait viser à identifier et à atténuer les risques des systèmes d'IA qui se posent pour la santé, la sécurité et les droits fondamentaux. Le système de gestion des risques devrait être régulièrement réexaminé et mis à jour afin de garantir le maintien de son efficacité, ainsi que la justification et la documentation de toutes les décisions et mesures importantes prises en vertu du présent règlement. Ce processus devrait garantir que le fournisseur détermine les risques ou les incidences négatives et mette en œuvre des mesures d'atténuation des risques connus et raisonnablement prévisibles des systèmes d'IA pour la santé, la sécurité et les droits fondamentaux à la lumière de leur destination et de leur mauvaise utilisation raisonnablement prévisible, y compris les risques éventuels découlant de l'interaction entre les systèmes d'IA et l'environnement dans lequel ils fonctionnent. Le système de gestion des risques devrait adopter les mesures de gestion des risques les plus appropriées à la lumière de l'état de la technique en matière d'IA. Lorsqu'il détermine les mesures de gestion des risques les plus

appropriées, le fournisseur devrait documenter et expliquer les choix effectués et, le cas échéant, associer des experts et des parties prenantes externes. Lorsqu'il s'agit de déterminer la mauvaise utilisation raisonnablement prévisible des systèmes d'IA à haut risque, le fournisseur devrait couvrir les utilisations des systèmes d'IA dont on peut raisonnablement prévoir, bien qu'elles ne soient pas directement couvertes par la destination et prévues dans la notice d'utilisation, qu'elles résultent d'un comportement humain aisément prévisible dans le contexte des caractéristiques et de l'utilisation spécifiques d'un système d'IA donné. Toutes circonstances connues ou prévisibles liées à l'utilisation du système d'IA à haut risque conformément à sa destination ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques pour la santé, la sécurité ou les droits fondamentaux, devraient figurer dans la notice d'utilisation fournie par le fournisseur. Il s'agit de veiller à ce que le déployeur en ait connaissance et en tienne compte lors de l'utilisation du système d'IA à haut risque. La détermination et la mise en œuvre de mesures d'atténuation des risques en cas de mauvaise utilisation prévisible au titre du présent règlement ne devraient pas nécessiter de la part du fournisseur, pour remédier à la mauvaise utilisation prévisible, des mesures d'entraînement supplémentaires spécifiques pour le système d'IA à haut risque. Les fournisseurs sont toutefois encouragés à envisager de telles mesures d'entraînement supplémentaires pour atténuer les mauvaises utilisations raisonnablement prévisibles, si cela est nécessaire et approprié.

(66) Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la gestion des risques, la qualité et la pertinence des jeux de données utilisés, la documentation technique et la tenue de registres, la transparence et la fourniture d'informations aux déployeurs, le contrôle humain, ainsi que la robustesse, l'exactitude et la sécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux. Aucune autre mesure moins contraignante pour le commerce n'étant raisonnablement disponible, ces exigences ne constituent pas des restrictions injustifiées aux échanges.

(67) Les données de haute qualité et l'accès à ces données jouent un rôle essentiel pour ce qui est de fournir une structure et d'assurer le bon fonctionnement de nombreux systèmes d'IA, en particulier lorsque des techniques axées sur l'entraînement de modèles sont utilisées, afin de garantir que le système d'IA à haut risque fonctionne comme prévu et en toute sécurité et qu'il ne devient pas une source de discrimination interdite par le droit de l'Union. Les jeux de données d'entraînement, de validation et de test de haute qualité nécessitent la mise en œuvre de pratiques de gouvernance et de gestion des données appropriées. Les jeux de données d'entraînement, de validation et de test, y compris les étiquettes, devraient être pertinents, suffisamment représentatifs et, dans toute la mesure du possible, exempts d'erreurs et complets au regard de la destination du système. Afin de faciliter le respect du droit de l'Union sur la protection des données, tel que le règlement (UE) 2016/679, les pratiques en matière de gouvernance et de gestion des données devraient inclure, dans le cas des données à caractère personnel, la transparence quant à la finalité initiale de la collecte des données. Les jeux de données devraient également posséder les propriétés statistiques voulues, y compris en ce qui concerne les personnes ou groupes de personnes pour lesquels le système d'IA à haut risque est destiné à être utilisé, en accordant une attention particulière à l'atténuation des éventuels biais dans les jeux de données qui sont susceptibles de porter atteinte à la santé et à la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de se traduire par

une discrimination interdite par le droit de l'Union, en particulier lorsque les données de sortie influencent les entrées pour les opérations futures («boucles de rétroaction»). Des biais peuvent, par exemple, être inhérents à des jeux de données sous-jacents, en particulier lorsque des données historiques sont utilisées, ou générés lorsque les systèmes sont mis en œuvre dans des conditions réelles. Les résultats produits par les systèmes d'IA pourraient être influencés par ces biais inhérents, qui ont tendance à se renforcer progressivement et ainsi à perpétuer et à amplifier les discriminations existantes, en particulier pour les personnes appartenant à certains groupes vulnérables, y compris les groupes ethniques ou raciaux. L'exigence selon laquelle les jeux de données doivent être dans toute la mesure du possible complets et exempts d'erreurs ne devrait pas avoir d'effet sur l'utilisation de techniques respectueuses de la vie privée dans le contexte du développement et de la mise à l'essai des systèmes d'IA. En particulier, les jeux de données devraient prendre en considération, dans la mesure requise au regard de leur destination, les propriétés, les caractéristiques ou les éléments qui sont propres au cadre géographique, contextuel, comportemental ou fonctionnel spécifique dans lequel le système d'IA est destiné à être utilisé. Les exigences relatives à la gouvernance des données peuvent être respectées en faisant appel à des tiers qui proposent des services de conformité certifiés, y compris la vérification de la gouvernance des données, l'intégrité des jeux de données et les pratiques d'entraînement, de validation et de mise à l'essai des données, dans la mesure où le respect des exigences du présent règlement en matière de données est garanti.

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

(69) Le droit au respect de la vie privée et à la protection des données à caractère personnel doit être garanti tout au long du cycle de vie du système d'IA. À cet égard, les principes de minimisation et de protection des données dès la conception et par défaut, tels qu'énoncés dans le droit de l'Union sur la protection des données, sont applicables lorsque des données à caractère personnel sont traitées. Les mesures prises par les fournisseurs pour garantir le respect de ces principes peuvent inclure non seulement l'anonymisation et le cryptage, mais aussi l'utilisation d'une technologie qui permet l'introduction d'algorithmes dans les données ainsi que l'entraînement des systèmes d'IA sans transmission entre parties ou copie des données brutes ou structurées elles-mêmes, sans préjudice des exigences en matière de gouvernance des données prévues par le présent règlement.

(70)Afin de protéger le droit d'autrui contre la discrimination qui pourrait résulter des biais dans les systèmes d'IA, les fournisseurs devraient, à titre exceptionnel, et dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais en ce qui concerne les systèmes d'IA à haut risque, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques et à la suite de l'application de toutes les conditions applicables prévues par le présent règlement en plus des conditions énoncées dans les règlements (UE) 2016/679 et (UE) 2018/1725 et dans la directive (UE) 2016/680, être en mesure de traiter également des catégories particulières de données à caractère personnel, pour des raisons d'intérêt public important au sens de l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et de l'article 10, paragraphe 2, point g), du règlement (UE) 2018/1725.

(71)Il est essentiel de disposer d'informations compréhensibles sur la manière dont les systèmes d'IA à haut risque ont été développés et sur leur fonctionnement tout au long de leur durée de vie afin de permettre la traçabilité de ces systèmes, de vérifier le respect des exigences du présent règlement et de surveiller le fonctionnement des systèmes en question et d'assurer leur surveillance après commercialisation. Cela nécessite la tenue de registres et la disponibilité d'une documentation technique contenant les informations nécessaires pour évaluer la conformité du système d'IA avec les exigences pertinentes et faciliter la surveillance après commercialisation. Ces informations devraient notamment porter sur les caractéristiques générales, les capacités et les limites du système, sur les algorithmes, les données et les processus d'entraînement, de mise à l'essai et de validation utilisés, ainsi que sur le système de gestion des risques mis en place et être établies de façon claire et exhaustive. La documentation technique devrait être dûment tenue à jour tout au long de la durée de vie du système d'IA. Par ailleurs, les systèmes d'IA à haut risque devraient permettre, sur le plan technique, l'enregistrement automatique des événements, au moyen de journaux, tout au long de la durée de vie du système.

(72)Afin de répondre aux préoccupations liées à l'opacité et à la complexité de certains systèmes d'IA et d'aider les déployeurs à remplir les obligations qui leur incombent en vertu du présent règlement, la transparence devrait être requise pour les systèmes d'IA à haut risque avant leur mise sur le marché ou leur mise en service. Les systèmes d'IA à haut risque devraient être conçus de manière à permettre aux déployeurs de comprendre le fonctionnement du système d'IA, d'évaluer sa fonctionnalité et de comprendre ses forces et ses limites. Les systèmes d'IA à haut risque devraient être accompagnés d'informations appropriées sous la forme d'une notice d'utilisation. Ces informations devraient inclure les caractéristiques, les capacités et les limites de la performance du système d'IA. Il s'agirait des informations sur les éventuelles circonstances connues et prévisibles liées à l'utilisation du système d'IA à haut risque, y compris l'action des déployeurs susceptible d'influencer le comportement et la performance du système, dans le cadre desquelles le système d'IA peut entraîner des risques pour la santé, la sécurité et les droits fondamentaux, sur les changements qui ont été déterminés au préalable et évalués à des fins de conformité par le fournisseur et sur les mesures de contrôle humain pertinentes, y compris les mesures visant à faciliter l'interprétation des sorties du système d'IA par les déployeurs. La transparence, y compris la notice d'utilisation jointe au système, devrait aider les déployeurs à utiliser celui-ci et à prendre des décisions en connaissance de cause. Les déployeurs devraient, entre autres, être mieux à même de faire le bon choix quant au système

qu'ils ont l'intention d'utiliser à la lumière des obligations qui leur sont applicables, d'être informés sur les utilisations prévues et interdites et d'utiliser le système d'IA correctement et le cas échéant. Afin d'améliorer la lisibilité et l'accessibilité des informations figurant dans la notice d'utilisation, il convient, le cas échéant, d'inclure des exemples illustratifs, par exemple sur les limitations et sur les utilisations prévues et interdites du système d'IA. Les fournisseurs devraient veiller à ce que toute la documentation, y compris la notice d'utilisation, contienne des informations utiles, complètes, accessibles et compréhensibles, compte tenu des besoins et des connaissances prévisibles des déployeurs visés. La notice d'utilisation devrait être mise à disposition dans une langue aisément compréhensible par les déployeurs visés, déterminée par l'État membre concerné.

(73) Les systèmes d'IA à haut risque devraient être conçus et développés de manière à ce que les personnes physiques puissent superviser leur fonctionnement et veiller à ce qu'ils soient utilisés comme prévu et à ce que leurs incidences soient prises en compte tout au long de leur cycle de vie. À cette fin, des mesures appropriées de contrôle humain devraient être établies par le fournisseur du système avant sa mise sur le marché ou sa mise en service. En particulier, le cas échéant, de telles mesures devraient garantir que le système est soumis à des contraintes opérationnelles intégrées qui ne peuvent pas être ignorées par le système lui-même, que le système répond aux ordres de l'opérateur humain et que les personnes physiques auxquelles le contrôle humain a été confié ont les compétences, la formation et l'autorité nécessaires pour s'acquitter de ce rôle. Il est également essentiel, le cas échéant, de veiller à ce que les systèmes d'IA à haut risque comprennent des mécanismes destinés à guider et à informer une personne physique à laquelle le contrôle humain a été confié, afin qu'elle puisse décider en connaissance de cause s'il faut intervenir, à quel moment et de quelle manière, pour éviter des conséquences négatives ou des risques, ou arrêter le système s'il ne fonctionne pas comme prévu. Compte tenu des conséquences importantes pour les personnes en cas d'erreur dans les correspondances établies par certains systèmes d'identification biométrique, il convient de prévoir pour ces systèmes une exigence de contrôle humain accru, de manière qu'aucune mesure ou décision ne puisse être prise par le déployeur sur la base de l'identification obtenue par le système, à moins qu'elle n'ait été vérifiée et confirmée séparément par au moins deux personnes physiques. Ces personnes pourraient provenir d'une ou de plusieurs entités et compter parmi elles la personne qui fait fonctionner le système ou l'utilise. Cette exigence ne devrait pas entraîner de charges ou de retards inutiles, et il pourrait suffire que les vérifications effectuées séparément par les différentes personnes soient automatiquement enregistrées dans les journaux générés par le système. Compte tenu des spécificités des domaines que sont les activités répressives, la migration, les contrôles aux frontières et l'asile, cette exigence ne devrait pas s'appliquer lorsque le droit de l'Union ou le droit national considère que cette application est disproportionnée.

(74) Les systèmes d'IA à haut risque devraient produire des résultats d'une qualité constante tout au long de leur cycle de vie et assurer un niveau approprié d'exactitude, de robustesse et de cybersécurité, au vu de leur destination et conformément à l'état de la technique généralement reconnu. La Commission et les organisations et parties prenantes concernées sont encouragées à tenir dûment compte de l'atténuation des risques et des incidences négatives du système d'IA. Le niveau attendu des indicateurs de performance devrait être indiqué dans la notice d'utilisation jointe au système. Les fournisseurs sont instamment invités à communiquer ces informations aux déployeurs d'une manière claire et aisément compréhensible, sans

malentendus ou déclarations trompeuses. Le droit de l'Union en matière de métrologie légale, y compris les directives 2014/31/UE ([35]) et 2014/32/UE ([36]) du Parlement européen et du Conseil, vise à garantir l'exactitude des mesures et à contribuer à la transparence et à la loyauté des transactions commerciales. Dans ce contexte, en coopération avec les parties prenantes et organisations concernées, telles que les autorités de métrologie et d'étalonnage des performances, la Commission devrait encourager, le cas échéant, l'élaboration de critères de référence et de méthodes de mesure pour les systèmes d'IA. Ce faisant, la Commission devrait prendre note des partenaires internationaux travaillant sur la métrologie et les indicateurs de mesure pertinents relatifs à l'IA et collaborer avec ceux-ci.

(75) La robustesse technique est une exigence essentielle pour les systèmes d'IA à haut risque. Il convient qu'ils soient résilients face aux comportements préjudiciables ou, plus généralement, indésirables pouvant résulter de limites intrinsèques aux systèmes ou dues à l'environnement dans lequel les systèmes fonctionnent (par exemple les erreurs, les défaillances, les incohérences et les situations inattendues). Par conséquent, des mesures techniques et organisationnelles devraient être prises pour garantir la robustesse des systèmes d'IA à haut risque, par exemple en concevant et développant des solutions techniques appropriées pour prévenir ou réduire au minimum les comportements préjudiciables ou, plus généralement, indésirables. Ces solutions techniques peuvent comprendre, par exemple, des mécanismes permettant au système d'interrompre son fonctionnement en toute sécurité (mesures de sécurité après défaillance) en présence de certaines anomalies ou en cas de fonctionnement en dehors de certaines limites déterminées au préalable. L'absence de protection contre ces risques pourrait avoir des incidences sur la sécurité ou entraîner des violations des droits fondamentaux, par exemple en raison de décisions erronées ou de sorties inexactes ou biaisées générées par le système d'IA.

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

(77) Sans préjudice des exigences relatives à la robustesse et à l'exactitude énoncées dans le présent règlement, les systèmes d'IA à haut risque qui relèvent du champ d'application du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, conformément audit règlement, peuvent démontrer leur conformité avec les exigences de cybersécurité du présent règlement en satisfaisant aux exigences essentielles de cybersécurité énoncées audit règlement. Lorsqu'ils satisfont aux exigences essentielles du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, les systèmes d'IA à haut risque devraient être réputés

conformes aux exigences de cybersécurité énoncées dans le présent règlement dans la mesure où le respect de ces exigences est démontré dans la déclaration UE de conformité, ou dans des parties de celle-ci, délivrée en vertu dudit règlement. À cette fin, l'évaluation des risques en matière de cybersécurité associés à un produit comportant des éléments numériques classé comme système d'IA à haut risque conformément au présent règlement, effectuée en vertu du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques, devrait tenir compte des risques pesant sur la cyberrésilience d'un système d'IA en ce qui concerne les tentatives de tiers non autorisés de modifier son utilisation, son comportement ou sa performance, y compris les vulnérabilités spécifiques à l'IA telles que l'empoisonnement des données ou les attaques hostiles, ainsi que, le cas échéant, les risques pesant sur les droits fondamentaux, comme l'exige le présent règlement.

(78) La procédure d'évaluation de la conformité prévue par le présent règlement devrait s'appliquer en ce qui concerne les exigences essentielles de cybersécurité d'un produit comportant des éléments numériques relevant du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et classé comme système d'IA à haut risque en vertu du présent règlement. Toutefois, l'application de cette règle ne devrait pas entraîner de réduction du niveau d'assurance nécessaire pour les produits critiques comportant des éléments numériques couverts par le règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques. Par conséquent, par dérogation à cette règle, les systèmes d'IA à haut risque qui relèvent du champ d'application du présent règlement et sont également considérés comme des produits critiques importants comportant des éléments numériques en vertu du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et auxquels s'applique la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe du présent règlement, sont soumis aux dispositions relatives à l'évaluation de la conformité du règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques en ce qui concerne les exigences essentielles de cybersécurité énoncées dans ledit règlement. Dans ce cas, les dispositions respectives relatives à l'évaluation de la conformité fondée sur le contrôle interne énoncées à l'annexe du présent règlement devraient s'appliquer à tous les autres aspects couverts par le présent règlement. En s'appuyant sur les connaissances et l'expertise de l'ENISA en ce qui concerne la politique de cybersécurité et les tâches qui lui sont confiées en vertu du règlement (UE) 2019/881 du Parlement européen et du Conseil ([37]), la Commission devrait coopérer avec l'ENISA sur les questions liées à la cybersécurité des systèmes d'IA.

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

(80) En leur qualité de signataires de la convention des Nations unies relative aux droits des personnes handicapées, l'Union et les États membres sont légalement tenus de protéger les personnes handicapées contre la discrimination et de promouvoir leur égalité, de veiller à ce

que les personnes handicapées aient accès, au même titre que les autres, aux technologies et aux systèmes d'information et de communication, ainsi que de garantir le respect de leur vie privée. Compte tenu de l'importance et de l'utilisation croissantes des systèmes d'IA, l'application des principes de conception universelle à toutes les nouvelles technologies et à tous les nouveaux services devrait garantir un accès complet et égal à toute personne potentiellement concernée par les technologies d'IA ou les utilisant, y compris les personnes handicapées, d'une manière qui tienne pleinement compte de leur dignité et de leur diversité intrinsèques. Il est donc essentiel que les fournisseurs garantissent la pleine conformité avec les exigences en matière d'accessibilité, y compris la directive (UE) 2016/2102 du Parlement européen et du Conseil ([38]) et la directive (UE) 2019/882. Les fournisseurs devraient veiller au respect de ces exigences dès la conception. Les mesures nécessaires devraient donc être aussi intégrées que possible dans la conception des systèmes d'IA à haut risque.

(81) Le fournisseur devrait mettre en place un système solide de gestion de la qualité, garantir le respect de la procédure d'évaluation de la conformité requise, rédiger la documentation pertinente et mettre en place un système solide de surveillance après commercialisation. Les fournisseurs de systèmes d'IA à haut risque qui sont soumis à des obligations en matière de systèmes de gestion de la qualité en vertu du droit sectoriel pertinent de l'Union devraient avoir la possibilité d'intégrer les éléments du système de gestion de la qualité prévus par le présent règlement dans le système de gestion de la qualité existant prévu dans cet autre droit sectoriel de l'Union. La complémentarité entre le présent règlement et le droit sectoriel existant de l'Union devrait également être prise en compte dans les futures activités ou orientations de normalisation de la Commission. Les autorités publiques qui mettent en service des systèmes d'IA à haut risque destinés à être utilisés exclusivement par elles peuvent adopter et mettre en œuvre les règles relatives au système de gestion de la qualité dans le cadre du système de gestion de la qualité adopté au niveau national ou régional, selon le cas, en tenant compte des spécificités du secteur, ainsi que des compétences et de l'organisation de l'autorité publique concernée.

(82) Pour permettre le contrôle de l'application du présent règlement et créer des conditions de concurrence équitables pour les opérateurs, et compte tenu des différentes formes de mise à disposition 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 leurs systèmes d'IA à disposition dans l'Union, les fournisseurs établis dans des pays tiers devraient nommer, par mandat écrit, un mandataire établi dans l'Union. Ce mandataire joue un rôle capital en ce sens qu'il veille à la conformité des systèmes d'IA à haut risque mis sur le marché ou mis en service dans l'Union par des fournisseurs qui ne sont pas établis dans l'Union et sert à ces derniers de point de contact établi dans l'Union.

(83) Compte tenu de la nature et de la complexité de la chaîne de valeur des systèmes d'IA, et conformément au nouveau cadre législatif, il est essentiel de garantir la sécurité juridique et de faciliter le respect du présent règlement. Par conséquent, il est nécessaire de préciser le rôle et les obligations spécifiques des opérateurs concernés tout au long de ladite chaîne de valeur, tels que les importateurs et les distributeurs qui peuvent contribuer au développement des systèmes d'IA. Dans certaines situations, ces opérateurs pourraient jouer plus d'un rôle en même temps

et devraient donc remplir toutes les obligations pertinentes associées à ces rôles. Par exemple, un opérateur pourrait agir à la fois en tant que distributeur et importateur.

(84)Afin de garantir la sécurité juridique, il est nécessaire de préciser que, dans certaines conditions particulières, tout distributeur, importateur, déployeur ou autre tiers devrait être considéré comme un fournisseur d'un système d'IA à haut risque et, par conséquent, assumer toutes les obligations correspondantes. Tel serait le cas si cette partie met son nom ou sa marque sur un système d'IA à haut risque déjà mis sur le marché ou mis en service, sans préjudice des dispositions contractuelles stipulant que les obligations sont attribuées d'une autre manière. Tel serait aussi le cas si cette partie apporte une modification substantielle à un système d'IA à haut risque qui a déjà été mis sur le marché ou a déjà été mis en service et de telle sorte qu'il demeure un système d'IA à haut risque conformément au présent règlement, ou si elle modifie la destination d'un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé comme étant à haut risque et qui a déjà été mis sur le marché ou mis en service, de telle sorte que le système d'IA devient un système d'IA à haut risque conformément au présent règlement. Ces dispositions devraient s'appliquer sans préjudice de dispositions plus spécifiques établies dans certains actes législatifs de l'Union en matière d'harmonisation reposant sur le nouveau cadre législatif avec lesquels le présent règlement devrait s'appliquer. Par exemple, l'article 16, paragraphe 2, du règlement (UE) 2017/745, qui dispose que certaines modifications ne devraient pas être considérées comme des modifications d'un dispositif susceptibles d'influer sur sa conformité avec les exigences applicables, devrait continuer de s'appliquer aux systèmes d'IA à haut risque constituant des dispositifs médicaux au sens dudit règlement.

(85)Les systèmes d'IA à usage général peuvent être utilisés comme des systèmes d'IA à haut risque en tant que tels ou comme des composants d'autres systèmes d'IA à haut risque. Dès lors, en raison de leur nature particulière, et afin de garantir un partage équitable des responsabilités tout au long de la chaîne de valeur de l'IA, les fournisseurs de systèmes d'IA à usage général, indépendamment du fait que ces systèmes puissent être utilisés comme des systèmes d'IA à haut risque en tant que tels par d'autres fournisseurs ou comme des composants de systèmes d'IA à haut risque, et sauf dispositions contraires du présent règlement, devraient coopérer étroitement avec les fournisseurs des systèmes d'IA à haut risque concernés afin de leur permettre de se conformer aux obligations pertinentes prévues par le présent règlement et avec les autorités compétentes établies en vertu du présent règlement.

(86)Lorsque, dans les conditions prévues par le présent règlement, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA ne devrait plus être considéré comme le fournisseur aux fins du présent règlement, et lorsque ce fournisseur n'a pas expressément exclu le changement du système d'IA en un système d'IA à haut risque, ce fournisseur devrait néanmoins coopérer étroitement, mettre à disposition les informations nécessaires et fournir l'accès technique raisonnablement attendu et toute autre assistance qui sont requis pour le respect des obligations énoncées dans le présent règlement, notamment en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque.

(87)En outre, lorsqu'un système d'IA à haut risque qui est un composant de sécurité d'un produit relevant du champ d'application de la législation d'harmonisation de l'Union reposant sur le nouveau cadre législatif n'est pas mis sur le marché ou mis en service indépendamment du produit, le fabricant du produit défini par cette législation devrait se conformer aux obligations

du fournisseur établies dans le présent règlement et devrait, en particulier, garantir que le système d'IA intégré dans le produit final est conforme aux exigences du présent règlement.

(88)Tout au long de la chaîne de valeur de l'IA, plusieurs parties fournissent souvent des systèmes, des outils et des services d'IA, mais aussi des composants ou des processus que le fournisseur intègre dans le système d'IA avec plusieurs objectifs, dont l'entraînement de modèles, le réentraînement de modèles, la mise à l'essai et l'évaluation de modèles, l'intégration dans des logiciels ou d'autres aspects du développement de modèles. Ces parties ont un rôle important à jouer dans la chaîne de valeur vis-à-vis du fournisseur du système d'IA à haut risque dans lequel leurs systèmes, outils, services, composants ou processus d'IA sont intégrés, et devraient fournir à ce fournisseur, en vertu d'un accord écrit, les informations, les capacités, l'accès technique et toute autre assistance nécessaires sur la base de l'état de la technique généralement reconnu, afin de lui permettre de se conformer pleinement aux obligations énoncées dans le présent règlement, sans compromettre leurs propres droits de propriété intellectuelle ou secrets d'affaires.

(89)Les tiers qui rendent accessibles au public des outils, services, processus ou composants d'IA autres que des modèles d'IA à usage général ne devraient pas être tenus de se conformer aux exigences visant les responsabilités tout au long de la chaîne de valeur de l'IA, en particulier à l'égard du fournisseur qui les a utilisés ou intégrés, lorsque ces outils, services, processus ou composants d'IA sont rendus accessibles sous licence libre et ouverte. Les développeurs d'outils, de services, de processus ou de composants d'IA libres et ouverts autres que les modèles d'IA à usage général devraient être encouragés à mettre en œuvre des pratiques documentaires largement adoptées, telles que les cartes modèles et les fiches de données, afin d'accélérer le partage d'informations tout au long de la chaîne de valeur de l'IA, ce qui permettrait de promouvoir des systèmes d'IA fiables dans l'Union.

(90)La Commission pourrait élaborer et recommander des clauses contractuelles types volontaires à établir entre les fournisseurs de systèmes d'IA à haut risque et les tiers qui fournissent des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans les systèmes d'IA à haut risque, afin de faciliter la coopération tout au long de la chaîne de valeur. Lorsqu'elle élabore des clauses contractuelles types volontaires, la Commission devrait aussi tenir compte des éventuelles exigences contractuelles applicables dans des secteurs ou des activités spécifiques.

(91)Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux potentiellement associés à leur utilisation, notamment en ce qui concerne la nécessité d'assurer un suivi adéquat de la performance d'un système d'IA dans un contexte réel, il convient de définir des responsabilités spécifiques pour les déployeurs. Les déployeurs devraient en particulier prendre des mesures techniques et organisationnelles appropriées pour pouvoir utiliser les systèmes d'IA à haut risque conformément à la notice d'utilisation, et certaines autres obligations devraient être prévues en ce qui concerne la surveillance du fonctionnement des systèmes d'IA et la tenue de registres, selon le cas. En outre, les déployeurs devraient veiller à ce que les personnes chargées de mettre en œuvre la notice d'utilisation et au contrôle humain des systèmes énoncées dans le présent règlement possèdent les compétences nécessaires, en particulier un niveau adéquat de maîtrise, de formation et d'autorité en matière d'IA pour s'acquitter correctement de ces tâches. Ces obligations

devraient être sans préjudice des autres obligations des déployeurs en ce qui concerne les systèmes d'IA à haut risque en vertu du droit de l'Union ou du droit national.

(92)Le présent règlement est sans préjudice de l'obligation qu'ont les employeurs d'informer ou d'informer et de consulter les travailleurs ou leurs représentants en vertu du droit et des pratiques nationales ou de l'Union, y compris la directive 2002/14/CE du Parlement européen et du Conseil ([39]), sur les décisions de mise en service ou d'utilisation de systèmes d'IA. Il reste nécessaire de veiller à ce que les travailleurs et leurs représentants soient informés du déploiement prévu de systèmes d'IA à haut risque sur le lieu de travail lorsque les conditions de cette obligation d'information ou d'information et de consultation figurant dans d'autres instruments juridiques ne sont pas remplies. En outre, ce droit à l'information est accessoire et nécessaire à l'objectif de protection des droits fondamentaux qui sous-tend le présent règlement. Par conséquent, il convient de prévoir une obligation d'information à cet effet dans le présent règlement, sans porter atteinte aux droits existants des travailleurs.

(93)Si des risques liés aux systèmes d'IA peuvent découler de la manière dont ces systèmes sont conçus, ils peuvent également provenir de la manière dont ces systèmes d'IA sont utilisés. Les déployeurs de systèmes d'IA à haut risque jouent donc un rôle essentiel pour ce qui est de garantir la protection des droits fondamentaux, en complétant les obligations du fournisseur lors du développement du système d'IA. Les déployeurs sont les mieux placés pour comprendre comment le système d'IA à haut risque sera utilisé concrètement et peuvent donc identifier les risques importants potentiels qui n'étaient pas prévus au cours de la phase de développement, en raison d'une connaissance plus précise du contexte d'utilisation et des personnes ou groupes de personnes susceptibles d'être concernés, y compris les groupes vulnérables. Les déployeurs de systèmes d'IA à haut risque énumérés dans une annexe du présent règlement contribuent également de façon essentielle à informer les personnes physiques et devraient, lorsqu'ils prennent des décisions ou facilitent la prise de décisions concernant des personnes physiques, selon le cas, informer lesdites personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque. Cette information devrait comprendre la destination du système et le type de décisions prises. Les déployeurs devraient aussi informer les personnes physiques de leur droit à une explication prévu par le présent règlement. En ce qui concerne les systèmes d'IA à haut risque utilisés à des fins répressives, cette obligation devrait être mise en œuvre conformément à l'article 13 de la directive (UE) 2016/680.

(94)Tout traitement de données biométriques intervenant dans l'utilisation de systèmes d'IA à des fins d'identification biométrique de nature répressive doit être conforme à l'article 10 de la directive (UE) 2016/680, qui n'autorise un tel traitement que lorsque cela est strictement nécessaire, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, et lorsqu'il est autorisé par le droit de l'Union ou le droit d'un État membre. Une telle utilisation, lorsqu'elle est autorisée, doit également respecter les principes énoncés à l'article 4, paragraphe 1, de la directive (UE) 2016/680, notamment la licéité, la loyauté et la transparence, la limitation des finalités, l'exactitude et la limitation de la conservation.

(95)Sans préjudice du droit de l'Union applicable, en particulier le règlement (UE) 2016/679 et la directive (UE) 2016/680, et compte tenu de la nature intrusive des systèmes d'identification biométrique à distance a posteriori, l'utilisation de systèmes d'identification biométrique à distance a posteriori devrait être soumise à des garanties. Les systèmes d'identification

biométrique à distance a posteriori devraient toujours être utilisés d'une manière proportionnée, légitime et strictement nécessaire, et donc ciblée, en ce qui concerne les personnes à identifier, le lieu et la portée temporelle et fondée sur un jeu de données fermé d'images vidéo légalement acquises. En tout état de cause, les systèmes d'identification biométrique à distance a posteriori ne devraient pas être utilisés dans le cadre d'activités répressives pour mener à une surveillance aveugle. Les conditions d'identification biométrique à distance a posteriori ne devraient en aucun cas constituer une base permettant de contourner les conditions applicables en ce qui concerne l'interdiction et les exceptions strictes pour l'identification biométrique à distance en temps réel.

(96) Afin de garantir efficacement la protection des droits fondamentaux, les déployeurs de systèmes d'IA à haut risque qui sont des organismes de droit public ou des entités privées fournissant des services publics et des déployeurs de certains systèmes d'IA à haut risque énumérés dans une annexe du présent règlement, tels que des entités bancaires ou d'assurance, devraient procéder à une analyse d'impact de ces systèmes concernant les droits fondamentaux avant de les mettre en service. Les services à caractère public importants pour les personnes peuvent également être fournis par des entités privées. Les entités privées fournissant de tels services publics sont liées à des missions d'intérêt public dans des domaines tels que l'éducation, les soins de santé, les services sociaux, le logement et l'administration de la justice. L'analyse d'impact concernant les droits fondamentaux vise à ce que le déployeur identifie les risques spécifiques pour les droits des personnes ou groupes de personnes susceptibles d'être concernés et à ce qu'il détermine les mesures à prendre en cas de matérialisation de ces risques. L'analyse d'impact devrait être réalisée avant le premier déploiement du système d'IA à haut risque et être mise à jour lorsque le déployeur estime que l'un des facteurs pertinents a changé. L'analyse d'impact devrait identifier les processus pertinents du déployeur dans lesquels le système d'IA à haut risque sera utilisé conformément à sa destination, et devrait indiquer la durée pendant laquelle le système est destiné à être utilisé et selon quelle fréquence ainsi que les catégories spécifiques de personnes physiques et de groupes susceptibles d'être concernés dans le contexte spécifique d'utilisation. L'analyse devrait aussi déterminer les risques spécifiques de préjudice susceptibles d'avoir une incidence sur les droits fondamentaux de ces personnes ou groupes. Afin que cette analyse soit réalisée correctement, le déployeur devrait tenir compte des informations pertinentes, y compris, mais sans s'y limiter, les informations communiquées par le fournisseur du système d'IA à haut risque dans la notice d'utilisation. À la lumière des risques recensés, les déployeurs devraient déterminer les mesures à prendre en cas de matérialisation de ces risques, y compris, par exemple, les dispositions en matière de gouvernance dans ce contexte spécifique d'utilisation, telles que les dispositions pour le contrôle humain conformément à la notice d'utilisation ou les procédures de traitement des plaintes et de recours, en ce qu'elles pourraient contribuer à atténuer les risques pour les droits fondamentaux dans des cas d'utilisation concrets. Après avoir réalisé cette analyse d'impact, le déployeur devrait en informer l'autorité de surveillance du marché concernée. Le cas échéant, pour recueillir les informations pertinentes nécessaires à la réalisation de l'analyse d'impact, les déployeurs de systèmes d'IA à haut risque, en particulier lorsque des systèmes d'IA sont utilisés dans le secteur public, pourraient associer les parties prenantes concernées, y compris les représentants de groupes de personnes susceptibles d'être concernés par le système d'IA, les experts indépendants et les organisations de la société civile, à la réalisation de cette analyse d'impact et à la conception des mesures

à prendre en cas de matérialisation des risques. Le Bureau européen de l'intelligence artificielle (ci-après dénommé «Bureau de l'IA») devrait élaborer un modèle de questionnaire afin de faciliter la mise en conformité et de réduire la charge administrative pesant sur les déployeurs.

(97) La notion de modèles d'IA à usage général devrait être clairement définie et distincte de la notion de systèmes d'IA afin de garantir la sécurité juridique. La définition devrait se fonder sur les principales caractéristiques fonctionnelles d'un modèle d'IA à usage général, en particulier la généralité et la capacité d'exécuter de manière compétente un large éventail de tâches distinctes. Ces modèles sont généralement entraînés avec de grandes quantités de données, au moyen de diverses méthodes, telles que l'apprentissage auto-supervisé, non supervisé ou par renforcement. Les modèles d'IA à usage général peuvent être mis sur le marché de différentes manières, notamment au moyen de bibliothèques, d'interfaces de programmation d'applications (API), de téléchargements directs ou de copies physiques. Ces modèles peuvent être modifiés ou affinés et ainsi se transformer en nouveaux modèles. Bien que les modèles d'IA soient des composants essentiels des systèmes d'IA, ils ne constituent pas en soi des systèmes d'IA. Les modèles d'IA nécessitent l'ajout d'autres composants, tels qu'une interface utilisateur, pour devenir des systèmes d'IA. Les modèles d'IA sont généralement intégrés dans les systèmes d'IA et en font partie. Le présent règlement prévoit des règles spécifiques pour les modèles d'IA à usage général et pour les modèles d'IA à usage général qui présentent des risques systémiques, lesquelles devraient également s'appliquer lorsque ces modèles sont intégrés dans un système d'IA ou en font partie. Il convient de considérer que les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient s'appliquer une fois que ces modèles sont mis sur le marché. Lorsque le fournisseur d'un modèle d'IA à usage général intègre un propre modèle dans son propre système d'IA qui est mis à disposition sur le marché ou mis en service, ce modèle devrait être considéré comme étant mis sur le marché et, par conséquent, les obligations prévues par le présent règlement pour les modèles devraient continuer de s'appliquer en plus de celles applicables aux systèmes d'IA. Les obligations prévues pour les modèles ne devraient en aucun cas s'appliquer lorsqu'un propre modèle est utilisé pour des processus purement internes qui ne sont pas essentiels à la fourniture d'un produit ou d'un service à des tiers et que les droits des personnes physiques ne sont pas affectés. Compte tenu de leurs effets potentiellement très négatifs, les modèles d'IA à usage général présentant un risque systémique devraient toujours être soumis aux obligations pertinentes prévues par le présent règlement. La définition ne devrait pas couvrir les modèles d'IA utilisés avant leur mise sur le marché aux seules fins d'activités de recherche, de développement et de prototypage. Cela est sans préjudice de l'obligation de se conformer au présent règlement lorsque, à la suite de telles activités, un modèle est mis sur le marché.

(98) Alors que la généralité d'un modèle pourrait, entre autres, également être déterminée par un nombre de paramètres, les modèles comptant au moins un milliard de paramètres et entraînés à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle devraient être considérés comme présentant une généralité significative et exécutant de manière compétente un large éventail de tâches distinctes.

(99) Les grands modèles d'IA génératifs sont un exemple typique d'un modèle d'IA à usage général, étant donné qu'ils permettent la production flexible de contenus, tels que du texte, de

l'audio, des images ou de la vidéo, qui peuvent aisément s'adapter à un large éventail de tâches distinctes.

(100)Lorsqu'un modèle d'IA à usage général est intégré dans un système d'IA ou en fait partie, ce système devrait être considéré comme un système d'IA à usage général lorsque, en raison de cette intégration, ce système a la capacité de répondre à divers usages. Un système d'IA à usage général peut être utilisé directement ou être intégré dans d'autres systèmes d'IA.

(101)Les fournisseurs de modèles d'IA à usage général ont un rôle et une responsabilité particuliers tout au long de la chaîne de valeur de l'IA, étant donné que les modèles qu'ils fournissent peuvent constituer la base d'une série de systèmes en aval, souvent fournis par des fournisseurs en aval, qui nécessitent une bonne compréhension des modèles et de leurs capacités, à la fois pour permettre l'intégration de ces modèles dans leurs produits et pour remplir les obligations qui leur incombent en vertu du présent règlement ou d'autres règlements. Par conséquent, des mesures de transparence proportionnées devraient être prévues, y compris l'élaboration et la tenue à jour de la documentation, et la fourniture d'informations sur le modèle d'IA à usage général en vue de son utilisation par les fournisseurs en aval. La documentation technique devrait être élaborée et tenue à jour par le fournisseur de modèles d'IA à usage général afin qu'elle puisse être mise, sur demande, à la disposition du Bureau de l'IA et des autorités nationales compétentes. L'ensemble minimal d'éléments à inclure dans cette documentation devrait figurer dans des annexes spécifiques du présent règlement. La Commission devrait être habilitée à modifier ces annexes par voie d'actes délégués à la lumière des évolutions technologiques.

(102)Les logiciels et les données, y compris les modèles, publiés dans le cadre d'une licence libre et ouverte grâce à laquelle ils peuvent être partagés librement et qui permet aux utilisateurs de librement consulter, utiliser, modifier et redistribuer ces logiciels et données ou leurs versions modifiées peuvent contribuer à la recherche et à l'innovation sur le marché et offrir d'importantes possibilités de croissance pour l'économie de l'Union. Les modèles d'IA à usage général publiés sous licence libre et ouverte devraient être considérés comme garantissant des niveaux élevés de transparence et d'ouverture si leurs paramètres, y compris les poids, les informations sur l'architecture du modèle et les informations sur l'utilisation du modèle, sont rendus publics. La licence devrait également être considérée comme libre et ouverte lorsqu'elle permet aux utilisateurs d'exploiter, de copier, de distribuer, d'étudier, de modifier et d'améliorer les logiciels et les données, y compris les modèles, à condition que le fournisseur initial du modèle soit crédité et que les conditions de distribution identiques ou comparables soient respectées.

(103)Les composants d'IA libres et ouverts couvrent les logiciels et les données, y compris les modèles et les modèles à usage général, outils, services ou processus d'un système d'IA. Les composants d'IA libres et ouverts peuvent être fournis par différents canaux, y compris leur développement dans des référentiels ouverts. Aux fins du présent règlement, les composants d'IA qui sont fournis contre paiement ou monétisés, y compris par la fourniture d'un soutien technique ou d'autres services, notamment au moyen d'une plateforme logicielle, liés au composant d'IA, ou l'utilisation de données à caractère personnel pour des raisons autres qu'aux fins exclusives de l'amélioration de la sécurité, de la compatibilité ou de l'interopérabilité des logiciels, à l'exception des transactions entre micro-entreprises, ne devraient pas bénéficier des exceptions prévues pour les composants d'IA libres et ouverts.

La mise à disposition de composants d'IA au moyen de référentiels ouverts ne devrait pas, en soi, constituer une monétisation.

(104) Les fournisseurs de modèles d'IA à usage général qui sont publiés sous licence libre et ouverte et dont les paramètres, y compris les poids, les informations sur l'architecture des modèles et les informations sur l'utilisation des modèles, sont rendus publics devraient faire l'objet d'exceptions en ce qui concerne les exigences en matière de transparence imposées pour les modèles d'IA à usage général, à moins que les modèles ne puissent être considérés comme présentant un risque systémique, auquel cas le fait que les modèles soient transparents et accompagnés d'une licence ouverte ne devrait pas être considéré comme une raison suffisante pour exclure le respect des obligations prévues par le présent règlement. En tout état de cause, étant donné que la publication de modèles d'IA à usage général sous licence libre et ouverte ne révèle pas nécessairement des informations importantes sur le jeu de données utilisé pour l'entraînement ou de réglage fin du modèle et sur la manière dont le respect de la législation sur le droit d'auteur a été assuré, l'exception prévue pour les modèles d'IA à usage général en ce qui concerne les exigences en matière de transparence ne devrait pas concerner l'obligation de produire un résumé du contenu utilisé pour l'entraînement des modèles ni l'obligation de mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur, en particulier pour identifier et respecter la réservation de droits au titre de l'article 4, paragraphe 3, de la directive (UE) 2019/790 du Parlement européen et du Conseil ([40]).

(105) Les modèles d'IA à usage général, en particulier les grands modèles d'IA génératifs, capables de générer du texte, des images et d'autres contenus, présentent des possibilités d'innovation uniques mais aussi des défis pour les artistes, les auteurs et les autres créateurs, et la manière dont leur contenu créatif est créé, distribué, utilisé et consommé. Le développement et l'entraînement de ces modèles requièrent un accès à de grandes quantités de texte, d'images, de vidéos et d'autres données. Les techniques de fouille de textes et de données peuvent être largement utilisées dans ce contexte pour extraire et analyser ces contenus, qui peuvent être protégés par le droit d'auteur et les droits voisins. Toute utilisation d'un contenu protégé par le droit d'auteur nécessite l'autorisation du titulaire de droits concerné, à moins que des exceptions et limitations pertinentes en matière de droit d'auteur ne s'appliquent. La directive (UE) 2019/790 a introduit des exceptions et des limitations autorisant les reproductions et extractions d'œuvres ou d'autres objets protégés aux fins de la fouille de textes et de données, sous certaines conditions. En vertu de ces règles, les titulaires de droits peuvent choisir de réserver leurs droits sur leurs œuvres ou autres objets protégés afin d'empêcher la fouille de textes et de données, à moins que celle-ci ne soit effectuée à des fins de recherche scientifique. Lorsque les droits d'exclusion ont été expressément réservés de manière appropriée, les fournisseurs de modèles d'IA à usage général doivent obtenir une autorisation des titulaires de droits s'ils souhaitent procéder à une fouille de textes et de données sur ces œuvres.

(106) Les fournisseurs qui mettent des modèles d'IA à usage général sur le marché de l'Union devraient veiller au respect des obligations pertinentes prévues par le présent règlement. À cette fin, les fournisseurs de modèles d'IA à usage général devraient mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur et les droits voisins, en particulier pour identifier et respecter la réservation de droits exprimées par les titulaires

de droits conformément à l'article 4, paragraphe 3, de la directive (UE) 2019/790. Tout fournisseur qui met un modèle d'IA à usage général sur le marché de l'Union devrait se conformer à cette obligation, quelle que soit la juridiction dans laquelle se déroulent les actes pertinents au titre du droit d'auteur qui sous-tendent l'entraînement de ces modèles d'IA à usage général. Cela est nécessaire pour garantir des conditions de concurrence équitables entre les fournisseurs de modèles d'IA à usage général, lorsqu'aucun fournisseur ne devrait pouvoir obtenir un avantage concurrentiel sur le marché de l'Union en appliquant des normes en matière de droit d'auteur moins élevées que celles prévues dans l'Union.

(107) Afin d'accroître la transparence concernant les données utilisées dans le cadre de l'entraînement préalable et de l'entraînement des modèles d'IA à usage général, y compris le texte et les données protégés par la législation sur le droit d'auteur, il convient que les fournisseurs de ces modèles élaborent et mettent à la disposition du public un résumé suffisamment détaillé du contenu utilisé pour entraîner les modèles d'IA à usage général. Tout en tenant dûment compte de la nécessité de protéger les secrets d'affaires et les informations commerciales confidentielles, ce résumé devrait être généralement complet en termes de contenu plutôt que détaillé sur le plan technique afin d'aider les parties ayant des intérêts légitimes, y compris les titulaires de droits d'auteur, à exercer et à faire respecter les droits que leur confère la législation de l'Union, par exemple en énumérant les principaux jeux ou collections de données utilisés pour entraîner le modèle, tels que les archives de données ou bases de données publiques ou privées de grande ampleur, et en fournissant un texte explicatif sur les autres sources de données utilisées. Il convient que le Bureau de l'IA fournisse un modèle de résumé, qui devrait être simple et utile et permettre au fournisseur de fournir le résumé requis sous forme descriptive.

(108) En ce qui concerne l'obligation imposée aux fournisseurs de modèles d'IA à usage général de mettre en place une politique visant à respecter la législation de l'Union sur le droit d'auteur et de mettre à la disposition du public un résumé du contenu utilisé pour l'entraînement, le Bureau de l'IA devrait vérifier si le fournisseur a rempli cette obligation sans vérifier ou évaluer œuvre par œuvre les données d'entraînement en ce qui concerne le respect du droit d'auteur. Le présent règlement n'affecte pas l'application des règles en matière de droit d'auteur prévues par la législation de l'Union.

(109) Le respect des obligations applicables aux fournisseurs de modèles d'IA à usage général devrait correspondre et être proportionné au type de fournisseur de modèles, excluant la nécessité de se conformer pour les personnes qui développent ou utilisent des modèles à des fins non professionnelles ou de recherche scientifique, lesquelles devraient néanmoins être encouragées à se conformer volontairement à ces exigences. Sans préjudice de la législation de l'Union sur le droit d'auteur, le respect de ces obligations devrait tenir dûment compte de la taille du fournisseur et permettre aux PME, y compris aux jeunes pousses, de recourir à des méthodes simplifiées de mise en conformité qui ne devraient pas représenter un coût excessif et décourager l'utilisation de tels modèles. En cas de modification ou de réglage fin d'un modèle, les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient se limiter à cette modification ou à ce réglage fin, par exemple en complétant la documentation technique existante avec des informations sur les modifications, y compris les nouvelles sources de données d'entraînement, aux fins de conformité avec les obligations relatives à la chaîne de valeur prévues par le présent règlement.

(110) Les modèles d'IA à usage général pourraient présenter des risques systémiques qui comprennent, sans s'y limiter, tout effet négatif réel ou raisonnablement prévisible en rapport avec des accidents majeurs, des perturbations de secteurs critiques et des conséquences graves pour la santé et la sécurité publiques, tout effet négatif réel ou raisonnablement prévisible sur les processus démocratiques, la sécurité publique et la sécurité économique, et la diffusion de contenus illicites, faux ou discriminatoires. Les risques systémiques devraient être perçus comme augmentant avec les capacités et la portée du modèle, peuvent survenir tout au long du cycle de vie du modèle et sont influencés par les conditions de mauvaise utilisation, la fiabilité du modèle, l'équité et la sécurité du modèle, le niveau d'autonomie du modèle, son accès aux outils, les modalités nouvelles ou combinées, les stratégies de publication et de distribution, le potentiel de suppression des garde-fous et d'autres facteurs. En particulier, les approches internationales ont jusqu'à présent mis en évidence la nécessité de prêter attention aux risques liés à une potentielle mauvaise utilisation intentionnelle ou à des problèmes non intentionnels de contrôle liés à l'alignement sur l'intention humaine, aux risques chimiques, biologiques, radiologiques et nucléaires, tels que les moyens d'abaisser les barrières à l'entrée, y compris pour la mise au point, l'acquisition ou l'utilisation d'armes, aux cybercapacités offensives, tels que les moyens permettant la découverte, l'exploitation ou l'utilisation opérationnelle de vulnérabilités, aux effets de l'interaction et de l'utilisation des outils, y compris, par exemple, la capacité de contrôler les systèmes physiques et d'interférer avec les infrastructures critiques, aux risques liés à la possibilité que les modèles fassent des copies d'eux-mêmes ou «s'auto-reproduisent» ou qu'ils entraînent d'autres modèles, à la manière dont les modèles peuvent donner lieu à des préjugés et des discriminations préjudiciables présentant des risques pour les individus, les communautés ou les sociétés, à la facilitation de la désinformation ou au préjudice porté à la vie privée par des menaces pour les valeurs démocratiques et les droits de l'homme, et au risque qu'un événement particulier entraîne une réaction en chaîne s'accompagnant d'effets négatifs considérables qui pourraient aller jusqu'à affecter toute une ville, tout un secteur d'activité ou toute une communauté.

(111) Il convient d'établir une méthode de classification des modèles d'IA à usage général en tant que modèle d'IA à usage général présentant des risques systémiques. Étant donné que les risques systémiques résultent de capacités particulièrement élevées, un modèle d'IA à usage général devrait être considéré comme présentant des risques systémiques s'il a des capacités à fort impact, évaluées sur la base de méthodologies et d'outils techniques appropriés, ou une incidence significative sur le marché intérieur en raison de sa portée. Les capacités à fort impact des modèles d'IA à usage général sont des capacités égales ou supérieures aux capacités des modèles d'IA à usage général les plus avancés. L'éventail complet des capacités d'un modèle pourrait être mieux compris après sa mise sur le marché ou lorsque les déployeurs interagissent avec le modèle. Selon l'état de la technique au moment de l'entrée en vigueur du présent règlement, la quantité cumulée de calculs utilisée pour l'entraînement du modèle d'IA à usage général mesurée en opérations en virgule flottante est l'une des approximations pertinentes pour les capacités du modèle. La quantité cumulée de calculs utilisée pour l'entraînement inclut les calculs utilisés pour l'ensemble des activités et méthodes destinées à renforcer les capacités du modèle avant le déploiement, telles que l'entraînement préalable, la production de données synthétiques et le réglage fin. Par conséquent, il convient de fixer un seuil initial d'opérations en virgule flottante, qui, s'il est atteint par un modèle d'IA à usage général, conduit à présumer qu'il s'agit d'un modèle d'IA

à usage général présentant des risques systémiques. Ce seuil devrait être ajusté au fil du temps pour tenir compte des évolutions technologiques et industrielles, telles que les améliorations algorithmiques ou l'amélioration de l'efficacité des matériels, et être complété par des critères de référence et des indicateurs pour la capacité du modèle. À cette fin, le Bureau de l'IA devrait coopérer avec la communauté scientifique, l'industrie, la société civile et d'autres experts. Les seuils, ainsi que les outils et les critères de référence pour l'évaluation des capacités à fort impact, devraient être de bons indicateurs de la généralité et des capacités des modèles d'IA à usage général ainsi que du risque systémique qui y est associé, et pourraient tenir compte de la manière dont le modèle sera mis sur le marché ou du nombre d'utilisateurs qu'il pourrait affecter. Afin de compléter ce système, la Commission devrait avoir la possibilité de prendre des décisions individuelles désignant un modèle d'IA à usage général comme modèle d'IA à usage général présentant un risque systémique s'il est constaté que ce modèle a des capacités ou une incidence équivalentes à celles relevant du seuil fixé. Ces décisions devraient être prises sur la base d'une évaluation globale des critères de désignation des modèles d'IA à usage général présentant un risque systémique énoncés dans une annexe du présent règlement, tels que la qualité ou la taille du jeu de données d'entraînement, le nombre d'utilisateurs professionnels et finaux du modèle, ses modalités d'entrée et de sortie, son niveau d'autonomie et d'évolutivité, ou les outils auxquels il a accès. Sur demande motivée d'un fournisseur dont le modèle a été désigné comme modèle d'IA à usage général présentant un risque systémique, la Commission devrait tenir compte de la demande et peut décider de réévaluer si le modèle d'IA à usage général peut encore être considéré comme présentant un risque systémique.

(112) Il convient également d'établir de façon précise une procédure de classification d'un modèle d'IA à usage général présentant un risque systémique. Il convient de présumer qu'un modèle d'IA à usage général qui atteint le seuil applicable pour les capacités à fort impact est un modèle d'IA à usage général présentant un risque systémique. Le fournisseur devrait informer le Bureau de l'IA au plus tard deux semaines après que les exigences ont été remplies ou qu'il a été établi qu'un modèle d'IA à usage général répondra aux exigences qui conduisent à la présomption. Cela est particulièrement important en ce qui concerne le seuil d'opérations en virgule flottante, car l'entraînement des modèles d'IA à usage général nécessite une planification considérable qui inclut l'allocation préalable des ressources de calcul, et, par conséquent, les fournisseurs de modèles d'IA à usage général sont en mesure de savoir si leur modèle atteindra le seuil avant l'achèvement de l'entraînement. Dans le cadre de cette information, le fournisseur devrait pouvoir démontrer que, en raison de ses caractéristiques spécifiques, un modèle d'IA à usage général ne présente pas, exceptionnellement, de risques systémiques et qu'il ne devrait donc pas être classé comme modèle d'IA à usage général présentant des risques systémiques. Ces éléments d'information sont utiles pour le Bureau de l'IA en ce qu'ils lui permettent d'anticiper la mise sur le marché de modèles d'IA à usage général présentant des risques systémiques, et les fournisseurs peuvent ainsi commencer à coopérer avec le Bureau de l'IA à un stade précoce. Ils sont particulièrement importants en ce qui concerne les modèles d'IA à usage général qu'il est prévu de publier en tant que source ouverte, étant donné que, après la publication des modèles de source ouverte, les mesures nécessaires pour garantir le respect des obligations prévues par le présent règlement peuvent être plus difficiles à mettre en œuvre.

(113)Si la Commission prend connaissance du fait qu'un modèle d'IA à usage général satisfait aux exigences de classification en tant que modèle d'IA à usage général présentant un risque systémique, qui n'était pas connu auparavant ou dont le fournisseur concerné n'avait pas informé la Commission, celle-ci devrait être habilitée à désigner ce modèle comme tel. Un système d'alertes qualifiées devrait garantir que le Bureau de l'IA est informé par le panel scientifique des modèles d'IA à usage général qui devraient éventuellement être classés comme modèles d'IA à usage général présentant un risque systémique, en plus des activités de suivi du Bureau de l'IA.

(114)Les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient être soumis non seulement aux obligations prévues pour les fournisseurs de modèles d'IA à usage général mais aussi à des obligations visant à identifier et à atténuer ces risques et à garantir un niveau adéquat de protection de la cybersécurité, que les modèles en question soient fournis en tant que modèles autonomes ou qu'ils soient intégrés dans un système ou un produit d'IA. Pour atteindre ces objectifs, le présent règlement devrait exiger des fournisseurs qu'ils effectuent les évaluations nécessaires des modèles, en particulier avant leur première mise sur le marché, y compris la réalisation et la documentation d'essais contradictoires des modèles, ainsi que, le cas échéant, au moyen d'essais internes ou externes indépendants. En outre, les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient évaluer et atténuer en permanence les risques systémiques, y compris, par exemple, en mettant en place des politiques de gestion des risques, telles que des processus de responsabilité et de gouvernance, en mettant en œuvre une surveillance après commercialisation, en prenant des mesures appropriées tout au long du cycle de vie du modèle et en coopérant avec les acteurs pertinents tout au long de la chaîne de valeur de l'IA.

(115)Les fournisseurs de modèles d'IA à usage général présentant des risques systémiques devraient évaluer et atténuer les éventuels risques systémiques. Si, malgré les efforts déployés pour recenser et prévenir les risques liés à un modèle d'IA à usage général susceptible de présenter des risques systémiques, le développement ou l'utilisation du modèle cause un incident grave, le fournisseur de modèle d'IA à usage général devrait, sans retard injustifié, réaliser un suivi de l'incident et communiquer toute information pertinente et toute mesure corrective éventuelle à la Commission et aux autorités nationales compétentes. En outre, les fournisseurs devraient garantir un niveau approprié de protection en matière de cybersécurité en ce qui concerne le modèle et son infrastructure physique, le cas échéant, tout au long du cycle de vie du modèle. La protection en matière de cybersécurité contre les risques systémiques associés à une utilisation malveillante ou à des attaques devrait tenir dûment compte des fuites accidentelles du modèle, des publications non autorisées, du contournement des mesures de sécurité ainsi que de la défense contre les cyberattaques, l'accès non autorisé ou le vol de modèle. Une telle protection pourrait être facilitée par la sécurisation des poids du modèle, des algorithmes, des serveurs et des jeux de données, notamment au moyen de mesures de sécurité opérationnelle relatives à la sécurité de l'information, de politiques spécifiques en matière de cybersécurité, de solutions techniques établies adéquates, et de contrôles de l'accès physique ou informatique, qui soient adaptés aux circonstances particulières et aux risques encourus.

(116)Le Bureau de l'IA devrait encourager et faciliter l'élaboration, le réexamen et l'adaptation des codes de bonne pratique, en tenant compte des approches internationales. Tous les

fournisseurs de modèles d'IA à usage général pourraient être invités à participer. Afin de veiller à ce que les codes de bonne pratique correspondent à l'état de la technique et prennent dûment en compte un ensemble divers de perspectives, le Bureau de l'IA devrait collaborer avec les autorités nationales compétentes concernées et pourrait, selon qu'il convient, consulter les organisations de la société civile et d'autres parties prenantes et experts pertinents, notamment le groupe scientifique, pour l'élaboration de ces codes. Les codes de bonne pratique devraient traiter des obligations incombant aux fournisseurs de modèles d'IA à usage général, et de modèles d'IA à usage général présentant des risques systémiques. En outre, en ce qui concerne les risques systémiques, les codes de bonne pratique devraient contribuer à établir une taxinomie des risques reprenant le type et la nature des risques systémiques au niveau de l'Union, ainsi que leur source. Les codes de bonne pratique devraient également mettre l'accent sur une évaluation des risques et des mesures d'atténuation spécifiques.

(117) Les codes de bonne pratique devraient constituer un outil central pour assurer le bon respect des obligations qui incombent aux fournisseurs de modèles d'IA à usage général au titre du présent règlement. Les fournisseurs devraient pouvoir s'appuyer sur des codes de bonne pratique pour démontrer qu'ils respectent leurs obligations. Par voie d'actes d'exécution, la Commission pourrait décider d'approuver un code de bonnes pratiques et de lui conférer une validité générale au sein de l'Union ou, à défaut, de fixer des règles communes pour la mise en œuvre des obligations pertinentes si un code de bonnes pratiques ne peut pas être mis au point avant que le présent règlement ne devienne applicable, ou si un tel code n'est pas considéré comme adéquat par le Bureau de l'IA. Dès lors qu'une norme harmonisée est publiée et jugée appropriée par le Bureau de l'IA au regard des obligations pertinentes, les fournisseurs devraient bénéficier de la présomption de conformité lorsqu'ils respectent une norme européenne harmonisée. En outre, les fournisseurs de modèles d'IA à usage général devraient être en mesure de démontrer la conformité en utilisant d'autres moyens adéquats en l'absence de codes de bonne pratique ou de normes harmonisées ou s'ils choisissent de ne pas s'appuyer sur ceux-ci.

(118) Le présent règlement régit les systèmes et modèles d'IA en instituant certaines exigences et obligations visant les acteurs du marché concernés qui les mettent sur le marché, les mettent en service ou les utilisent dans l'Union, complétant ainsi les obligations incombant aux fournisseurs de services intermédiaires qui intègrent de tels systèmes ou modèles dans leurs services relevant du règlement (UE) 2022/2065. Dans la mesure où ces systèmes ou modèles sont intégrés dans des très grandes plateformes en ligne ou des très grands moteurs de recherche en ligne, ils sont soumis au cadre de gestion des risques établi par le règlement (UE) 2022/2065. Par conséquent, il devrait être présumé que les obligations correspondantes du présent règlement sont remplies, à moins que des risques systémiques importants non couverts par le règlement (UE) 2022/2065 n'apparaissent et ne soient recensés dans de tels modèles. Dans ce contexte, les fournisseurs de très grandes plateformes en ligne et de très grands moteurs de recherche en ligne sont tenus d'évaluer les risques systémiques découlant de la conception, du fonctionnement et de l'utilisation de leurs services, y compris la manière dont la conception des systèmes algorithmiques utilisés dans un service pourrait contribuer à ces risques, ainsi que les risques systémiques découlant de mauvaises utilisations éventuelles. Ces fournisseurs sont également tenus de prendre les mesures d'atténuation appropriées pour assurer le respect des droits fondamentaux.

(119)Compte tenu du rythme rapide de l'innovation et de l'évolution technologique des services numériques relevant du champ d'application de différents instruments du droit de l'Union, en particulier à la lumière de l'utilisation et de la perception de leurs destinataires, les systèmes d'IA régis par le présent règlement pourraient être fournis en tant que services intermédiaires ou parties de ceux-ci au sens du règlement (UE) 2022/2065, qui devrait être interprété de manière neutre sur le plan technologique. Par exemple, les systèmes d'IA pourraient être utilisés pour fournir des moteurs de recherche en ligne, en particulier, dans la mesure où un système d'IA tel qu'un dialogueur réalise des recherches sur, en principe, tous les sites web, puis en intègre les résultats dans ses connaissances existantes et utilise les connaissances mises à jour pour générer une sortie unique qui combine différentes sources d'information.

(120)En outre, les obligations imposées aux fournisseurs et aux déployeurs de certains systèmes d'IA au titre du présent règlement afin de permettre la détection et la mention du fait que les sorties produites par ces systèmes sont générées ou manipulées par une IA revêtent une importance particulière pour faciliter la mise en œuvre effective du règlement (UE) 2022/2065. Cela vaut en particulier pour les obligations incombant aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne consistant à recenser et à atténuer les risques systémiques susceptibles de découler de la diffusion de contenus qui ont été générés ou manipulés par une IA, en particulier le risque d'effets négatifs réels ou prévisibles sur les processus démocratiques, le débat public et les processus électoraux, notamment par le biais de la désinformation.

(121)La normalisation devrait jouer un rôle essentiel pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec le présent règlement, suivant les technologies les plus récentes, et de promouvoir l'innovation ainsi que la compétitivité et la croissance dans le marché unique. Le respect des normes harmonisées telles que définies à l'article 2, point 1) c), du règlement (UE) nº 1025/2012 du Parlement européen et du Conseil ([41]), qui doivent normalement tenir compte des évolutions technologiques les plus récentes, devrait être un moyen pour les fournisseurs de démontrer la conformité avec les exigences du présent règlement. Il convient donc d'encourager une représentation équilibrée des intérêts en associant toutes les parties prenantes concernées à l'élaboration des normes, en particulier les PME, les organisations de consommateurs et les acteurs environnementaux et sociaux, conformément aux articles 5 et 6 du règlement (UE) nº 1025/2012. Afin de faciliter le respect de la législation, les demandes de normalisation devraient être formulées par la Commission sans retard injustifié. Lorsqu'elle élabore les demandes de normalisation, la Commission devrait consulter le forum consultatif et le Comité IA afin de recueillir l'expertise pertinente. Toutefois, en l'absence de références pertinentes à des normes harmonisées, la Commission devrait être en mesure d'établir, au moyen d'actes d'exécution, et après consultation du forum consultatif, des spécifications communes pour certaines exigences au titre du présent règlement. Les spécifications communes devraient être une solution de repli exceptionnelle pour faciliter l'obligation du fournisseur de se conformer aux exigences du présent règlement, lorsque la demande de normalisation n'a été acceptée par aucune des organisations européennes de normalisation, ou lorsque les normes harmonisées pertinentes ne répondent pas suffisamment aux préoccupations en matière de droits fondamentaux, ou lorsque les normes harmonisées ne sont pas conformes à la demande, ou lorsque l'adoption d'une norme harmonisée appropriée accuse des retards. Lorsqu'un tel retard dans l'adoption d'une norme

harmonisée est dû à la complexité technique de ladite norme, la Commission devrait en tenir compte avant d'envisager l'établissement de spécifications communes. Lorsqu'elle élabore des spécifications communes, la Commission est encouragée à coopérer avec des partenaires internationaux et des organismes internationaux de normalisation.

(122) Il convient que, sans préjudice de l'utilisation de normes harmonisées et de spécifications communes, les fournisseurs d'un système d'IA à haut risque qui a été entraîné et testé avec des données reflétant le cadre géographique, comportemental, contextuel ou fonctionnel spécifique dans lequel il est destiné à être utilisé soient présumés comme se conformant à la mesure pertinente prévue au titre de l'exigence en matière de gouvernance des données énoncée dans le présent règlement. Sans préjudice des exigences liées à la robustesse et à l'exactitude énoncées dans le présent règlement, conformément à l'article 54, paragraphe 3, du règlement (UE) 2019/881, les systèmes d'IA à haut risque qui ont été certifiés ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité en vertu dudit règlement et dont les références ont été publiées au *Journal officiel de l'Union européenne* devraient être présumés conformes aux exigences de cybersécurité du présent règlement dans la mesure où le certificat de cybersécurité ou la déclaration de conformité, ou des parties de ceux-ci, couvrent l'exigence de cybersécurité du présent règlement. Cet aspect demeure sans préjudice du caractère volontaire dudit schéma de cybersécurité.

(123) 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.

(124) Afin de réduire au minimum la charge pesant sur les opérateurs et d'éviter les éventuels doubles emplois, la conformité avec les exigences du présent règlement des systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation existante de l'Union fondée sur le nouveau cadre législatif devrait être évaluée dans le cadre de l'évaluation de la conformité déjà prévue en vertu de cette législation. L'applicabilité des exigences du présent règlement ne devrait donc pas avoir d'incidence sur la logique, la méthode ou la structure générale propres à l'évaluation de la conformité au titre de la législation d'harmonisation de l'Union pertinente.

(125) Compte tenu de la complexité des systèmes d'IA à haut risque et des risques qui y sont associés, il importe d'élaborer une procédure d'évaluation de la conformité adéquat faisant intervenir les organismes notifiés pour ces systèmes, dite «évaluation de conformité par un tiers». Toutefois, étant donné l'expérience actuelle des organismes professionnels de certification avant mise sur le marché dans le domaine de la sécurité des produits et de la nature différente des risques encourus, il convient de limiter, au moins dans une phase initiale d'application du présent règlement, le champ d'application des évaluations de la conformité réalisées par un tiers aux systèmes d'IA à haut risque autres que ceux liés à des produits. Par conséquent, l'évaluation de la conformité de ces systèmes devrait en règle générale être réalisée par le fournisseur sous sa propre responsabilité, à la seule exception des systèmes d'IA destinés à être utilisés à des fins de biométrie.

(126) Afin de procéder à des évaluations de la conformité par un tiers lorsque cela est nécessaire, les organismes notifiés devraient être notifiés en vertu du présent règlement par les autorités nationales compétentes, sous réserve qu'ils satisfassent à un ensemble d'exigences portant en

particulier sur leur indépendance, leur compétence, l'absence de conflits d'intérêts et les exigences appropriées en matière de cybersécurité. La notification de ces organismes devrait être envoyée par les autorités nationales compétentes à la Commission et aux autres États membres à l'aide de l'outil de notification électronique mis au point et géré par la Commission, conformément à l'annexe I, article R23, de la décision n° 768/2008/CE.

(127) Conformément aux engagements pris par l'Union au titre de l'accord de l'Organisation mondiale du commerce sur les obstacles techniques au commerce, il convient de faciliter la reconnaissance mutuelle des résultats des évaluations de la conformité produits par les organismes d'évaluation de la conformité compétents, indépendamment du territoire sur lequel ils sont établis, à condition que ces organismes d'évaluation de la conformité établis en vertu du droit d'un pays tiers satisfassent aux exigences applicables en vertu du présent règlement et que l'Union ait conclu un accord en ce sens. Dans ce contexte, la Commission devrait étudier activement d'éventuels instruments internationaux à cette fin et, en particulier, œuvrer à la conclusion d'accords de reconnaissance mutuelle avec des pays tiers.

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

(129) Le marquage «CE» devrait être apposé sur les systèmes d'IA à haut risque pour indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement dans le marché intérieur. Pour les systèmes d'IA à haut risque intégrés à un produit, un marquage «CE» physique devrait être apposé, éventuellement complété par un marquage «CE» numérique. Pour les systèmes d'IA à haut risque fournis uniquement sous forme numérique, il convient d'utiliser un marquage «CE» numérique. Les États membres devraient s'abstenir de créer des entraves injustifiées à la mise sur le marché ou à la mise en service de systèmes d'IA à haut risque qui satisfont aux exigences fixées dans le présent règlement et portent le marquage «CE».

(130) Dans certaines conditions, la disponibilité rapide de technologies innovantes peut être cruciale pour la santé et la sécurité des personnes, pour la protection de l'environnement et la lutte contre le changement climatique et pour la société dans son ensemble. Il convient donc que, pour des motifs exceptionnels liés à la sécurité publique ou à la protection de la vie et de la santé des personnes physiques, à la protection de l'environnement et à la protection d'actifs industriels et d'infrastructures d'importance majeure, les autorités de surveillance du marché 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. Dans des situations dûment justifiées, prévues dans le présent règlement, les autorités répressives ou les autorités de protection civile

peuvent mettre en service un système d'IA à haut risque spécifique sans avoir obtenu l'autorisation de l'autorité de surveillance du marché, à condition que cette autorisation soit demandée sans retard injustifié pendant ou après l'utilisation.

(131) Afin de faciliter les travaux de la Commission et des États membres dans le domaine de l'IA et d'accroître la transparence à l'égard du public, les fournisseurs de systèmes d'IA à haut risque autres que ceux liés à des produits relevant du champ d'application de la législation d'harmonisation existante de l'Union en la matière, ainsi que les fournisseurs qui considèrent qu'un système d'IA inscrit sur la liste des cas d'utilisation à haut risque dans une annexe du présent règlement n'est pas à haut risque sur la base d'une dérogation, devraient être tenus de s'enregistrer eux-mêmes et d'enregistrer les informations relatives à leur système d'IA dans une base de données de l'UE, qui sera établie et gérée par la Commission. Avant d'utiliser un système d'IA inscrit sur la liste des cas d'utilisation à haut risque dans une annexe du présent règlement, les déployeurs de systèmes d'IA à haut risque qui sont des autorités, des agences ou des organismes publics devraient s'enregistrer dans une telle base de données et sélectionner le système qu'ils envisagent d'utiliser. Les autres déployeurs devraient être autorisés à le faire volontairement. Cette section de la base de données de l'UE devrait être accessible au public sans frais, et les informations qu'elle contient devraient être consultables grâce à une navigation aisée et être facilement compréhensibles et lisibles par machine. La base de données de l'UE devrait également être conviviale, par exemple en offrant des fonctionnalités de recherche, y compris par mots-clés, afin de permettre au grand public de trouver les informations pertinentes devant être transmises au moment de l'enregistrement des systèmes d'IA à haut risque et les informations sur le cas d'utilisation de systèmes d'IA à haut risque, énoncés dans une annexe du présent règlement, auquel les systèmes d'IA à haut risque correspondent. Toute modification substantielle de systèmes d'IA à haut risque devrait également être enregistrée dans la base de données de l'UE. En ce qui concerne les systèmes d'IA à haut risque dans les domaines des activités répressives, de la migration, de l'asile et de la gestion des contrôles aux frontières, les obligations en matière d'enregistrement devraient être remplies dans une section non publique sécurisée de la base de données de l'UE. L'accès à la section non publique sécurisée devrait être strictement réservé à la Commission, ainsi qu'aux autorités de surveillance du marché pour ce qui est de la section nationale de cette base de données les concernant. Les systèmes d'IA à haut risque dans le domaine des infrastructures critiques ne devraient être enregistrés qu'au niveau national. La Commission devrait faire fonction de responsable du traitement pour la base de données de l'UE, conformément au règlement (UE) 2018/1725. Afin de garantir que la base de données de l'UE soit pleinement opérationnelle une fois déployée, la procédure de création de la base de données devrait prévoir le développement de spécifications fonctionnelles par la Commission et un rapport d'audit indépendant. La Commission devrait tenir compte des risques liés à la cybersécurité dans l'accomplissement de ses missions en tant que responsable du traitement des données dans la base de données de l'UE. Afin de maximiser la disponibilité et l'utilisation de la base de données de l'UE, y compris les informations mises à disposition par son intermédiaire, la base de données de l'UE devrait être conforme aux exigences prévues par la directive (UE) 2019/882.

(132) Certains systèmes d'IA destinés à interagir avec des personnes physiques ou à générer du contenu peuvent présenter des risques spécifiques d'usurpation d'identité ou de tromperie, qu'ils soient ou non considérés comme étant à haut risque. Dans certaines circonstances,

l'utilisation de ces systèmes devrait donc être soumise à des obligations de transparence spécifiques sans préjudice des exigences et obligations relatives aux systèmes d'IA à haut risque et sous réserve d'exemptions ciblées destinées à tenir compte des besoins spécifiques des activités répressives. En particulier, les personnes physiques devraient être avisées qu'elles interagissent avec un système d'IA, sauf si cela ressort clairement du point de vue d'une personne physique normalement informée et raisonnablement attentive et avisée, compte tenu des circonstances et du contexte d'utilisation. Lors de la mise en œuvre de cette obligation, les caractéristiques des personnes physiques appartenant à des groupes vulnérables en raison de leur âge ou d'un handicap devraient être prises en compte dans la mesure où le système d'IA est destiné à interagir également avec ces groupes. En outre, les personnes physiques devraient être mises au courant lorsqu'elles sont exposées à des systèmes d'IA qui, en traitant leurs données biométriques, peuvent identifier ou déduire les émotions ou intentions de ces personnes ou les affecter à des catégories spécifiques. Ces catégories spécifiques peuvent avoir trait à des aspects tels que le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, les traits personnels, l'origine ethnique, les préférences et les intérêts personnels. Ces informations et notifications devraient être fournies dans des formats accessibles aux personnes handicapées.

(133) Divers systèmes d'IA peuvent générer de grandes quantités de contenu de synthèse qu'il devient de plus en plus difficile pour les êtres humains de distinguer du contenu authentique généré par des humains. La large disponibilité et les capacités croissantes de ces systèmes ont des conséquences importantes sur l'intégrité de l'écosystème informationnel et la confiance en celui-ci, ce qui pose de nouveaux risques de désinformation et de manipulation à grande échelle, de fraude, d'usurpation d'identité et de tromperie des consommateurs. Compte tenu de ces effets, du rythme rapide de l'évolution technologique et de la nécessité de nouvelles méthodes et techniques pour déterminer l'origine des informations, il convient d'exiger que les fournisseurs de ces systèmes intègrent des solutions techniques permettant le marquage dans un format lisible par machine et la détection du fait que les sorties ont été générées ou manipulées par un système d'IA, et non par un être humain. De telles techniques et méthodes devraient être aussi fiables, interopérables, efficaces et solides que la technologie le permet, et tenir compte des techniques disponibles ou d'une combinaison de ces techniques, telles que les filigranes, les identifications de métadonnées, les méthodes cryptographiques permettant de prouver la provenance et l'authenticité du contenu, les méthodes d'enregistrement, les empreintes digitales ou d'autres techniques, selon qu'il convient. Lorsqu'ils mettent en œuvre cette obligation, les fournisseurs devraient également tenir compte des spécificités et des limites des différents types de contenu, ainsi que des évolutions technologiques et du marché pertinentes dans le domaine, tels qu'elles ressortent de l'état de la technique généralement reconnu. Ces techniques et méthodes peuvent être mises en œuvre au niveau du système d'IA ou au niveau du modèle d'IA, y compris pour les modèles d'IA à usage général qui génèrent du contenu, ce qui facilitera l'accomplissement de cette obligation par le fournisseur en aval du système d'IA. Dans un souci de proportionnalité, il convient d'envisager que cette obligation de marquage ne s'applique pas aux systèmes d'IA qui remplissent une fonction d'assistance pour la mise en forme standard ou les systèmes d'IA qui ne modifient pas de manière substantielle les données d'entrée fournies par le déployeur ou leur sémantique.

(134) Outre les solutions techniques utilisées par les fournisseurs du système, les déployeurs qui se servent d'un système d'IA pour générer ou manipuler des images ou des contenus audio ou

vidéo présentant une ressemblance sensible avec des personnes, des objets, des lieux, des entités ou des événements existants et pouvant être perçu à tort par une personne comme authentiques ou véridiques (hypertrucages), devraient aussi déclarer de manière claire et reconnaissable que le contenu a été créé ou manipulé par une IA en étiquetant les sorties d'IA en conséquence et en mentionnant son origine artificielle. Le respect de cette obligation de transparence ne devrait pas être interprété comme indiquant que l'utilisation du système d'IA ou des sorties qu'il génère entrave le droit à la liberté d'expression et le droit à la liberté des arts et des sciences garantis par la Charte, en particulier lorsque le contenu fait partie d'un travail ou d'un programme manifestement créatif, satirique, artistique; de fiction ou analogue, sous réserve de garanties appropriées pour les droits et libertés de tiers. Dans ces cas, l'obligation de transparence s'appliquant aux hypertrucages au titre du présent règlement se limite à la divulgation de l'existence de tels contenus générés ou manipulés, d'une manière appropriée qui n'entrave pas l'affichage ou la jouissance de l'œuvre, y compris son exploitation et son utilisation normales, tout en préservant l'utilité et la qualité de l'œuvre. En outre, il convient d'envisager une obligation d'information similaire en ce qui concerne le texte généré ou manipulé par l'IA dans la mesure où celui-ci est publié dans le but d'informer le public sur des questions d'intérêt public, à moins que le contenu généré par l'IA n'ait fait l'objet d'un processus d'examen humain ou de contrôle éditorial et qu'une personne physique ou morale assume la responsabilité éditoriale pour la publication du contenu.

(135) Sans préjudice de la nature obligatoire et de la pleine applicabilité des obligations de transparence, la Commission peut également encourager et faciliter l'élaboration de codes de bonne pratique au niveau de l'Union afin de faciliter la mise en œuvre effective des obligations relatives à la détection et à l'étiquetage des contenus générés ou manipulés par une IA, y compris pour favoriser des modalités pratiques visant, selon qu'il convient, à rendre les mécanismes de détection accessibles et à faciliter la coopération avec d'autres acteurs tout au long de la chaîne de valeur, à diffuser les contenus ou à vérifier leur authenticité et leur provenance pour permettre au public de reconnaître efficacement les contenus générés par l'IA.

(136) Les obligations incombant aux fournisseurs et aux déployeurs de certains systèmes d'IA au titre du présent règlement afin de permettre la détection et la mention du fait que les sorties de ces systèmes sont générées ou manipulées par une IA revêtent une importance particulière pour faciliter la mise en œuvre effective du règlement (UE) 2022/2065. Cela vaut en particulier pour les obligations incombant aux fournisseurs de très grandes plateformes en ligne ou de très grands moteurs de recherche en ligne consistant à recenser et à atténuer les risques systémiques susceptibles de découler de la diffusion de contenus qui ont été générés ou manipulés par une IA, en particulier le risque d'effets négatifs réels ou prévisibles sur les processus démocratiques, le débat public et les processus électoraux, notamment par le biais de la désinformation. L'exigence relative à l'étiquetage des contenus générés par des systèmes d'IA au titre du présent règlement est sans préjudice de l'obligation prévue à l'article 16, paragraphe 6, du règlement (UE) 2022/2065 imposant aux fournisseurs de services d'hébergement de traiter les signalements de contenus illégaux qu'ils reçoivent au titre de l'article 16, paragraphe 1, dudit règlement, et elle ne devrait pas influencer l'évaluation et la décision quant à l'illégalité du contenu en question. Cette évaluation ne devrait être effectuée qu'au regard des règles régissant la légalité du contenu.

(137)Le respect des obligations de transparence applicables aux systèmes d'IA relevant du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système d'IA ou de ses sorties est licite en vertu du présent règlement ou d'autres actes législatifs de l'Union et des États membres et devrait être sans préjudice d'autres obligations de transparence pour les déployeurs de systèmes d'IA prévues par le droit de l'Union ou le droit national.

(138)L'IA est une famille de technologies en évolution rapide qui nécessite la mise en place d'un contrôle réglementaire et d'un espace sûr et contrôlé pour l'expérimentation, garantissant également une innovation responsable et l'intégration de garanties et de mesures d'atténuation des risques appropriées. Pour garantir un cadre juridique favorable à l'innovation, à l'épreuve du temps et résilient face aux perturbations, les États membres devraient veiller à ce que leurs autorités nationales compétentes mettent en place au moins un bac à sable réglementaire de l'IA au niveau national pour faciliter le développement et la mise à l'essai de systèmes d'IA innovants sous un contrôle réglementaire strict avant que ces systèmes ne soient mis sur le marché ou mis en service d'une autre manière. Les États membres pourraient également satisfaire à cette obligation en participant à des bacs à sable réglementaires déjà existants ou en établissant conjointement un bac à sable avec les autorités compétentes d'un ou de plusieurs États membres, pour autant que cette participation offre un niveau de couverture nationale équivalent pour les États membres participants. Les bacs à sable réglementaires de l'IA pourraient être mis en place sous forme physique, numérique ou hybride et admettre des produits tant physiques que numériques. Les autorités chargées de les mettre en place devraient également veiller à ce que les bacs à sable réglementaires de l'IA disposent des ressources appropriées pour assurer leur fonctionnement, y compris les ressources financières et humaines.

(139)Les bacs à sable réglementaires de l'IA devraient avoir pour objectif de favoriser l'innovation dans le domaine de l'IA en créant un environnement contrôlé d'expérimentation et d'essai au stade du développement et de la précommercialisation afin de garantir la conformité des systèmes d'IA innovants avec le présent règlement et d'autres dispositions pertinentes du droit de l'Union et du droit national. De plus, les bacs à sable réglementaires de l'IA devraient viser à renforcer la sécurité juridique pour les innovateurs ainsi que le contrôle et la compréhension, par les autorités compétentes, des possibilités, des risques émergents et des conséquences de l'utilisation de l'IA, de faciliter l'apprentissage réglementaire pour les autorités et les entreprises, y compris en vue d'ajustements futurs du cadre juridique, de soutenir la coopération et l'échange de bonnes pratiques avec les autorités participant au bac à sable réglementaire de l'IA, et d'accélérer l'accès aux marchés, notamment en supprimant les obstacles pour les PME, y compris les jeunes pousses. Les bacs à sable réglementaires de l'IA devraient être largement disponibles dans toute l'Union, et il convient de prêter une attention particulière à leur accessibilité pour les PME, y compris les jeunes pousses. La participation au bac à sable réglementaire de l'IA devrait se concentrer sur les questions qui créent une insécurité juridique pour les fournisseurs et les fournisseurs potentiels avant d'innover, d'expérimenter l'IA dans l'Union et de contribuer à un apprentissage réglementaire fondé sur des données probantes. La surveillance des systèmes d'IA dans le bac à sable réglementaire de l'IA devrait donc porter sur leur développement, leur entraînement, leur mise à l'essai et leur validation avant que les systèmes ne soient mis sur le marché ou mis en service, ainsi que sur la notion et la survenance de modifications substantielles

susceptibles de nécessiter une nouvelle procédure d'évaluation de la conformité. Tout risque important recensé lors du développement et de la mise à l'essai de ces systèmes d'IA devrait donner lieu à des mesures d'atténuation adéquates et, à défaut, à la suspension du processus de développement et d'essai. Au besoin, les autorités nationales compétentes mettant en place des bacs à sable réglementaires de l'IA devraient coopérer avec d'autres autorités concernées, y compris celles qui supervisent la protection des droits fondamentaux, et pourraient permettre la participation d'autres acteurs de l'écosystème de l'IA, tels que les organisations nationales ou européennes de normalisation, les organismes notifiés, les installations d'essai et d'expérimentation, les laboratoires de recherche et d'expérimentation, les pôles européens d'innovation numérique, ainsi que les parties prenantes et les organisations de la société civile concernées. Pour assurer une mise en œuvre uniforme dans toute l'Union et des économies d'échelle, il convient d'établir des règles communes pour la mise en place des bacs à sable réglementaires de l'IA ainsi qu'un cadre de coopération entre les autorités compétentes intervenant dans la surveillance des bacs à sable. Les bacs à sable réglementaires de l'IA établis en vertu du présent règlement devraient être sans préjudice d'autres actes législatifs autorisant la création d'autres bacs à sable en vue de garantir le respect de dispositions de droit autres que le présent règlement. Le cas échéant, les autorités compétentes concernées chargées de ces autres bacs à sable réglementaires devraient prendre en considération les avantages de l'utilisation de ces bacs à sable également aux fins d'assurer la conformité des systèmes d'IA avec le présent règlement. Sous réserve d'un accord entre les autorités nationales compétentes et les participants au bac à sable réglementaire de l'IA, il peut également être procédé à des essais en conditions réelles supervisés dans le cadre du bac à sable réglementaire de l'IA.

(140) Le présent règlement devrait constituer la base juridique pour l'utilisation, par les fournisseurs et fournisseurs potentiels du bac à sable réglementaire de l'IA, des données à caractère personnel collectées à d'autres fins pour le développement de certains systèmes d'IA d'intérêt public dans le cadre du bac à sable réglementaire de l'IA, uniquement dans des conditions déterminées, conformément à l'article 6, paragraphe 4, et à l'article 9, paragraphe 2, point g), du règlement (UE) 2016/679 et aux articles 5, 6 et 10 du règlement (UE) 2018/1725, et sans préjudice de l'article 4, paragraphe 2, et de l'article 10 de la directive (UE) 2016/680. Toutes les autres obligations des responsables du traitement et tous les autres droits des personnes concernées en vertu des règlements (UE) 2016/679 et (UE) 2018/1725 et de la directive (UE) 2016/680 restent applicables. En particulier, le présent règlement ne devrait pas constituer une base juridique au sens de l'article 22, paragraphe 2, point b), du règlement (UE) 2016/679 et de l'article 24, paragraphe 2, point b), du règlement (UE) 2018/1725. Les fournisseurs et fournisseurs potentiels participant au bac à sable réglementaire de l'IA devraient prévoir des garanties appropriées et coopérer avec les autorités compétentes, notamment en suivant leurs orientations et en agissant rapidement et de bonne foi pour atténuer adéquatement tout risque important recensé pour la sécurité, la santé et les droits fondamentaux susceptible de survenir au cours du développement, de la mise à l'essai et de l'expérimentation dans ledit bac à sable.

(141) Afin d'accélérer le processus de développement et la mise sur le marché des systèmes d'IA à haut risque énumérés dans une annexe du présent règlement, il importe que les fournisseurs ou fournisseurs potentiels de ces systèmes puissent également bénéficier d'un régime particulier pour soumettre ces systèmes à des essais en conditions réelles sans participer à un

bac à sable réglementaire de l'IA. Toutefois, dans de tels cas, compte tenu des conséquences possibles de ces essais sur des personnes physiques, il convient de veiller à ce que le présent règlement introduise des garanties et des conditions appropriées et suffisantes pour les fournisseurs ou fournisseurs potentiels. Ces garanties devraient comprendre, entre autres, une demande de consentement éclairé de la part des personnes physiques pour participer à des essais en conditions réelles, sauf en ce qui concerne les services répressifs lorsque la recherche d'un consentement éclairé empêcherait que le système d'IA ne soit mis à l'essai. Le consentement des participants à la participation à ces essais au titre du présent règlement est distinct et sans préjudice du consentement des personnes concernées au traitement de leurs données à caractère personnel en vertu de la législation applicable en matière de protection des données. Il importe également important de réduire les risques au minimum et de permettre aux autorités compétentes d'exercer un contrôle et, par conséquent, d'exiger des fournisseurs potentiels qu'ils disposent d'un plan d'essais en conditions réelles présenté à l'autorité de surveillance du marché compétente, d'enregistrer les essais dans des sections spécifiques de la base de données de l'UE, sous réserve de quelques exceptions limitées, de fixer des limitations de la période pendant laquelle les essais peuvent être menés et d'exiger des garanties supplémentaires pour les personnes appartenant à certains groupes vulnérables, ainsi qu'un accord écrit définissant les rôles et les responsabilités des fournisseurs potentiels et des déployeurs et établissant un contrôle effectif par le personnel compétent participant aux essais en conditions réelles. En outre, il convient d'envisager des garanties supplémentaires pour veiller à ce que les prédictions, recommandations ou décisions d'un système d'IA puissent être infirmées et ignorées de manière effective et à ce que les données à caractère personnel soient protégées et supprimées lorsque les personnes concernées ont retiré leur consentement à participer aux essais, sans qu'il soit porté atteinte aux droits dont elles disposent en tant que personnes concernées en vertu du droit de l'Union en matière de protection des données. En ce qui concerne le transfert de données, il convient en outre d'envisager que les données collectées et traitées aux fins des essais en conditions réelles ne soient transférées vers des pays tiers que lorsque des garanties appropriées et applicables en vertu du droit de l'Union sont en place, en particulier conformément aux bases pour le transfert de données à caractère personnel prévues par le droit de l'Union en matière de protection des données, et que des garanties appropriées soient mises en place pour les données à caractère non personnel conformément au droit de l'Union, notamment les règlements (UE) 2022/868 ([42]) et (UE) 2023/2854 ([43]) du Parlement européen et du Conseil.

(142) Afin de veiller à ce que l'IA engendre des résultats bénéfiques sur le plan social et environnemental, les États membres sont encouragés à soutenir et à promouvoir la recherche et le développement de solutions d'IA propices à tels résultats, telles que des solutions fondées sur l'IA destinées à renforcer l'accessibilité pour les personnes handicapées, à réduire les inégalités socio-économiques ou à atteindre les objectifs environnementaux, en y affectant des ressources suffisantes, y compris des financements publics et de l'Union, et, lorsqu'il convient et pour autant que les critères d'éligibilité et de sélection soient remplis, en envisageant des projets spécifiques qui poursuivent ces objectifs. Ces projets devraient être fondés sur le principe d'une coopération interdisciplinaire entre les développeurs d'IA, les experts en matière d'inégalité et de non-discrimination, d'accessibilité, de droits des consommateurs, de droits environnementaux et numériques, ainsi que les universitaires.

(143)Afin de promouvoir et de protéger l'innovation, il est important que les intérêts des PME, y compris les jeunes pousses, qui sont des fournisseurs ou des déployeurs de systèmes d'IA bénéficient d'une attention particulière. À cette fin, les États membres devraient prendre des initiatives à l'intention de ces opérateurs, notamment en matière de sensibilisation et de communication d'informations. Les États membres devraient fournir aux PME, y compris les jeunes pousses, qui ont leur siège social ou une succursale dans l'Union un accès prioritaire aux bacs à sable réglementaires de l'IA, à condition qu'elles remplissent les conditions d'éligibilité et les critères de sélection et sans exclure que d'autres fournisseurs et fournisseurs potentiels accèdent aux bacs à sable pour autant que les mêmes conditions et critères soient remplis. Les États membres devraient utiliser les canaux de communication existants, et en établissent de nouveaux s'il y a lieu, avec les PME, y compris les jeunes pousses, les déployeurs, d'autres innovateurs et, le cas échéant, les autorités publiques locales afin de soutenir les PME tout au long de leur trajectoire de développement en leur fournissant des orientations et en répondant à leurs questions concernant la mise en œuvre du présent règlement. Le cas échéant, ces canaux devraient collaborer pour créer des synergies et assurer la cohérence des orientations fournies aux PME, y compris les jeunes pousses, et aux déployeurs. En outre, les États membres devraient faciliter la participation des PME et d'autres parties concernées aux processus d'élaboration de la normalisation. Par ailleurs, les intérêts et les besoins spécifiques des fournisseurs qui sont des PME, y compris des jeunes pousses, devraient être pris en considération lorsque les organismes notifiés fixent les redevances d'évaluation de la conformité. La Commission devrait évaluer régulièrement les coûts de certification et de mise en conformité pour les PME, y compris les jeunes pousses, en menant des consultations transparentes, et devrait collaborer avec les États membres pour réduire ces coûts. Par exemple, les frais de traduction liés à la documentation obligatoire et à la communication avec les autorités peuvent représenter un coût important pour les fournisseurs et d'autres opérateurs, en particulier pour ceux de plus petite envergure. Les États membres devraient éventuellement veiller à ce qu'une des langues qu'ils choisissent et acceptent pour la documentation pertinente des fournisseurs et pour la communication avec les opérateurs soit une langue comprise par le plus grand nombre possible de déployeurs transfrontières. Afin de répondre aux besoins spécifiques des PME, y compris les jeunes pousses, la Commission devrait fournir des modèles normalisés pour les domaines qui relèvent du présent règlement, sur demande du Comité IA. En outre, la Commission devrait compléter les efforts déployés par les États membres en mettant en place une plateforme d'information unique présentant des informations facilement exploitables concernant le présent règlement à l'intention de tous les fournisseurs et déployeurs, en organisant des campagnes de communication appropriées pour faire connaître les obligations découlant du présent règlement, et en évaluant et en promouvant la convergence des bonnes pratiques dans les procédures de passation de marchés publics relatifs aux systèmes d'IA. Les entreprises qui jusqu'à récemment relevaient des «petites entreprises» au sens de l'annexe à la recommandation 2003/361/CE de la Commission ([44]) devraient avoir accès à ces mesures de soutien, étant donné que ces nouvelles moyennes entreprises peuvent parfois manquer des ressources juridiques et de la formation nécessaires pour avoir une bonne compréhension du présent règlement et en respecter les dispositions.

(144)Afin de promouvoir et de protéger l'innovation, la plateforme d'IA à la demande, ainsi que l'ensemble des programmes et projets de financement pertinents de l'Union, tels que le

programme pour une Europe numérique et Horizon Europe, mis en œuvre par la Commission et les États membres au niveau national ou de l'Union, selon qu'il convient, devraient contribuer à la réalisation des objectifs du présent règlement.

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

(146) En outre, au vu de la très petite taille de certains opérateurs et afin d'assurer la proportionnalité en ce qui concerne les coûts de l'innovation, il convient de permettre aux microentreprises de satisfaire à l'une des obligations les plus coûteuses, à savoir celle de mettre en place un système de gestion de la qualité, d'une manière simplifiée qui réduirait la charge administrative et les coûts pour ces entreprises sans affecter le niveau de protection et la nécessité de se conformer aux exigences applicables aux systèmes d'IA à haut risque. La Commission devrait élaborer des lignes directrices pour préciser quels éléments du système de gestion de la qualité les microentreprises doivent respecter dans le système simplifié.

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

(148) Le présent règlement devrait établir un cadre de gouvernance qui permette à la fois de coordonner et de soutenir l'application du présent règlement au niveau national, ainsi que de renforcer les capacités au niveau de l'Union et d'intégrer les parties prenantes dans le domaine de l'IA. La mise en œuvre et le contrôle de l'application effectifs du présent règlement requièrent un cadre de gouvernance qui permette de coordonner et de renforcer l'expertise centrale au niveau de l'Union. Le Bureau de l'IA a été créé par voie d'une décision de la Commission ([45]) et a pour mission d'approfondir l'expertise et de renforcer les capacités de l'Union dans le domaine de l'IA ainsi que de contribuer à la mise en œuvre de la législation de l'Union sur l'IA. Les États membres devraient faciliter l'accomplissement des missions du Bureau de l'IA en vue de soutenir le développement de l'expertise de l'Union et des capacités au niveau de l'Union et de renforcer le fonctionnement du marché unique numérique. En outre, il convient d'établir un Comité IA composé de représentants des États membres, un groupe scientifique visant à intégrer la communauté scientifique et un forum consultatif visant à recueillir les contributions des parties concernées en vue de la mise en

œuvre du présent règlement, au niveau de l'Union et au niveau national. Le développement de l'expertise et des capacités de l'Union devrait également consister à utiliser les ressources et l'expertise existantes, en particulier grâce à des synergies avec les structures établies dans le contexte de l'application au niveau de l'Union d'autres dispositions législatives et à des synergies avec des initiatives connexes au niveau de l'Union, telles que l'entreprise commune EuroHPC et les installations de mise à l'essai de l'IA et d'expérimentations relevant du programme pour une Europe numérique.

(149) Afin de faciliter une mise en œuvre aisée, efficace et harmonisée du présent règlement, il convient de créer un Comité IA. Ce Comité IA devrait tenir compte des différents intérêts de l'écosystème de l'IA et être composé de représentants des États membres. Le Comité IA devrait être chargé d'un certain nombre de tâches consultatives, parmi lesquelles la formulation d'avis, de recommandations, de conseils ou la contribution à des orientations sur des questions liées à la mise en œuvre du présent règlement, y compris sur les questions relatives à l'exécution, les spécifications techniques ou les normes existantes concernant les exigences établies dans le présent règlement, et la fourniture de conseils à la Commission et aux États membres ainsi qu'à leurs autorités nationales compétentes sur des questions spécifiques liées à l'IA. Afin d'offrir une certaine souplesse aux États membres dans la désignation de leurs représentants au sein du Comité IA, ces représentants peuvent être toute personne appartenant à des entités publiques qui devraient avoir les compétences et les pouvoirs nécessaires pour faciliter la coordination au niveau national et contribuer à l'accomplissement des tâches du Comité IA. Le Comité IA devrait établir deux sous-groupes permanents chargés de fournir une plateforme de coopération et d'échange entre les autorités de surveillance du marché et les autorités notifiantes sur des questions liées respectivement à la surveillance du marché et aux organismes notifiés. Le sous-groupe permanent pour la surveillance du marché devrait agir au titre de groupe de coopération administrative (ADCO) pour le présent règlement au sens de l'article 30 du règlement (UE) 2019/1020. Conformément à l'article 33 dudit règlement, la Commission devrait apporter son soutien aux activités du sous-groupe permanent en procédant à des évaluations ou à des études du marché, en particulier en vue de recenser les aspects du présent règlement appelant une coordination particulière urgente entre les autorités de surveillance du marché. Le Comité IA peut créer d'autres sous-groupes permanents ou temporaires, s'il y a lieu, afin d'examiner des questions spécifiques. Le Comité IA devrait également coopérer, lorsqu'il y a lieu, avec les organes, groupes d'experts et réseaux compétents de l'Union actifs dans le contexte de dispositions législatives pertinentes de l'Union, notamment ceux qui agissent au titre de la législation applicable de l'Union en matière de données, et de produits et services numériques.

(150) En vue d'assurer la participation des parties prenantes à la mise en œuvre et à l'application du présent règlement, il convient d'établir un forum consultatif chargé de conseiller le Comité IA et la Commission et de leur fournir une expertise technique. Afin d'assurer une représentation diversifiée et équilibrée des parties prenantes tenant compte des différents intérêts commerciaux et non commerciaux et, au sein de la catégorie des intérêts commerciaux, eu égard aux PME et autres entreprises, le forum consultatif devrait être composé, entre autres, de représentants du secteur, des jeunes pousses, des PME, du milieu universitaire, de la société civile, y compris les partenaires sociaux, ainsi que de l'Agence des droits fondamentaux, de l'ENISA, du Comité européen de normalisation (CEN), du Comité

européen de normalisation électrotechnique (CENELEC) et de l'Institut européen de normalisation des télécommunications (ETSI).

(151)Afin de soutenir la mise en œuvre et le contrôle du respect du présent règlement, en particulier les activités de suivi du Bureau de l'IA concernant les modèles d'IA à usage général, il convient d'établir un groupe scientifique composé d'experts indépendants. Les experts indépendants constituant le groupe scientifique devraient être choisis en fonction de leur expertise à la pointe des connaissances scientifiques ou techniques dans le domaine de l'IA. Ils devraient s'acquitter de leurs tâches avec impartialité et objectivité et veiller à la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités. Afin de permettre le renforcement des capacités nationales nécessaires au contrôle effectif du respect du présent règlement, les États membres devraient être en mesure de solliciter l'aide de la réserve d'experts constituant le groupe scientifique pour leurs activités répressives.

(152)Afin de soutenir un contrôle de l'application adéquat en ce qui concerne les systèmes d'IA et de renforcer les capacités des États membres, il convient de créer et de mettre à la disposition des États membres des structures de soutien de l'Union pour les essais en matière d'IA.

(153)Les États membres jouent un rôle clé dans l'application et le contrôle du respect du présent règlement. À cet égard, chaque État membre devrait désigner au moins une autorité notifiante et au moins une autorité de surveillance du marché en tant qu'autorités nationales compétentes chargées de contrôler l'application et la mise en œuvre du présent règlement. Les États membres peuvent décider de désigner une entité publique, quel qu'en soit le type, qui soit chargée d'exécuter les tâches des autorités nationales compétentes au sens du présent règlement, en fonction de leurs caractéristiques et besoins organisationnels nationaux spécifiques. Afin d'accroître l'efficacité de l'organisation du côté des États membres et de définir un point de contact unique avec le public et les homologues au niveau des États membres et de l'Union, chaque État membre devrait désigner une autorité de surveillance du marché pour tenir le rôle de point de contact unique.

(154)Les autorités nationales compétentes devraient exercer leurs pouvoirs de manière indépendante, impartiale et sans parti pris, afin de préserver les principes d'objectivité de leurs activités et de leurs tâches et d'assurer l'application et la mise en œuvre du présent règlement. Les membres de ces autorités devraient s'abstenir de toute action incompatible avec leurs fonctions et devraient être soumis aux règles de confidentialité prévues par le présent règlement.

(155)Afin de veiller à ce que les fournisseurs de systèmes d'IA à haut risque puissent prendre en considération l'expérience acquise dans l'utilisation de systèmes d'IA à haut risque pour améliorer leurs systèmes et le processus de conception et de développement, ou qu'ils puissent prendre d'éventuelles mesures correctives en temps utile, tous les fournisseurs devraient avoir mis en place un système de surveillance après commercialisation. Le cas échéant, la surveillance après commercialisation devrait comprendre une analyse de l'interaction avec d'autres systèmes d'IA, y compris d'autres dispositifs et logiciels. La surveillance après commercialisation ne devrait pas couvrir les données opérationnelles sensibles des utilisateurs de systèmes d'IA qui sont des autorités répressives. Ce système est aussi essentiel pour garantir que les risques potentiels découlant des systèmes d'IA qui continuent à «apprendre» après avoir été mis sur le marché ou mis en service puissent être

traités plus efficacement et en temps utile. Dans ce contexte, les fournisseurs devraient également être tenus de mettre en place un système pour signaler aux autorités compétentes tout incident grave résultant de l'utilisation de leurs systèmes d'IA, à savoir un incident ou un dysfonctionnement entraînant la mort ou une atteinte grave à la santé, une perturbation grave et irréversible de la gestion et de l'exploitation des infrastructures critiques, des infractions aux obligations découlant du droit de l'Union visant à protéger les droits fondamentaux ou une atteinte grave aux biens ou à l'environnement.

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

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

(158) Le droit de l'Union en matière de services financiers comprend des règles et des exigences en matière de gouvernance interne et de gestion des risques qui sont applicables aux établissements financiers réglementés dans le cadre de la fourniture de ces services, y compris lorsqu'ils font usage de systèmes d'IA. Afin d'assurer la cohérence de l'application et du contrôle du respect des obligations découlant du présent règlement et des règles et

exigences pertinentes prévues par les actes juridiques de l'Union sur les services financiers, les autorités compétentes chargées de la surveillance et du contrôle de l'application de ces actes juridiques, en particulier les autorités compétentes au sens du règlement (UE) nº 575/2013 du Parlement européen et du Conseil ([46]) et des directives 2008/48/CE ([47]), 2009/138/CE ([48]), 2013/36/UE ([49]), 2014/17/UE ([50]) et (UE) 2016/97 ([51]) du Parlement européen et du Conseil, devraient être désignées, dans les limites de leurs compétences respectives, comme les autorités compétentes aux fins de la surveillance de la mise en œuvre du présent règlement, y compris pour les activités de surveillance du marché, en ce qui concerne les systèmes d'IA fournis ou utilisés par des établissements financiers réglementés et surveillés, à moins que les États membres ne décident de désigner une autre autorité pour remplir ces tâches de surveillance du marché. Ces autorités compétentes devraient disposer, en vertu du présent règlement et du règlement (UE) 2019/1020, de tous les pouvoirs nécessaires pour faire respecter les exigences et obligations du présent règlement, y compris le pouvoir d'effectuer des activités de surveillance du marché ex post qui peuvent être intégrées, le cas échéant, dans leurs mécanismes et procédures de surveillance existants au titre du droit de l'Union en matière de services financiers. Il convient d'envisager que, lorsqu'elles agissent en tant qu'autorités de surveillance du marché au titre du présent règlement, les autorités nationales responsables de la surveillance des établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) nº 1024/2013 du Conseil ([52]), doivent communiquer sans délai à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt pour les missions de surveillance prudentielle de la Banque centrale européenne telles qu'elles sont définies dans ledit règlement. Pour renforcer encore la cohérence entre le présent règlement et les règles applicables aux établissements de crédit régis par la directive 2013/36/UE, il convient aussi d'intégrer certaines des obligations procédurales des fournisseurs en ce qui concerne la gestion des risques, la surveillance après commercialisation et la documentation dans les obligations et procédures existantes au titre de la directive 2013/36/UE. Afin d'éviter les chevauchements, des dérogations limitées devraient aussi être envisagées en ce qui concerne le système de gestion de la qualité des fournisseurs et l'obligation de suivi imposée aux déployeurs de systèmes d'IA à haut risque dans la mesure où les dispositions y afférentes s'appliquent aux établissements de crédit régis par la directive 2013/36/UE. Le même régime devrait s'appliquer aux entreprises d'assurance et de réassurance et aux sociétés holding d'assurance relevant de la directive 2009/138/CE, aux intermédiaires d'assurance relevant de la directive (UE) 2016/97, ainsi qu'aux autres types d'établissements financiers soumis à des exigences en matière de gouvernance, de dispositifs ou de processus internes établis en vertu des dispositions pertinentes du droit de l'Union en matière de services financiers afin d'assurer la cohérence et l'égalité de traitement dans le secteur financier.

(159) Chaque autorité de surveillance du marché chargée des systèmes d'IA à haut risque dans le domaine de la biométrie énumérés dans une annexe du présent règlement, dans la mesure où ces systèmes sont utilisés à des fins liées aux activités répressives, à la migration, à l'asile et à la gestion des contrôles aux frontières ou à l'administration de la justice et aux processus démocratiques, devrait disposer de pouvoirs effectifs en matière d'enquête et de mesures correctives, y compris au minimum le pouvoir d'obtenir l'accès à toutes les données à caractère personnel traitées et à toutes les informations nécessaires à l'accomplissement de

ses tâches. Les autorités de surveillance du marché devraient être en mesure d'exercer leurs pouvoirs en toute indépendance. Toute restriction de leur accès à des données opérationnelles sensibles au titre du présent règlement devrait être sans préjudice des pouvoirs qui leur sont conférés par la directive (UE) 2016/680. Aucune exclusion concernant la divulgation de données aux autorités nationales chargées de la protection des données au titre du présent règlement ne devrait avoir d'incidence sur les pouvoirs actuels ou futurs de ces autorités au-delà du champ d'application du présent règlement.

(160) Les autorités de surveillance du marché et la Commission devraient être en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener par les autorités de surveillance du marché ou par les autorités de surveillance du marché conjointement avec la Commission, visant à promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser et de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont recensés comme présentant un risque grave dans au moins deux États membres. Les activités conjointes visant à promouvoir le respect de la législation devraient être menées conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA devrait assurer la coordination centrale des enquêtes conjointes.

(161) Il est nécessaire de clarifier les responsabilités et les compétences au niveau de l'Union et au niveau national en ce qui concerne les systèmes d'IA qui reposent sur des modèles d'IA à usage général. Afin d'éviter les chevauchements de compétences, lorsqu'un système est fondé sur un modèle d'IA à usage général et que le modèle et le système sont fournis par le même fournisseur, la surveillance devrait avoir lieu au niveau de l'Union par l'intermédiaire du Bureau de l'IA, qui devrait disposer à cette fin des pouvoirs d'une autorité de surveillance du marché au sens du règlement (UE) 2019/1020. Dans tous les autres cas, les autorités nationales de surveillance du marché demeurent chargées de la surveillance des systèmes d'IA. Toutefois, pour les systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque, les autorités de surveillance du marché devraient coopérer avec le Bureau de l'IA pour mener les évaluations de la conformité, et informer le Comité IA et les autres autorités de surveillance du marché en conséquence. En outre, toute autorité de surveillance du marché devrait être en mesure de solliciter l'assistance du Bureau de l'IA lorsqu'elle n'est pas en mesure de conclure une enquête sur un système d'IA à haut risque parce qu'elle ne peut accéder à certaines informations liées au modèle d'IA à usage général sur lequel repose ce système. Dans de tels cas, la procédure relative à l'assistance mutuelle pour les cas transfrontières prévue au chapitre VI du règlement (UE) 2019/1020 devrait s'appliquer mutatis mutandis.

(162) Afin de tirer le meilleur parti de l'expertise centralisée de l'Union et des synergies au niveau de l'Union, les pouvoirs de surveillance et de contrôle du respect des obligations incombant aux fournisseurs de modèles d'IA à usage général devraient relever de la compétence de la Commission. Le Bureau de l'IA devrait être en mesure de prendre toutes les mesures nécessaires pour contrôler la mise en œuvre effective du présent règlement en ce qui concerne les modèles d'IA à usage général. Il devrait être en mesure d'enquêter sur d'éventuelles infractions aux règles incombant aux fournisseurs de modèles d'IA à usage général, aussi bien de sa propre initiative, selon les résultats de ses activités de surveillance, ou sur demande des autorités de surveillance du marché conformément aux conditions prévues par le présent

règlement. Afin de contribuer à une surveillance effective par le Bureau de l'IA, celui-ci devrait donner la possibilité aux fournisseurs en aval d'introduire des réclamations concernant d'éventuelles infractions aux règles relatives aux fournisseurs de modèles et systèmes d'IA à usage général.

(163) En vue de compléter les systèmes de gouvernance des modèles d'IA à usage général, le groupe scientifique devrait soutenir les activités de surveillance du Bureau de l'IA et pourrait, dans certains cas, soumettre au Bureau de l'IA des alertes qualifiées qui déclenchent des mesures de suivi telles que des enquêtes. Cela devrait être le cas lorsque le groupe scientifique a des raisons de soupçonner qu'un modèle d'IA à usage général présente un risque concret et identifiable au niveau de l'Union. Cela devrait aussi être le cas lorsque le groupe scientifique a des raisons de soupçonner qu'un modèle d'IA à usage général remplit les critères qui conduiraient à une classification en tant que modèle d'IA à usage général présentant un risque systémique. Afin que le groupe scientifique dispose des informations nécessaires à l'exécution de ces tâches, il devrait exister un mécanisme permettant au groupe scientifique de demander à la Commission d'exiger du fournisseur qu'il fournisse des documents ou des informations.

(164) Le Bureau de l'IA devrait être en mesure de prendre les mesures nécessaires pour contrôler la mise en œuvre effective et le respect des obligations incombant aux fournisseurs de modèles d'IA à usage général énoncées dans le présent règlement. Le Bureau de l'IA devrait être en mesure d'enquêter sur d'éventuelles infractions conformément aux pouvoirs qui lui sont conférés au titre du présent règlement, y compris en exigeant des documents et des informations, en réalisant des évaluations, ainsi qu'en exigeant que des mesures soient prises par les fournisseurs de modèles d'IA à usage général. Lors de la réalisation des évaluations, afin de tirer parti d'une expertise indépendante, le Bureau de l'IA devrait pouvoir faire appel à des experts indépendants pour réaliser les évaluations en son nom. Le respect des obligations devrait pouvoir être imposé, entre autres, par des demandes de prendre des mesures appropriées, y compris des mesures d'atténuation des risques dans le cas de risques systémiques recensés, ainsi qu'en restreignant la mise à disposition du modèle sur le marché, en le retirant ou en le rappelant. À titre de garantie, lorsque cela est nécessaire en sus des droits procéduraux prévus par le présent règlement, les fournisseurs de modèles d'IA à usage général devraient jouir des droits procéduraux prévus à l'article 18 du règlement (UE) 2019/1020, qui devraient s'appliquer mutatis mutandis, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

(165) Le développement de systèmes d'IA autres que les systèmes d'IA à haut risque dans le respect des exigences du présent règlement peut conduire à une plus large adoption d'une IA éthique et digne de confiance dans l'Union. Les fournisseurs de systèmes d'IA qui ne sont pas à haut risque devraient être encouragés à établir des codes de conduite, accompagnés de mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire de tout ou partie des exigences obligatoires applicables aux systèmes d'IA à haut risque, adaptés en fonction de la destination des systèmes et des risques plus faibles encourus et tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur, tels que les cartes modèles et les fiches de données. Les fournisseurs et, le cas échéant, les déployeurs de tous les systèmes d'IA, à haut risque ou non, et modèles d'IA devraient aussi être encouragés à appliquer sur une base volontaire des exigences supplémentaires liées, par exemple, aux

éléments des lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance, à la durabilité environnementale, aux mesures relatives à la maîtrise de l'IA, à la conception et au développement inclusifs et diversifiés des systèmes d'IA, y compris en prêtant attention aux personnes vulnérables et à l'accessibilité pour les personnes handicapées, à la participation des parties prenantes avec la contribution, le cas échéant, de parties prenantes concernées telles que les organisations d'entreprises et de la société civile, le milieu universitaire, les organismes de recherche, les syndicats et les organisations de protection des consommateurs à la conception et au développement des systèmes d'IA, ainsi qu'à la diversité des équipes de développement, y compris l'équilibre hommes-femmes. Afin que les codes de conduite volontaires portent leurs effets, ils devraient s'appuyer sur des objectifs clairs et des indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs. Ils devraient également être élaborés de manière inclusive, selon qu'il convient, avec la participation des parties prenantes concernées telles que les organisations d'entreprises et de la société civile, le milieu universitaire, les organismes de recherche, les syndicats et les organisations de protection des consommateurs. La Commission peut élaborer des initiatives, y compris de nature sectorielle, pour faciliter la suppression des obstacles techniques entravant l'échange transfrontière de données pour le développement de l'IA, notamment en ce qui concerne l'infrastructure d'accès aux données et l'interopérabilité sémantique et technique des différents types de données.

(166) Il importe que les systèmes d'IA liés à des produits qui ne sont pas à haut risque au titre du présent règlement et qui ne sont donc pas tenus d'être conformes aux exigences énoncées pour les systèmes d'IA à haut risque soient néanmoins sûrs lorsqu'ils sont mis sur le marché ou mis en service. Pour contribuer à cet objectif, l'application du règlement (UE) 2023/988 du Parlement européen et du Conseil ([53]) constituerait un filet de sécurité.

(167) Afin d'assurer une coopération constructive et en toute confiance entre les autorités compétentes au niveau de l'Union et au niveau national, toutes les parties intervenant dans l'application du présent règlement devraient respecter la confidentialité des informations et des données obtenues dans le cadre de l'exécution de leurs tâches, conformément au droit de l'Union et au droit national. Elles devraient s'acquitter de leurs tâches et activités de manière à protéger, en particulier, les droits de propriété intellectuelle, les informations commerciales confidentielles et les secrets d'affaires, la mise en œuvre effective du présent règlement, les intérêts en matière de sécurité nationale et publique, l'intégrité des procédures pénales et administratives et l'intégrité des informations classifiées.

(168) Le respect des dispositions du présent règlement devrait pouvoir être imposé au moyen de sanctions et d'autres mesures d'exécution. Les États membres devraient prendre toutes les mesures nécessaires pour que les dispositions du présent règlement soient mises en œuvre et, notamment, prévoir des sanctions effectives, proportionnées et dissuasives en cas de violation de ces dispositions, et dans le respect du principe non bis in idem. Afin de renforcer et d'harmoniser les sanctions administratives applicables en cas de violation du présent règlement, il convient d'établir le montant maximal pour la fixation des amendes administratives pour certaines infractions spécifiques. Pour évaluer le montant des amendes, les États membres devraient, dans chaque cas d'espèce, tenir compte de toutes les caractéristiques propres à la situation spécifique, en prenant notamment en considération la nature, la gravité et la durée de l'infraction et ses conséquences, ainsi que la taille du

fournisseur, en particulier s'il s'agit d'une PME, y compris les jeunes pousses. Le Contrôleur européen de la protection des données devrait avoir le pouvoir d'infliger des amendes aux institutions, agences et organes de l'Union relevant du présent règlement.

(169) Le respect des obligations incombant aux fournisseurs de modèles d'IA à usage général au titre du présent règlement devrait pouvoir être imposé, entre autres, au moyen d'amendes. À cette fin, des niveaux appropriés d'amendes devraient également être fixés pour les infractions à ces obligations, y compris le non-respect de mesures demandées par la Commission en vertu au présent règlement, sous réserve de délais de prescription appropriés conformément du principe de proportionnalité. Toutes les décisions prises par la Commission au titre du présent règlement sont soumises au contrôle de la Cour de justice de l'Union européenne conformément au traité sur le fonctionnement de l'Union européenne, y compris la compétence de pleine juridiction de la Cour de justice en ce qui concerne les sanctions en application de l'article 261 du traité sur le fonctionnement de l'Union européenne.

(170) Le droit de l'Union et le droit national prévoient déjà des voies de recours effectives pour les personnes physiques et morales qui subissent une atteinte à leurs droits et libertés en raison de l'utilisation de systèmes d'IA. Sans préjudice de ces recours, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement devrait avoir le droit d'introduire une réclamation auprès de l'autorité de surveillance du marché concernée.

(171) Les personnes concernées devraient avoir le droit d'obtenir une explication lorsque la décision d'un déployeur est principalement fondée sur les sorties de certains systèmes d'IA à haut risque qui relèvent du champ d'application du présent règlement et lorsque cette décision produit des effets juridiques ou cause un préjudice important de façon similaire à ces personnes d'une manière qu'elles considèrent comme ayant une incidence négative sur leur santé, leur sécurité ou leurs droits fondamentaux. Cette explication devrait être claire et pertinente, et constituer une base à partir de laquelle les personnes concernées peuvent exercer leurs droits. Le droit d'obtenir une explication ne devrait pas s'appliquer à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions découlent du droit de l'Union ou du droit national et ne devrait s'appliquer que dans la mesure où ce droit n'est pas déjà prévu par le droit de l'Union.

(172) Les personnes agissant en tant que lanceurs d'alerte eu égard à des infractions au présent règlement devraient être protégées en vertu du droit de l'Union. La directive (UE) 2019/1937 du Parlement européen et du Conseil ([54]) devrait donc s'appliquer aux signalements d'infractions au présent règlement et à la protection des personnes signalant ces infractions.

(173) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, le pouvoir d'adopter des actes conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne devrait être délégué à la Commission pour lui permettre de modifier les conditions dans lesquelles un système d'IA ne doit pas être considéré comme étant à haut risque, la liste des systèmes d'IA à haut risque, les dispositions relatives à la documentation technique, le contenu de la déclaration «UE» de conformité, les dispositions relatives aux procédures d'évaluation de la conformité, les dispositions établissant les systèmes d'IA à haut risque auxquels devrait s'appliquer la procédure d'évaluation de la conformité fondée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique, le seuil, les critères de référence et les indicateurs, y compris en complétant ces

critères de référence et indicateurs, dans les règles de classification des modèles d'IA à usage général présentant un risque systémique, les critères de désignation des modèles d'IA à usage général présentant un risque systémique, la documentation technique destinée aux fournisseurs de modèles d'IA à usage général et les informations relatives à la transparence pour les fournisseurs de modèles d'IA à usage général. Il importe particulièrement que la Commission procède aux consultations appropriées durant son travail préparatoire, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer» ([55]). En particulier, afin d'assurer une participation égale à la préparation des actes délégués, le Parlement européen et le Conseil reçoivent tous les documents en même temps que les experts des États membres, et leurs experts ont systématiquement accès aux réunions des groupes d'experts de la Commission participant à la préparation des actes délégués.

(174) Compte tenu de l'évolution rapide des technologies et de l'expertise technique requise aux fins de la bonne application du présent règlement, la Commission devrait évaluer et réexaminer le présent règlement au plus tard le 2 août 2029 et tous les quatre ans par la suite, et faire rapport au Parlement européen et au Conseil. En outre, en tenant compte des conséquences sur le champ d'application du présent règlement, la Commission devrait procéder à une évaluation de la nécessité de modifier une fois par an la liste des systèmes d'IA à haut risque et la liste des pratiques interdites. En outre, au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission devrait évaluer la nécessité de modifier les rubriques de la liste des domaines à haut risque figurant à l'annexe du présent règlement, les systèmes d'IA relevant des obligations de transparence, l'efficacité du système de surveillance et de gouvernance ainsi que l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, y compris la nécessité de mesures ou d'actions supplémentaires, et faire rapport au Parlement européen et au Conseil. Enfin, au plus tard le 2 août 2028 et tous les trois ans par la suite, la Commission devrait évaluer l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées pour les systèmes d'IA à haut risque dans le cas des systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour de tels systèmes d'IA.

(175) Afin de garantir des conditions uniformes de mise en œuvre du présent règlement, il convient de conférer des compétences d'exécution à la Commission. Ces compétences devraient être exercées en conformité avec le règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([56]).

(176) Étant donné que l'objectif du présent règlement, à savoir améliorer le fonctionnement du marché intérieur et promouvoir l'adoption d'une IA axée sur l'humain et digne de confiance tout en garantissant un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux consacrés dans la Charte, y compris la démocratie, l'état de droit et la protection de l'environnement, contre les effets néfastes des systèmes d'IA dans l'Union, et en soutenant l'innovation, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison des dimensions et des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité

énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(177) Afin d'assurer la sécurité juridique, de veiller à ce que les opérateurs disposent d'une période d'adaptation appropriée et d'éviter toute perturbation du marché, y compris en assurant la continuité de l'utilisation des systèmes d'IA, il convient que le présent règlement s'applique aux systèmes d'IA à haut risque qui ont été mis sur le marché ou mis en service avant la date générale d'application de celui-ci, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leur conception ou de leur destination. Il convient de préciser qu'à cet égard, la notion d'importante modification devrait être comprise comme équivalente sur le fond à celle de modification substantielle, qui est utilisée uniquement en ce qui concerne les systèmes d'IA à haut risque au titre du présent règlement. À titre exceptionnel et compte tenu de l'obligation de rendre des comptes au public, les exploitants de systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe du présent règlement et les exploitants de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques devraient prendre les mesures nécessaires pour se conformer aux exigences du présent règlement, respectivement, d'ici à la fin de 2030 et au plus tard le 2 août 2030.

(178) Les fournisseurs de systèmes d'IA à haut risque sont encouragés à commencer à se conformer, sur une base volontaire, aux obligations pertinentes du présent règlement dès la période transitoire.

(179) Le présent règlement devrait s'appliquer à partir du 2 août 2026. Toutefois, compte tenu du risque inacceptable associé à certaines utilisations de l'IA, les interdictions ainsi que les dispositions générales du présent règlement devraient déjà s'appliquer à compter du 2 février 2025. Si le plein effet de ces interdictions découle de la mise en place de la gouvernance et du contrôle du respect du présent règlement, il importe d'anticiper l'application des interdictions afin de tenir compte des risques inacceptables et d'avoir un effet sur d'autres procédures, par exemple en droit civil. En outre, l'infrastructure liée à la gouvernance et au système d'évaluation de la conformité devrait être opérationnelle avant le 2 août 2026, et les dispositions relatives aux organismes notifiés et à la structure de gouvernance devraient donc s'appliquer à compter du 2 août 2025. Compte tenu du rythme rapide des avancées technologiques et de l'adoption des modèles d'IA à usage général, les obligations incombant aux fournisseurs de modèles d'IA à usage général devraient s'appliquer à compter du 2 août 2025. Les codes de bonne pratique devraient être prêts au plus tard le 2 mai 2025 afin de permettre aux fournisseurs de démontrer leur conformité à temps. Le Bureau de l'IA devrait veiller à ce que les règles et procédures de classification soient à jour des évolutions technologiques. En outre, les États membres devraient définir et notifier à la Commission les règles relatives aux sanctions, y compris les amendes administratives, et veiller à ce qu'elles soient correctement et efficacement mises en œuvre à la date d'application du présent règlement. Par conséquent, les dispositions relatives aux sanctions devraient s'appliquer à compter du 2 août 2025.

(180) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphes 1 et 2, du règlement (UE) 2018/1725 et ont rendu leur avis conjoint le 18 juin 2021,

ONT ADOPTÉ LE PRÉSENT RÈGLEMENT:

# CHAPITRE I

# DISPOSITIONS GÉNÉRALES

*Article premier*

## Objet

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

2. Le présent règlement établit:

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

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

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

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

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

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

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

*Article 2*

## Champ d'application

1. Le présent règlement s'applique:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 3*

**Définitions**

Aux fins du présent règlement, on entend par:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

45) «autorités répressives»,

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

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

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

47) «Bureau de l'IA», la fonction de la Commission consistant à contribuer à la mise en œuvre, au suivi et à la surveillance des systèmes d'IA et de modèles d'IA à usage général et de la

gouvernance de l'IA, établi par la décision de la Commission du 24 janvier 2024; les références faites au Bureau de l'IA dans le présent règlement s'entendent comme faites à la Commission;

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

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

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

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

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

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

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

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

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

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

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

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

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

57) «essais en conditions réelles», les essais temporaires d'un système d'IA aux fins de sa destination en conditions réelles en dehors d'un laboratoire ou d'un environnement simulé d'une autre manière, visant à recueillir des données fiables et solides et à évaluer et vérifier la

conformité du système d'IA aux exigences du présent règlement; les essais en conditions réelles ne remplissent pas les conditions pour constituer une mise sur le marché ni une mise en service du système d'IA au sens du présent règlement, pour autant que toutes les conditions prévues à l'article 57 ou à l'article 60 soient remplies;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 4*

**Maîtrise de l'IA**

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

## CHAPITRE II
## PRATIQUES INTERDITES EN MATIÈRE D'IA

*Article 5*

**Pratiques interdites en matière d'IA**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'autorité judiciaire compétente ou une autorité administrative indépendante dont la décision est contraignante n'accorde l'autorisation que si elle estime, sur la base d'éléments objectifs ou d'indications claires qui lui sont présentés, que l'utilisation du système d'identification biométrique à distance en temps réel concerné est nécessaire et proportionnée à la réalisation de l'un des objectifs énumérés au paragraphe 1, premier alinéa, point h), tels qu'indiqués dans la

demande et, en particulier, que cette utilisation reste limitée au strict nécessaire dans le temps et du point de vue de la portée géographique et personnelle. Lorsqu'elle statue sur la demande, cette autorité tient compte des éléments visés au paragraphe 2. Aucune décision produisant des effets juridiques défavorables à l'égard d'une personne ne peut être prise sur la seule base de la sortie du système d'identification biométrique à distance «en temps réel».

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

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

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

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

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

## CHAPITRE III

## SYSTÈMES D'IA À HAUT RISQUE

## *SECTION 1*

## *Classification de systèmes d'IA comme systèmes à haut risque*

*Article 6*

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Après consultation du Comité européen de l'intelligence artificielle (ci-après dénommé «Comité IA»), et au plus tard le 2 février 2026, la Commission fournit des lignes directrices

précisant la mise en œuvre pratique du présent article, conformément à l'article 96, assorties d'une liste exhaustive d'exemples pratiques de cas d'utilisation de systèmes d'IA qui sont à haut risque et de cas d'utilisation qui ne le sont pas.

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

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

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

*Article 7*

**Modifications de l'annexe III**

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

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

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

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

a) la destination du système d'IA;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## *SECTION 2*

## *Exigences applicables aux systèmes d'IA à haut risque*

### *Article 8*

### Respect des exigences

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

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

*Article 9*

**Système de gestion des risques**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 10*

**Données et gouvernance des données**

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

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

a) les choix de conception pertinents;

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

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

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

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

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

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

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

3. Les jeux de données d'entraînement, de validation et de test sont pertinents, suffisamment représentatifs et, dans toute la mesure possible, exempts d'erreurs et complets au regard de la destination. Ils possèdent les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes ou groupes de personnes à l'égard desquels le système d'IA à haut risque est destiné à être utilisé. Ces caractéristiques des jeux de données peuvent être remplies au niveau des jeux de données pris individuellement ou d'une combinaison de ceux-ci.

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

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

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

b) les catégories particulières de données à caractère personnel sont soumises à des limitations techniques relatives à la réutilisation des données à caractère personnel, ainsi qu'aux mesures

les plus avancées en matière de sécurité et de protection de la vie privée, y compris la pseudonymisation;

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

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

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

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

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

*Article 11*

**Documentation technique**

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

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

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

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

*Article 12*

**Enregistrement**

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

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

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

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

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

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

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

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

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

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

*Article 13*

**Transparence et fourniture d'informations aux déployeurs**

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

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

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

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

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

i) sa destination;

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

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

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

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

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

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

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

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

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

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

*Article 14*

**Contrôle humain**

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 15*

**Exactitude, robustesse et cybersécurité**

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

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

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

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

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

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

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

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

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

## *SECTION 3*

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

### *Article 16*

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

Les fournisseurs de systèmes d'IA à haut risque:

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

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

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

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

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

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

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

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

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

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

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

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

*Article 17*

**Système de gestion de la qualité**

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

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

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

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

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

être réalisées;

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

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

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

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

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

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

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

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

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

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

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

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

*Article 18*

**Conservation des documents**

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

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

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

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

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

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

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

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

*Article 19*

**Journaux générés automatiquement**

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

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

*Article 20*

**Mesures corrective et devoir d'information**

1. Les fournisseurs de systèmes d'IA à haut risque qui considèrent ou ont des raisons de considérer qu'un système d'IA à haut risque qu'ils ont mis sur le marché ou mis en service n'est pas conforme au présent règlement prennent immédiatement les mesures correctives nécessaires pour le mettre en conformité, le retirer, le désactiver ou le rappeler, selon le cas. Ils informent les

distributeurs du système d'IA à haut risque concerné et, le cas échéant, les déployeurs, le mandataire et les importateurs en conséquence.

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

*Article 21*

**Coopération avec les autorités compétentes**

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

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

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

*Article 22*

**Mandataires des fournisseurs de systèmes d'IA à haut risque**

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

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

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

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

b) tenir à la disposition des autorités compétentes et des autorités ou organismes nationaux visés à l'article 74, paragraphe 10, pendant une période de dix ans après la mise sur le marché ou la mise en service du système d'IA à haut risque, les coordonnées du fournisseur ayant désigné le

mandataire, une copie de la déclaration UE de conformité visée à l'article 47, la documentation technique et, le cas échéant, le certificat délivré par l'organisme notifié;

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

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

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

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

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

*Article 23*

**Obligations des importateurs**

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

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

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

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

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

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

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

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

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

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

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

*Article 24*

**Obligations des distributeurs**

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

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

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

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

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

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

*Article 25*

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

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

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

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

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

2. Lorsque les circonstances visées au paragraphe 1, se produisent, le fournisseur qui a initialement mis sur le marché ou mis en service le système d'IA n'est plus considéré comme un fournisseur de ce système d'IA spécifique aux fins du présent règlement. Ce fournisseur initial coopère étroitement avec les nouveaux fournisseurs et met à disposition les informations nécessaires et fournit l'accès technique raisonnablement attendu et toute autre assistance nécessaire au respect des obligations énoncées dans le présent règlement, en particulier en ce qui concerne la conformité avec l'évaluation de la conformité des systèmes d'IA à haut risque. Le présent paragraphe ne s'applique pas dans les cas où le fournisseur initial a clairement précisé que son système d'IA ne doit pas être transformé en un système d'IA à haut risque et ne relève donc pas de l'obligation relative à la remise de la documentation.

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

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

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

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

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

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

*Article 26*

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

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

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

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

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

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

le fournisseur, l'article 73 s'applique mutatis mutandis. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs de systèmes d'IA qui sont des autorités répressives.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 27*

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

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

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

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

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

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

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

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

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

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

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

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

## *SECTION 4*

## *Autorités notifiantes et organismes notifiés*

### *Article 28*

### Autorités notifiantes

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

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

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

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

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

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

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

*Article 29*

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

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

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

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

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

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

*Article 30*

**Procédure de notification**

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

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

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

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

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

*Article 31*

**Exigences concernant les organismes notifiés**

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

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

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

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

fonctionnement de l'organisme d'évaluation de la conformité ou l'utilisation de ces systèmes d'IA à haut risque à des fins personnelles.

5. L'organisme d'évaluation de la conformité, ses cadres supérieurs et le personnel chargé d'exécuter ses tâches d'évaluation de la conformité ne participent pas directement à la conception, au développement, à la commercialisation ou à l'utilisation de systèmes d'IA à haut risque, pas plus qu'ils ne représentent les parties engagées dans ces activités. Ils n'exercent aucune activité susceptible d'entrer en conflit avec leur indépendance de jugement ou leur intégrité en ce qui concerne les activités d'évaluation de la conformité pour lesquelles ils sont notifiés. Cela s'applique en particulier aux services de conseil.

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

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

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

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

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

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

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

*Article 32*

**Présomption de conformité avec les exigences concernant les organismes notifiés**

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

*Article 33*

**Filiales des organismes notifiés et sous-traitance**

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

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

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

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

*Article 34*

**Obligations opérationnelles des organismes notifiés**

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

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

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

*Article 35*

**Numéros d'identification et listes des organismes notifiés**

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

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

*Article 36*

**Modifications apportées aux notifications**

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

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

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

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

4. Lorsqu'une autorité notifiante a des raisons suffisantes de considérer qu'un organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, l'autorité notifiante procède sans retard à une enquête avec la plus grande diligence. Dans ce contexte, elle informe l'organisme notifié concerné des objections soulevées et lui donne la possibilité de faire connaître son point de vue. Si l'autorité notifiante conclut que l'organisme notifié ne répond plus aux exigences définies à l'article 31, ou qu'il ne s'acquitte pas de ses obligations, elle soumet la désignation à des restrictions, la suspend ou la retire, selon le cas, en fonction de la gravité du manquement. Elle en informe immédiatement la Commission et les autres États membres.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 37*

**Contestation de la compétence des organismes notifiés**

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

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

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

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

*Article 38*

**Coordination des organismes notifiés**

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

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

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

*Article 39*

**Organismes d'évaluation de la conformité de pays tiers**

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

## *SECTION 5*

## *Normes, évaluation de la conformité, certificats, enregistrement*

*Article 40*

### Normes harmonisées et travaux de normalisation

1. Les systèmes d'IA à haut risque ou les modèles d'IA à usage général conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* conformément au règlement (UE) nº 1025/2012 sont présumés conformes aux exigences visées à la section 2 du présent chapitre ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, du présent règlement, dans la mesure où ces exigences ou obligations sont couvertes par ces normes.

2. Conformément à l'article 10 du règlement (UE) nº 1025/2012, la Commission présente sans retard injustifié des demandes de normalisation couvrant toutes les exigences énoncées à la section 2 du présent chapitre et, le cas échéant, les demandes de normalisation couvrant les obligations énoncées au chapitre V, sections 2 et 3, du présent règlement. La demande de normalisation inclut également une demande de livrables sur les processus de déclaration et de documentation afin d'améliorer les performances des systèmes d'IA en matière de ressources, telles que la réduction de la consommation d'énergie et d'autres ressources par le système d'IA à haut risque au cours de son cycle de vie, et sur le développement économe en énergie de modèles d'IA à usage général. Lors de la préparation d'une demande de normalisation, la Commission consulte le Comité IA et les parties prenantes concernées, y compris le forum consultatif.

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

La Commission demande aux organisations européennes de normalisation de fournir la preuve qu'elles mettent tout en œuvre pour atteindre les objectifs visés aux premier et deuxième alinéas du présent paragraphe, conformément à l'article 24 du règlement (UE) nº 1025/2012.

3. Les participants au processus de normalisation s'efforcent de favoriser les investissements et l'innovation dans le domaine de l'IA, y compris en renforçant la sécurité juridique, ainsi que la compétitivité et la croissance du marché de l'Union, de contribuer à renforcer la coopération mondiale en faveur d'une normalisation en tenant compte des normes internationales existantes dans le domaine de l'IA qui sont conformes aux valeurs et aux intérêts de l'Union et aux droits fondamentaux, et de renforcer la gouvernance multipartite en veillant à une représentation équilibrée des intérêts et à la participation effective de toutes les parties prenantes concernées conformément aux articles 5, 6 et 7 du règlement (UE) nº 1025/2012.

*Article 41*

### Spécifications communes

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

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

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

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

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

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

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

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

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

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

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

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

5. Lorsque les fournisseurs de systèmes d'IA à haut risque ou de modèles d'IA à usage général ne respectent pas les spécifications communes visées au paragraphe 1, ils justifient dûment avoir adopté des solutions techniques qui satisfont aux exigences visées à la section 2 du présent chapitre

ou, le cas échéant, aux obligations énoncées au chapitre V, sections 2 et 3, à un niveau au moins équivalent auxdites spécifications.

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

*Article 42*

**Présomption de conformité avec certaines exigences**

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

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

*Article 43*

**Évaluation de la conformité**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

sur la protection des droits fondamentaux, ainsi que de la disponibilité de capacités et de ressources suffisantes au sein des organismes notifiés.

*Article 44*

**Certificats**

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

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

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

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

*Article 45*

**Obligations d'information des organismes notifiés**

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

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

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

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

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

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

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

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

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

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

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

*Article 46*

**Dérogation à la procédure d'évaluation de la conformité**

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

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

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

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

5. Si, dans un délai de quinze jours civils suivant la réception de la notification visée au paragraphe 3, un État membre soulève des objections à l'encontre d'une autorisation délivrée par une autorité de surveillance du marché d'un autre État membre, ou si la Commission estime que

l'autorisation est contraire au droit de l'Union ou que la conclusion des États membres quant à la conformité du système visée au paragraphe 3 n'est pas fondée, la Commission entame sans retard des consultations avec l'État membre concerné. Les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Sur cette base, la Commission décide si l'autorisation est justifiée ou non. La Commission communique sa décision à l'État membre concerné ainsi qu'aux opérateurs concernés.

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

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

*Article 47*

**Déclaration UE de conformité**

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

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

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

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

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

*Article 48*

**Marquage CE**

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

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

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

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

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

*Article 49*

**Enregistrement**

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

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

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

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

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

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

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

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

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

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

## CHAPITRE IV

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

*Article 50*

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

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

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

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

prévention ou de détection des infractions pénales ou d'enquêtes en la matière, sous réserve de garanties appropriées pour les droits et libertés des tiers et conformément au droit de l'Union.

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

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

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

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

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

## CHAPITRE V
## MODÈLES D'IA À USAGE GÉNÉRAL

### *SECTION 1*
### *Règles de classification*

*Article 51*

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

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

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

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

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

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

*Article 52*

**Procédure**

1. Lorsqu'un modèle d'IA à usage général remplit la condition visée à l'article 51, paragraphe 1, point a), le fournisseur concerné en informe la Commission sans tarder et, en tout état de cause, dans un délai de deux semaines après la date à laquelle ce critère est rempli ou après qu'il a été établi qu'il le sera. Cette notification comprend les informations nécessaires pour démontrer que le critère pertinent a été rempli. Si la Commission apprend l'existence d'un modèle d'IA à usage général présentant un risque systémique dont elle n'a pas été informée, elle peut décider de le désigner comme modèle présentant un risque systémique.

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

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

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

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

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

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

## *SECTION 2*

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

### *Article 53*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 54*

**Mandataires des fournisseurs de modèles d'IA à usage général**

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

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

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

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

b) tenir à la disposition du Bureau de l'IA et des autorités nationales compétentes une copie de la documentation technique prévue à l'annexe XI, pendant une période de dix ans après la mise

sur le marché du modèle d'IA à usage général, et les coordonnées du fournisseur ayant désigné le mandataire;

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

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

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

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

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

## *SECTION 3*

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

*Article 55*

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

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

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

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

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

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

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

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

## *SECTION 4*

## *Codes de bonnes pratiques*

### *Article 56*

### Codes de bonne pratique

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

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

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

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

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

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

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

4. Le Bureau de l'IA et le Comité IA s'efforcent de veiller à ce que les codes de bonne pratique définissent clairement leurs objectifs spécifiques et contiennent des engagements ou des mesures, y compris, le cas échéant, des indicateurs de performance clés, afin de garantir la réalisation de ces

objectifs, et à ce qu'ils tiennent dûment compte des besoins et des intérêts de l'ensemble des parties intéressées, y compris les personnes concernées, au niveau de l'Union.

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

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

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

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

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

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

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

## CHAPITRE VI

## MESURES DE SOUTIEN À L'INNOVATION

*Article 57*

### Bacs à sable réglementaires de l'IA

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

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

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

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

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

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

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

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

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

8. Sous réserve des dispositions relatives à la confidentialité énoncées à l'article 78 et avec l'accord du fournisseur ou du fournisseur potentiel, la Commission et le Comité IA sont autorisés

à accéder aux rapports de sortie et en tiennent compte, le cas échéant, dans l'exercice des tâches qui leur incombent en vertu du présent règlement. Si le fournisseur ou le fournisseur potentiel et l'autorité nationale compétente y consentent explicitement, le rapport de sortie peut être mis à la disposition du public par l'intermédiaire de la plateforme d'information unique visée au présent article.

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

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

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

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

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

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

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

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

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

matière de conformité, aucune amende administrative n'est infligée en ce qui concerne ces dispositions.

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

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

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

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

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

*Article 58*

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

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

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

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

c) les conditions applicables aux participants.

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

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

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

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

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

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

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

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

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

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

i) que les bacs à sable réglementaire de l'IA facilitent le développement d'outils et d'infrastructures pour la mise à l'essai, l'étalonnage des performances, l'évaluation et l'explication des aspects des systèmes d'IA pertinents pour l'apprentissage réglementaire, tels

que la précision, la solidité et la cybersécurité, ainsi que les mesures d'atténuation des risques d'atteinte aux droits fondamentaux et à la société au sens large.

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

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

*Article 59*

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

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

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

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

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

   iii) la durabilité énergétique;

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

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

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

c) il existe des mécanismes de suivi efficaces pour déterminer si des risques élevés pour les droits et les libertés des personnes concernées, visés à l'article 35 du règlement (UE) 2016/679 et

à l'article 39 du règlement (UE) 2018/1725, sont susceptibles de survenir lors de l'expérimentation menée dans le cadre du bac à sable, ainsi que des mécanismes de réponse permettant d'atténuer rapidement ces risques et, au besoin, de faire cesser le traitement des données;

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

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

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

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

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

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

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

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

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

autre base juridique, dans le respect du droit de l'Union relatif à la protection des données à caractère personnel.

*Article 60*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 61*

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

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

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

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

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

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

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

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

*Article 62*

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

1. Les États membres:

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

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

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

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

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

3. Le Bureau de l'IA:

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

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

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

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

*Article 63*

**Dérogations pour des opérateurs spécifiques**

1. Les microentreprises au sens de la recommandation 2003/361/CE peuvent se conformer de manière simplifiée à certains éléments du système de gestion de la qualité requis par l'article 17 du présent règlement, pour autant qu'elles n'aient pas d'entreprises partenaires ou d'entreprises liées

au sens de ladite recommandation. À cette fin, la Commission élabore des lignes directrices sur les éléments du système de gestion de la qualité qui peuvent être respectés de manière simplifiée en tenant compte des besoins des microentreprises, sans affecter le niveau de protection ni la nécessité de se conformer aux exigences relatives aux systèmes d'IA à haut risque.

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

## CHAPITRE VII
## GOUVERNANCE

### *SECTION 1*
### *Gouvernance au niveau de l'Union*

*Article 64*

**Bureau de l'IA**

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

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

*Article 65*

**Création et structure du Comité européen de l'intelligence artificielle**

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

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

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

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

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

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

c) soient habilités à faciliter la cohérence et la coordination entre les autorités nationales compétentes de leur État membre en ce qui concerne la mise en œuvre du présent règlement, y

compris par la collecte de données et d'informations pertinentes aux fins de l'accomplissement de leurs tâches au sein du Comité IA.

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

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

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

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

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

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

*Article 66*

**Tâches du Comité IA**

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

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

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

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

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

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

application cohérente et efficace, y compris:

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

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

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

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

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

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

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

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

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

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

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

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

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

d'informations entre les bacs à sable réglementaires de l'IA;

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

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

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

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

*Article 67*

**Forum consultatif**

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

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

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

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

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

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

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

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

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

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

*Article 68*

**Groupe scientifique d'experts indépendants**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*Article 69*

**Accès des États membres au groupe scientifique**

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

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

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

***SECTION 2***

***Autorités nationales compétentes***

*Article 70*

**Désignation des autorités nationales compétentes et des points de contact uniques**

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

2. Les États membres communiquent à la Commission les autorités notifiantes et les autorités de surveillance du marché désignées et les tâches incombant à ces autorités, ainsi que toute

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

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

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

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

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

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

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

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

## CHAPITRE VIII

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

*Article 71*

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

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

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

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

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

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

6. La Commission est la responsable du traitement pour la base de données de l'UE. Elle met à la disposition des fournisseurs, des fournisseurs potentiels et des déployeurs un soutien technique et administratif approprié. La base de données de l'UE est conforme aux exigences applicables en matière d'accessibilité.

## CHAPITRE IX

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

### *SECTION 1*

### *Surveillance après commercialisation*

*Article 72*

**Surveillance après commercialisation par les fournisseurs et plan de surveillance après commercialisation pour les systèmes d'IA à haut risque**

1. Les fournisseurs établissent et documentent un système de surveillance après commercialisation d'une manière qui soit proportionnée à la nature des technologies d'IA et des

risques du système d'IA à haut risque.

2. Le système de surveillance après commercialisation collecte, documente et analyse, de manière active et systématique, les données pertinentes qui peuvent être fournies par les déployeurs ou qui peuvent être collectées via d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur cycle de vie, et qui permettent au fournisseur d'évaluer si les systèmes d'IA respectent en permanence les exigences énoncées au chapitre III, section 2. Le cas échéant, la surveillance après commercialisation comprend une analyse de l'interaction avec d'autres systèmes d'IA. Cette obligation ne couvre pas les données opérationnelles sensibles des déployeurs qui sont des autorités répressives.

3. Le système de surveillance après commercialisation repose sur un plan de surveillance après commercialisation. Le plan de surveillance après commercialisation fait partie de la documentation technique visée à l'annexe IV. La Commission adopte un acte d'exécution fixant des dispositions détaillées établissant un modèle pour le plan de surveillance après commercialisation et la liste des éléments à inclure dans le plan au plus tard le 2 février 2026. Cet acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

4. Pour les systèmes d'IA à haut risque relevant de la législation d'harmonisation de l'Union énumérés à la section A de l'annexe I, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de ces actes, afin d'assurer la cohérence, d'éviter les doubles emplois et de réduire au minimum les charges supplémentaires, les fournisseurs ont le choix d'intégrer, le cas échéant, les éléments nécessaires décrits aux paragraphes 1, 2 et 3 en utilisant le modèle visé au paragraphe 3 dans les systèmes et plans existants au titre desdits actes, pour autant que cela donne lieu à un niveau de protection équivalent.

Le premier alinéa du présent paragraphe s'applique également aux systèmes d'IA à haut risque visés à l'annexe III, point 5, mis sur le marché ou mis en service par des établissements financiers qui sont soumis à des exigences en vertu de la législation de l'Union sur les services financiers concernant leur gouvernance, leurs dispositifs ou leurs processus internes.

## *SECTION 2*

## *Partage d'informations sur les incidents graves*

### *Article 73*

### Signalement d'incidents graves

1. Les fournisseurs de systèmes d'IA à haut risque mis sur le marché de l'Union signalent tout incident grave aux autorités de surveillance du marché des États membres dans lesquels cet incident s'est produit.

2. Le signalement visé au paragraphe 1 est effectué immédiatement après que le fournisseur a établi un lien de causalité, ou la probabilité raisonnable qu'un tel lien existe, entre le système d'IA et l'incident grave et, en tout état de cause, au plus tard 15 jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

Le délai pour le signalement visé au premier alinéa tient compte de l'ampleur de l'incident grave.

3. Nonobstant le paragraphe 2 du présent article, en cas d'infraction de grande ampleur ou d'incident grave au sens de l'article 3, point 49), b), le signalement visé au paragraphe 1 du présent

article est effectué immédiatement, et au plus tard deux jours après que le fournisseur ou, le cas échéant, le déployeur a eu connaissance de cet incident.

4. Nonobstant le paragraphe 2, en cas de décès d'une personne, le signalement est effectué immédiatement après que le fournisseur ou le déployeur a établi un lien de causalité entre le système d'IA à haut risque et l'incident grave ou dès qu'il soupçonne un tel lien, mais au plus tard 10 jours après la date à laquelle le fournisseur ou, le cas échéant, le déployeur a eu connaissance de l'incident grave.

5. Si cela est nécessaire pour assurer un signalement en temps utile, le fournisseur ou, le cas échéant, le déployeur peut soumettre un signalement initial incomplet, suivi d'un signalement complet.

6. À la suite du signalement d'un incident grave en application du paragraphe 1, le fournisseur mène sans tarder les investigations nécessaires liées à l'incident grave et au système d'IA concerné. Ces investigations comprennent notamment une évaluation des risques résultant de l'incident, ainsi que des mesures correctives.

Le fournisseur coopère avec les autorités compétentes et, le cas échéant, avec l'organisme notifié concerné, au cours des investigations visées au premier alinéa, et ne mène aucune investigation nécessitant de modifier le système d'IA concerné d'une manière susceptible d'avoir une incidence sur toute évaluation ultérieure des causes de l'incident, avant d'informer les autorités compétentes de telles mesures.

7. Dès réception d'une notification relative à un incident grave visé à l'article 3, point 49) c), l'autorité de surveillance du marché compétente informe les autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1. La Commission élabore des orientations spécifiques pour faciliter le respect des obligations énoncées au paragraphe 1 du présent article. Ces orientations sont publiées au plus tard le 2 août 2025, et font l'objet d'une évaluation régulière.

8. L'autorité de surveillance du marché prend les mesures qui s'imposent, conformément à l'article 19 du règlement (UE) 2019/1020, dans un délai de sept jours à compter de la date à laquelle elle a reçu la notification visée au paragraphe 1 du présent article, et suit les procédures de notification prévues par ledit règlement.

9. Pour les systèmes d'IA à haut risque visés à l'annexe III qui sont mis sur le marché ou mis en service par des fournisseurs qui sont soumis à des instruments législatifs de l'Union établissant des obligations de signalement équivalentes à celles énoncées dans le présent règlement, la notification des incidents graves est limitée à ceux visés à l'article 3, point 49) c).

10. Pour les systèmes d'IA à haut risque qui sont des composants de sécurité de dispositifs, ou qui sont eux-mêmes des dispositifs, relevant des règlements (UE) 2017/745 et (UE) 2017/746, la notification des incidents graves est limitée à ceux qui sont visés à l'article 3, point 49) c), du présent règlement, et est adressée à l'autorité nationale compétente choisie à cette fin par les États membres dans lesquels l'incident s'est produit.

11. Les autorités nationales compétentes notifient immédiatement à la Commission tout incident grave, qu'elles aient ou non pris des mesures à cet égard, conformément à l'article 20 du règlement (UE) 2019/1020.

## *SECTION 3*

*Contrôle de l'application*

*Article 74*

**Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union**

1. Le règlement (UE) 2019/1020 s'applique aux systèmes d'IA relevant du présent règlement. Aux fins du contrôle effectif de l'application du présent règlement:

a) toute référence à un opérateur économique en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les opérateurs identifiés à l'article 2, paragraphe 1, du présent règlement;

b) toute référence à un produit en vertu du règlement (UE) 2019/1020 s'entend comme incluant tous les systèmes d'IA relevant du champ d'application du présent règlement.

2. Dans le cadre des obligations d'information qui leur incombent en vertu de l'article 34, paragraphe 4, du règlement (UE) 2019/1020, les autorités de surveillance du marché communiquent chaque année à la Commission et aux autorités nationales de la concurrence concernées toute information recueillie dans le cadre des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de l'Union relatif aux règles de concurrence. Elles font également rapport chaque année à la Commission sur les recours aux pratiques interdites intervenus au cours de l'année concernée et sur les mesures prises.

3. Pour les systèmes d'IA à haut risque liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure à la section A de l'annexe I, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité responsable des activités de surveillance du marché désignée en vertu de ces actes juridiques.

Par dérogation au premier alinéa, et dans des circonstances appropriées, les États membres peuvent désigner une autre autorité compétente pour faire office d'autorité de surveillance du marché, à condition d'assurer la coordination avec les autorités sectorielles de surveillance du marché compétentes chargées du contrôle de l'application des actes juridiques énumérés à l'annexe I.

4. Les procédures visées aux articles 79 à 83 du présent règlement ne s'appliquent pas aux systèmes d'IA liés à des produits couverts par la législation d'harmonisation de l'Union dont la liste figure la section A de l'annexe I, lorsque ces actes juridiques prévoient déjà des procédures assurant un niveau de protection équivalent et ayant le même objectif. En pareils cas, ce sont les procédures sectorielles pertinentes qui s'appliquent.

5. Sans préjudice des pouvoirs conférés aux autorités de surveillance du marché par l'article 14 du règlement (UE) 2019/1020, afin d'assurer le contrôle effectif de l'application du présent règlement, les autorités de surveillance du marché peuvent exercer les pouvoirs visés à l'article 14, paragraphe 4, points d) et j), dudit règlement à distance, le cas échéant.

6. Pour les systèmes d'IA à haut risque mis sur le marché, mis en service ou utilisés par des établissements financiers régis par la législation de l'Union sur les services financiers, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité nationale responsable de la surveillance financière de ces établissements en vertu de cette législation dans la mesure où la mise sur le marché, la mise en service ou l'utilisation du système d'IA est directement liée à la fourniture de ces services financiers.

7. Par dérogation au paragraphe 6, dans des circonstances appropriées, et pour autant que la coordination soit assurée, l'État membre peut désigner une autre autorité compétente comme autorité de surveillance du marché aux fins du présent règlement.

Les autorités nationales de surveillance du marché surveillant les établissements de crédit réglementés régis par la directive 2013/36/UE, qui participent au mécanisme de surveillance unique institué par le règlement (UE) n° 1024/2013, devraient communiquer sans tarder à la Banque centrale européenne toute information identifiée dans le cadre de leurs activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour les missions de surveillance prudentielle de la Banque centrale européenne définies dans ledit règlement.

8. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, du présent règlement, dans la mesure où ils sont utilisés à des fins répressives, de gestion des frontières et de justice et démocratie, et pour les systèmes d'IA à haut risque énumérés à l'annexe III, points 6, 7 et 8, du présent règlement, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités compétentes en matière de contrôle de la protection des données en vertu du règlement (UE) 2016/679 ou de la directive (UE) 2016/680, soit toute autre autorité désignée en application des mêmes conditions énoncées aux articles 41 à 44 de la directive (UE) 2016/680. Les activités de surveillance du marché ne portent en aucune manière atteinte à l'indépendance des autorités judiciaires ni n'interfèrent d'une autre manière avec leurs activités lorsque ces autorités agissent dans l'exercice de leurs fonctions judiciaires.

9. Lorsque les institutions, organes ou organismes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données est leur autorité de surveillance du marché, sauf en ce qui concerne la Cour de justice de l'Union européenne agissant dans l'exercice de ses fonctions judiciaires.

10. Les États membres facilitent la coordination entre les autorités de surveillance du marché désignées en vertu du présent règlement et les autres autorités ou organismes nationaux compétents pour surveiller l'application de la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, ou dans d'autres législations de l'Union, qui sont susceptibles d'être pertinents pour les systèmes d'IA à haut risque visés à l'annexe III.

11. Les autorités de surveillance du marché et la Commission sont en mesure de proposer des activités conjointes, y compris des enquêtes conjointes, à mener soit par les autorités de surveillance du marché, soit par les autorités de surveillance du marché conjointement avec la Commission, qui ont pour objectif de promouvoir le respect de la législation, de déceler la non-conformité, de sensibiliser ou de fournir des orientations au regard du présent règlement en ce qui concerne des catégories spécifiques de systèmes d'IA à haut risque qui sont identifiés comme présentant un risque grave dans deux États membres ou plus conformément à l'article 9 du règlement (UE) 2019/1020. Le Bureau de l'IA fournit une aide à la coordination des enquêtes conjointes.

12. Sans préjudice des pouvoirs prévus par le règlement (UE) 2019/1020, et lorsque cela est pertinent et limité à ce qui est nécessaire à l'accomplissement de leurs tâches, les fournisseurs accordent aux autorités de surveillance du marché un accès complet à la documentation ainsi qu'aux jeux de données d'entraînement, de validation et de test utilisés pour le développement des systèmes d'IA à haut risque, y compris, lorsque cela est approprié et sous réserve de garanties de

sécurité, par l'intermédiaire d'interfaces de programmation d'application (API) ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

13. Les autorités de surveillance du marché se voient accorder l'accès au code source du système d'IA à haut risque sur demande motivée et uniquement lorsque les deux conditions suivantes sont réunies:

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

b) les procédures d'essai ou d'audit et les vérifications fondées sur les données et la documentation communiquées par le fournisseur ont été entièrement accomplies ou se sont révélées insuffisantes.

14. Toute information ou documentation obtenue par les autorités de surveillance du marché est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

*Article 75*

**Assistance mutuelle, surveillance du marché et contrôle des systèmes d'IA à usage général**

1. Lorsqu'un système d'IA repose sur un modèle d'IA à usage général, et que le modèle et le système sont mis au point par le même fournisseur, le Bureau de l'IA est habilité à contrôler et surveiller la conformité de ce système d'IA avec les obligations prévues par le présent règlement. Pour s'acquitter de ses tâches de contrôle et de surveillance, le Bureau de l'IA dispose de tous les pouvoirs d'une autorité de surveillance du marché prévus dans la présente section et dans le règlement (UE) 2019/1020.

2. Lorsqu'elles ont des raisons suffisantes de considérer que des systèmes d'IA à usage général qui peuvent être utilisés directement par les déployeurs pour au moins un usage classé comme étant à haut risque en vertu du présent règlement ne sont pas conformes aux exigences énoncées dans le présent règlement, les autorités de surveillance du marché concernées coopèrent avec le Bureau de l'IA pour procéder à des évaluations de la conformité, et en informent le Comité IA et les autres autorités de surveillance du marché.

3. Lorsqu'une autorité de surveillance du marché n'est pas en mesure de conclure son enquête sur le système d'IA à haut risque en raison de son incapacité à accéder à certaines informations relatives au modèle d'IA à usage général bien qu'elle ait déployé tous les efforts appropriés pour obtenir ces informations, elle peut présenter une demande motivée au Bureau de l'IA, par laquelle l'accès à ces informations est mis en œuvre. Dans ce cas, le Bureau de l'IA fournit sans tarder à l'autorité requérante, et en tout état de cause dans un délai de 30 jours, toute information qu'il juge pertinente pour déterminer si un système d'IA à haut risque est non conforme. Les autorités de surveillance du marché garantissent la confidentialité des informations qu'elles obtiennent conformément à l'article 78 du présent règlement. La procédure prévue au chapitre VI du règlement (UE) 2019/1020 s'applique mutatis mutandis.

*Article 76*

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

1. Les autorités de surveillance du marché ont les compétences et les pouvoirs nécessaires pour veiller à ce que les essais en conditions réelles soient conformes au présent règlement.

2. Lorsque des essais en conditions réelles sont effectués pour des systèmes d'IA supervisés dans un bac à sable réglementaire de l'IA en vertu de l'article 58, les autorités de surveillance du marché vérifient le respect de l'article 60 dans le cadre de leur rôle de surveillance du bac à sable réglementaire de l'IA. Ces autorités peuvent, lorsqu'il y a lieu, autoriser le fournisseur ou le fournisseur potentiel à effectuer les essais en conditions réelles, par dérogation aux conditions énoncées à l'article 60, paragraphe 4, points f) et g).

3. Lorsqu'une autorité de surveillance du marché a été informée d'un incident grave par le fournisseur potentiel, le fournisseur ou tout tiers, ou qu'elle a d'autres raisons de penser que les conditions énoncées aux articles 60 et 61 ne sont pas remplies, elle peut prendre l'une ou l'autre des décisions suivantes sur son territoire, selon le cas:

a) suspendre ou faire cesser les essais en conditions réelles;

b) exiger du fournisseur ou du fournisseur potentiel et du déployeur ou futur déployeur qu'ils modifient tout aspect des essais en conditions réelles.

4. Lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3 du présent article, ou a formulé une objection au sens de l'article 60, paragraphe 4, point b), la décision ou l'objection est motivée et indique les modalités selon lesquelles le fournisseur ou le fournisseur potentiel peut contester la décision ou l'objection.

5. Le cas échéant, lorsqu'une autorité de surveillance du marché a pris une décision visée au paragraphe 3, elle en communique les motifs aux autorités de surveillance du marché des autres États membres dans lesquels le système d'IA a été testé conformément au plan d'essais.

*Article 77*

**Pouvoirs des autorités de protection des droits fondamentaux**

1. Les autorités ou organismes publics nationaux qui supervisent ou font respecter les obligations au titre du droit de l'Union visant à protéger les droits fondamentaux, y compris le droit à la non-discrimination, en ce qui concerne l'utilisation des systèmes d'IA à haut risque visés à l'annexe III sont habilités à demander toute documentation créée ou conservée en vertu du présent règlement et à y avoir accès dans une langue et un format accessibles lorsque l'accès à cette documentation est nécessaire à l'accomplissement effectif de leur mandat dans les limites de leurs compétences. L'autorité ou l'organisme public concerné informe l'autorité de surveillance du marché de l'État membre concerné de toute demande de ce type.

2. Au plus tard le 2 novembre 2024, chaque État membre identifie les autorités ou organismes publics visés au paragraphe 1 et met la liste de ces autorités ou organismes à la disposition du public. Les États membres notifient la liste à la Commission et aux autres États membres, et tiennent cette liste à jour.

3. Lorsque la documentation visée au paragraphe 1 ne suffit pas pour déterminer s'il y a eu violation des obligations au titre du droit de l'Union protégeant les droits fondamentaux, l'autorité ou l'organisme public visé au paragraphe 1 peut présenter à l'autorité de surveillance du marché une demande motivée visant à organiser des tests du système d'IA à haut risque par des moyens techniques. L'autorité de surveillance du marché organise les tests avec la participation étroite de l'autorité ou organisme public ayant présenté la demande dans un délai raisonnable après celle-ci.

4. Toute information ou documentation obtenue par les autorités ou organismes publics nationaux visés au paragraphe 1 du présent article en application des dispositions du présent article est traitée conformément aux obligations de confidentialité énoncées à l'article 78.

*Article 78*

**Confidentialité**

1. La Commission, les autorités de surveillance du marché et les organismes notifiés, ainsi que toute autre personne physique ou morale associée à l'application du présent règlement respectent, conformément au droit de l'Union ou au droit national, la confidentialité des informations et des données obtenues dans l'exécution de leurs tâches et activités de manière à protéger, en particulier:

a) les droits de propriété intellectuelle et les informations confidentielles de nature commerciale ou les secrets d'affaires des personnes physiques ou morales, y compris le code source, à l'exception des cas visés à l'article 5 de la directive (UE) 2016/943 du Parlement européen et du Conseil ([57]);

b) la mise en œuvre effective du présent règlement, notamment en ce qui concerne les inspections, les investigations ou les audits;

c) les intérêts en matière de sécurité nationale et publique;

d) la conduite des procédures pénales ou administratives;

e) les informations classifiées en vertu du droit de l'Union ou du droit national.

2. Les autorités associées à l'application du présent règlement conformément au paragraphe 1 demandent uniquement les données qui sont strictement nécessaires à l'évaluation du risque posé par les systèmes d'IA et à l'exercice de leurs pouvoirs conformément au présent règlement et au règlement (UE) 2019/1020. Elles mettent en place des mesures de cybersécurité adéquates et efficaces pour protéger la sécurité et la confidentialité des informations et des données obtenues, et suppriment les données collectées dès qu'elles ne sont plus nécessaires aux fins pour lesquelles elles ont été obtenues, conformément au droit de l'Union ou au droit national applicable.

3. Sans préjudice des paragraphes 1 et 2, les informations échangées à titre confidentiel entre les autorités nationales compétentes ou entre celles-ci et la Commission ne sont pas divulguées sans consultation préalable de l'autorité nationale compétente dont elles émanent et du déployeur lorsque les systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, sont utilisés par les autorités répressives, les autorités chargées des contrôles aux frontières, les services de l'immigration ou les autorités compétentes en matière d'asile et lorsque cette divulgation risquerait de porter atteinte aux intérêts en matière de sécurité nationale et publique. Cet échange d'informations ne couvre pas les données opérationnelles sensibles relatives aux activités des autorités répressives, des autorités chargées des contrôles aux frontières, des services de l'immigration ou des autorités compétentes en matière d'asile.

Lorsque les autorités répressives, les services de l'immigration ou les autorités compétentes en matière d'asile sont fournisseurs de systèmes d'IA à haut risque visés à l'annexe III, point 1, 6 ou 7, la documentation technique visée à l'annexe IV reste dans les locaux de ces autorités. Ces autorités veillent à ce que les autorités de surveillance du marché visées à l'article 74, paragraphes 8 et 9, selon le cas, puissent, sur demande, avoir immédiatement accès à la documentation ou en obtenir une copie. Seuls les membres du personnel de l'autorité de

surveillance du marché disposant d'une habilitation de sécurité au niveau approprié sont autorisés à avoir accès à cette documentation ou à une copie de celle-ci.

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

5. La Commission et les États membres peuvent, lorsque cela est nécessaire et conformément aux dispositions pertinentes des accords internationaux et commerciaux, échanger des informations confidentielles avec les autorités de réglementation de pays tiers avec lesquels ils ont conclu des accords bilatéraux ou multilatéraux en matière de confidentialité garantissant un niveau de confidentialité approprié.

*Article 79*

**Procédure applicable au niveau national aux systèmes d'IA présentant un risque**

1. On entend par systèmes d'IA présentant un risque, un «produit présentant un risque» au sens de l'article 3, point 19), du règlement (UE) 2019/1020, dans la mesure où ils présentent des risques pour la santé ou la sécurité, ou pour les droits fondamentaux, des personnes.

2. Lorsque l'autorité de surveillance du marché d'un État membre a des raisons suffisantes de considérer qu'un système d'IA présente un risque au sens du paragraphe 1 du présent article, elle procède à une évaluation de la conformité du système d'IA concerné avec l'ensemble des exigences et obligations énoncées dans le présent règlement. Une attention particulière est accordée aux systèmes d'IA présentant un risque pour les groupes vulnérables. Lorsque sont identifiés des risques pour les droits fondamentaux, l'autorité de surveillance du marché informe également les autorités ou organismes publics nationaux concernés visés à l'article 77, paragraphe 1, et coopère pleinement avec eux. Les opérateurs concernés coopèrent, en tant que de besoin, avec l'autorité de surveillance du marché et avec les autres autorités ou organismes publics nationaux visés à l'article 77, paragraphe 1.

Si, au cours de cette évaluation, l'autorité de surveillance du marché ou, le cas échéant, l'autorité de surveillance du marché en coopération avec l'autorité publique nationale visée à l'article 77, paragraphe 1, constate que le système d'IA ne respecte pas les exigences et obligations énoncées dans le présent règlement, elle invite sans retard injustifié l'opérateur concerné à prendre toutes les mesures correctives appropriées pour mettre le système d'IA en conformité, le retirer du marché ou le rappeler dans un délai qu'elle peut prescrire, et en tout état de cause au plus tard dans les 15 jours ouvrables, ou dans un délai prévu par la législation d'harmonisation de l'Union concernée, le délai le plus court étant retenu.

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

3. Lorsque l'autorité de surveillance du marché considère que la non-conformité n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées de l'opérateur.

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

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

6. La notification visée au paragraphe 5 contient toutes les précisions disponibles, notamment les informations nécessaires pour identifier le système d'IA non conforme, son origine et la chaîne d'approvisionnement, la nature de la non-conformité alléguée et du risque encouru, ainsi que la nature et la durée des mesures nationales prises et les arguments avancés par l'opérateur concerné. En particulier, l'autorité de surveillance du marché indique si la non-conformité découle d'une ou plusieurs des causes suivantes:

a) le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5;

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

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

d) le non-respect de l'article 50.

7. Les autorités de surveillance du marché autres que l'autorité de surveillance du marché de l'État membre qui a entamé la procédure informent sans retard injustifié la Commission et les autres États membres de toute mesure adoptée et de toute information supplémentaire dont elles disposent à propos de la non-conformité du système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans les trois mois suivant la réception de la notification visée au paragraphe 5, aucune objection n'a été émise par une autorité de surveillance du marché d'un État membre ou par la Commission à l'encontre d'une mesure provisoire prise par une autorité de surveillance du marché d'un autre État membre, cette mesure est réputée justifiée. Cette disposition est sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020. Le délai de trois mois visé au présent paragraphe est ramené à 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 du présent règlement.

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

*Article 80*

**Procédure applicable aux systèmes d'IA classés par le fournisseur comme n'étant pas à haut risque en application de l'annexe III**

1. Lorsqu'une autorité de surveillance du marché a des raisons suffisantes de considérer qu'un système d'IA classé par le fournisseur comme n'étant pas à haut risque en application de l'article 6,

paragraphe 3, est en réalité à haut risque, elle procède à une évaluation du système d'IA concerné quant à la question de sa classification en tant que système d'IA à haut risque sur la base des conditions énoncées à l'article 6, paragraphe 3, et dans les lignes directrices de la Commission.

2. Lorsque, au cours de cette évaluation, l'autorité de surveillance du marché constate que le système d'IA concerné est à haut risque, elle demande sans retard injustifié au fournisseur concerné de prendre toutes les mesures nécessaires pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement, ainsi que de prendre les mesures correctives appropriées dans un délai que l'autorité de surveillance du marché peut prescrire.

3. Lorsque l'autorité de surveillance du marché considère que l'utilisation du système d'IA concerné n'est pas limitée à son territoire national, elle informe la Commission et les autres États membres, sans retard injustifié, des résultats de l'évaluation et des mesures qu'elle a exigées du fournisseur.

4. Le fournisseur veille à ce que toutes les mesures nécessaires soient prises pour mettre le système d'IA en conformité avec les exigences et obligations énoncées dans le présent règlement. Lorsque le fournisseur d'un système d'IA concerné ne met pas le système d'IA en conformité avec ces exigences et obligations dans le délai visé au paragraphe 2 du présent article, il fait l'objet d'amendes conformément à l'article 99.

5. Le fournisseur s'assure que toutes les mesures correctives appropriées sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union.

6. Lorsque le fournisseur du système d'IA concerné ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2 du présent article, l'article 79, paragraphe 5 à 9, s'applique.

7. Lorsque, au cours de l'évaluation prévue au paragraphe 1 du présent article, l'autorité de surveillance du marché établit que le système d'IA a été classé à tort par le fournisseur comme n'étant pas à haut risque afin de contourner l'application des exigences figurant au chapitre III, section 2, le fournisseur fait l'objet d'amendes conformément à l'article 99.

8. Dans l'exercice de leur pouvoir de contrôle de l'application du présent article, et conformément à l'article 11 du règlement (UE) 2019/1020, les autorités de surveillance du marché peuvent effectuer des contrôles appropriés, en tenant compte notamment des informations stockées dans la base de données de l'UE visée à l'article 71 du présent règlement.

*Article 81*

**Procédure de sauvegarde de l'Union**

1. Lorsque, dans un délai de trois mois suivant la réception de la notification visée à l'article 79, paragraphe 5, ou dans un délai de 30 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, l'autorité de surveillance du marché d'un État membre soulève des objections à l'encontre d'une mesure prise par une autre autorité de surveillance du marché, ou que la Commission estime que cette mesure est contraire au droit de l'Union, la Commission entame sans retard injustifié des consultations avec l'autorité de surveillance du marché de l'État membre concerné et le ou les opérateurs, et procède à l'évaluation de la mesure nationale. En fonction des résultats de cette évaluation, la Commission, dans un délai de six mois, ou de 60 jours en cas de non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5, à compter

de la notification visée à l'article 79, paragraphe 5, décide si la mesure nationale est justifiée ou non et communique sa décision à l'autorité de surveillance du marché de l'État membre concerné. La Commission informe également toutes les autres autorités de surveillance du marché de sa décision.

2. Lorsque la Commission estime que la mesure prise par l'État membre concerné est justifiée, tous les États membres veillent à prendre des mesures restrictives appropriées à l'égard du système d'IA concerné, par exemple en exigeant le retrait du système d'IA de leur marché sans retard injustifié, et en informent la Commission. Lorsque la Commission estime que la mesure nationale n'est pas justifiée, l'État membre concerné retire la mesure et en informe la Commission.

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

*Article 82*

**Systèmes d'IA conformes qui présentent un risque**

1. Lorsque, ayant réalisé une évaluation au titre de l'article 79, après avoir consulté l'autorité publique nationale concernée visée à l'article 77, paragraphe 1, l'autorité de surveillance du marché d'un État membre constate que, bien qu'un système d'IA à haut risque soit conforme au présent règlement, il comporte néanmoins un risque pour la santé ou la sécurité des personnes, pour les droits fondamentaux, ou pour d'autres aspects relatifs à la protection de l'intérêt public, elle demande à l'opérateur concerné de prendre toutes les mesures appropriées pour faire en sorte que le système d'IA concerné, une fois mis sur le marché ou mis en service, ne présente plus ce risque, et ce sans retard injustifié, dans un délai qu'elle peut prescrire.

2. Le fournisseur ou autre opérateur concerné s'assure que des mesures correctives sont prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché de l'Union dans le délai prescrit par l'autorité de surveillance du marché de l'État membre visée au paragraphe 1.

3. Les États membres informent immédiatement la Commission et les autres États membres d'une constatation au titre du paragraphe 1. Les informations fournies incluent toutes les précisions disponibles, notamment les données nécessaires à l'identification du système d'IA concerné, l'origine et la chaîne d'approvisionnement de ce système d'IA, la nature du risque encouru, ainsi que la nature et la durée des mesures nationales prises.

4. La Commission entame sans retard injustifié des consultations avec les États membres concernés et les opérateurs concernés, et évalue les mesures nationales prises. En fonction des résultats de cette évaluation, la Commission décide si la mesure est justifiée ou non et, si nécessaire, propose d'autres mesures appropriées.

5. La Commission communique immédiatement sa décision aux États membres concernés ainsi qu'aux opérateurs concernés. Elle en informe également les autres États membres.

*Article 83*

**Non-conformité formelle**

1. Lorsque l'autorité de surveillance du marché d'un État membre fait l'une des constatations ci-après, elle invite le fournisseur concerné à mettre un terme à la non-conformité en question, dans un délai qu'elle peut prescrire:

a) le marquage CE a été apposé en violation de l'article 48;

b) le marquage CE n'a pas été apposé;

c) la déclaration UE de conformité visée à l'article 47 n'a pas été établie;

d) la déclaration UE de conformité visée à l'article 47 n'a pas été établie correctement;

e) l'enregistrement dans la base de données de l'UE visée à l'article 71 n'a pas été effectué;

f) le cas échéant, il n'a pas été désigné de mandataire;

g) la documentation technique n'est pas disponible.

2. Si le cas de non-conformité visé au paragraphe 1 persiste, l'autorité de surveillance du marché de l'État membre concerné prend toutes les mesures appropriées et proportionnées pour restreindre ou interdire la mise à disposition du système d'IA à haut risque sur le marché ou pour assurer son rappel ou son retrait sans tarder du marché.

*Article 84*

**Structures de soutien de l'Union pour les essais en matière d'IA**

1. La Commission désigne une ou plusieurs structures de soutien de l'Union pour les essais en matière d'IA conformément à l'article 21, paragraphe 6, du règlement (UE) 2019/1020 dans le domaine de l'intelligence artificielle.

2. Sans préjudice des tâches visées au paragraphe 1, les structures de soutien de l'Union pour les essais en matière d'IA fournissent également des avis techniques ou scientifiques indépendants à la demande du Comité IA, de la Commission ou des autorités de surveillance du marché.

## *SECTION 4*

## *Voies de recours*

*Article 85*

**Droit d'introduire une réclamation auprès d'une autorité de surveillance du marché**

Sans préjudice d'autres recours administratifs ou judiciaires, toute personne physique ou morale ayant des motifs de considérer qu'il y a eu violation des dispositions du présent règlement peut déposer des réclamations auprès de l'autorité de surveillance du marché concernée.

Conformément au règlement (UE) 2019/1020, ces réclamations sont prises en compte aux fins de l'exercice des activités de surveillance du marché, et sont traitées conformément aux procédures spécifiques établies en conséquence par les autorités de surveillance du marché.

*Article 86*

**Droit à l'explication des décisions individuelles**

1. Toute personne concernée faisant l'objet d'une décision prise par un déployeur sur la base des sorties d'un système d'IA à haut risque mentionné à l'annexe III, à l'exception des systèmes énumérés au point 2 de ladite annexe, et qui produit des effets juridiques ou affecte significativement cette personne de façon similaire d'une manière qu'elle considère comme ayant des conséquences négatives sur sa santé, sa sécurité ou ses droits fondamentaux a le droit d'obtenir du déployeur des explications claires et pertinentes sur le rôle du système d'IA dans la procédure décisionnelle et sur les principaux éléments de la décision prise.

2. Le paragraphe 1 ne s'applique pas à l'utilisation de systèmes d'IA pour lesquels des exceptions ou des restrictions à l'obligation prévue audit paragraphe découlent du droit de l'Union ou du droit national dans le respect du droit de l'Union.

3. Le présent article ne s'applique que dans la mesure où le droit visé au paragraphe 1 n'est pas prévu par ailleurs dans le droit de l'Union.

*Article 87*

**Signalement de violations et protection des auteurs de signalement**

La directive (UE) 2019/1937 s'applique aux signalements de violations du présent règlement et à la protection des personnes signalant ces violations.

## *SECTION 5*

## *Surveillance, enquêtes, contrôle de l'application et contrôle en ce qui concerne les fournisseurs de modèles d'IA à usage général*

*Article 88*

**Contrôle de l'exécution des obligations incombant aux fournisseurs de modèles d'IA à usage général**

1. La Commission dispose de pouvoirs exclusifs pour surveiller et contrôler le respect du chapitre V, en tenant compte des garanties procédurales prévues à l'article 94. La Commission confie l'exécution de ces tâches au Bureau de l'IA, sans préjudice des pouvoirs d'organisation dont elle dispose ainsi que de la répartition des compétences entre les États membres et l'Union fondée sur les traités.

2. Sans préjudice de l'article 75, paragraphe 3, les autorités de surveillance du marché peuvent demander à la Commission d'exercer les pouvoirs prévus dans la présente section, lorsque cela est nécessaire et proportionné pour contribuer à l'accomplissement des tâches qui leur incombent en vertu du présent règlement.

*Article 89*

**Mesures de contrôle**

1. Aux fins de l'exécution des tâches qui lui sont conférées dans le cadre de la présente section, le Bureau de l'IA peut prendre les mesures nécessaires pour contrôler la mise en œuvre et le respect effectifs du présent règlement par les fournisseurs de modèles d'IA à usage général, y compris leur adhésion à des codes de bonne pratique approuvés.

2. Les fournisseurs en aval ont le droit d'introduire une réclamation pour violation du présent règlement. La réclamation est dûment motivée et indique au moins:

a) le point de contact du fournisseur du modèle d'IA à usage général concerné;

b) une description des faits pertinents, les dispositions concernées du présent règlement et la raison pour laquelle le fournisseur en aval considère que le fournisseur du modèle d'IA à usage général concerné a enfreint le présent règlement;

c) toute autre information que le fournisseur en aval qui a envoyé la demande juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

*Article 90*

**Alertes de risques systémiques données par le groupe scientifique**

1. Le groupe scientifique peut adresser une alerte qualifiée au Bureau de l'IA lorsqu'il a des raisons de soupçonner:

a) qu'un modèle d'IA à usage général présente un risque concret identifiable au niveau de l'Union; ou

b) qu'un modèle d'IA à usage général satisfait aux conditions visées à l'article 51.

2. À la suite d'une telle alerte qualifiée, la Commission, par l'intermédiaire du Bureau de l'IA et après en avoir informé le Comité IA, peut exercer les pouvoirs prévus à la présente section aux fins de l'évaluation de la question. Le Bureau de l'IA informe le Comité IA de toute mesure prise conformément aux articles 91 à 94.

3. L'alerte qualifiée est dûment motivée et indique au moins:

a) le point de contact du fournisseur du modèle d'IA à usage général concerné présentant un risque systémique;

b) une description des faits pertinents et les motifs de l'alerte donnée par le groupe scientifique;

c) toute autre information que le groupe scientifique juge pertinente, y compris, le cas échéant, les informations recueillies de sa propre initiative.

*Article 91*

**Pouvoir de demander de la documentation et des informations**

1. La Commission peut demander au fournisseur du modèle d'IA à usage général concerné de fournir la documentation établie par le fournisseur conformément aux articles 53 et 55, ou toute information supplémentaire nécessaire pour évaluer la conformité du fournisseur avec le présent règlement.

2. Avant d'envoyer la demande d'informations, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.

3. Sur demande dûment motivée du groupe scientifique, la Commission peut adresser une demande d'informations au fournisseur d'un modèle d'IA à usage général, lorsque l'accès à ces informations est nécessaire et proportionné pour l'accomplissement des tâches du groupe scientifique au titre de l'article 68, paragraphe 2.

4. La demande d'informations mentionne la base juridique et l'objet de la demande, précise quelles informations sont requises, fixe un délai dans lequel les informations doivent être fournies, et indique les amendes prévues à l'article 101 en cas de fourniture d'informations inexactes, incomplètes ou trompeuses.

5. Le fournisseur du modèle d'IA à usage général concerné, ou son représentant, fournit les informations demandées. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas de personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts fournissent les informations demandées pour le compte du fournisseur du modèle d'IA à usage général concerné. Les avocats dûment habilités à agir peuvent fournir des informations pour le compte de leurs clients. Les clients demeurent néanmoins pleinement responsables si les informations fournies sont incomplètes, inexactes ou trompeuses.

*Article 92*

**Pouvoir de procéder à des évaluations**

1. Le Bureau de l'IA, après consultation du Comité IA, peut procéder à des évaluations du modèle d'IA à usage général concerné:

a) pour évaluer le respect, par le fournisseur, des obligations prévues par le présent règlement, lorsque les informations recueillies en vertu de l'article 91 sont insuffisantes; ou

b) pour enquêter sur les risques systémiques, au niveau de l'Union, des modèles d'IA à usage général présentant un risque systémique, en particulier à la suite d'une alerte qualifiée du groupe scientifique conformément à l'article 90, paragraphe 1, point a).

2. La Commission peut décider de désigner des experts indépendants chargés de procéder à des évaluations pour son compte, y compris des experts du groupe scientifique établi en vertu de l'article 68. Les experts indépendants désignés pour cette tâche satisfont aux critères énoncés à l'article 68, paragraphe 2.

3. Aux fins du paragraphe 1, la Commission peut demander l'accès au modèle d'IA à usage général concerné par l'intermédiaire d'API ou d'autres moyens et outils techniques appropriés, y compris le code source.

4. La demande d'accès indique la base juridique, l'objet et les motifs de la demande et fixe le délai dans lequel l'accès doit être accordé, ainsi que les amendes prévues à l'article 101 en cas de non-fourniture de l'accès.

5. Les fournisseurs du modèle d'IA à usage général concerné ou son représentant fournissent les informations requises. Dans le cas de personnes morales, d'entreprises ou de sociétés, ou lorsque le fournisseur n'a pas la personnalité juridique, les personnes autorisées à les représenter en vertu de la loi ou de leurs statuts, accordent l'accès demandé pour le compte du fournisseur du modèle d'IA à usage général concerné.

6. La Commission adopte des actes d'exécution établissant les modalités détaillées et les conditions des évaluations, y compris les modalités détaillées d'intervention d'experts indépendants, et la procédure relative à leur sélection. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

7. Avant de demander l'accès au modèle d'IA à usage général concerné, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général afin de recueillir davantage d'informations sur les essais internes du modèle, les garanties internes visant à prévenir les risques systémiques, ainsi que d'autres procédures internes et les mesures que le fournisseur a prises pour atténuer ces risques.

*Article 93*

**Pouvoir de demander des mesures**

1. Lorsque cela est nécessaire et approprié, la Commission peut demander aux fournisseurs:

a) de prendre les mesures appropriées pour se conformer aux obligations énoncées à aux articles 53 et 54;

b) de mettre en œuvre des mesures d'atténuation, lorsque l'évaluation effectuée conformément à l'article 92 a suscité des préoccupations sérieuses et fondées quant à un risque systémique au niveau de l'Union;

c) de restreindre la mise à disposition du modèle sur le marché, de le retirer ou de le rappeler.

2. Avant qu'une mesure ne soit demandée, le Bureau de l'IA peut entamer un dialogue structuré avec le fournisseur du modèle d'IA à usage général.

3. Si, au cours du dialogue structuré visé au paragraphe 2, le fournisseur du modèle d'IA à usage général présentant un risque systémique s'engage à mettre en œuvre des mesures d'atténuation pour faire face à un risque systémique au niveau de l'Union, la Commission peut, par une décision, rendre ces engagements contraignants et déclarer qu'il n'y a plus lieu d'agir.

*Article 94*

**Droits procéduraux des opérateurs économiques du modèle d'IA à usage général**

L'article 18 du règlement (UE) 2019/1020 s'applique mutatis mutandis aux fournisseurs du modèle d'IA à usage général, sans préjudice des droits procéduraux plus spécifiques prévus par le présent règlement.

## CHAPITRE X
## CODES DE CONDUITE ET LIGNES DIRECTRICES

*Article 95*

**Codes de conduite pour l'application volontaire de certaines exigences**

1. Le Bureau de l'IA et les États membres encouragent et facilitent l'élaboration de codes de conduite, comportant des mécanismes de gouvernance connexes, destinés à favoriser l'application volontaire, aux systèmes d'IA autres que les systèmes d'IA à haut risque, de tout ou partie des exigences énoncées au chapitre III, section 2, en tenant compte des solutions techniques disponibles et des bonnes pratiques du secteur permettant l'application de ces exigences.

2. Le Bureau de l'IA et les États membres facilitent l'élaboration de codes de conduite concernant l'application volontaire, y compris par les déployeurs, d'exigences spécifiques à tous les systèmes

d'IA, sur la base d'objectifs clairs et d'indicateurs de performance clés permettant de mesurer la réalisation de ces objectifs, y compris des éléments tels que, entre autres:

a) les éléments applicables prévus dans les lignes directrices de l'Union en matière d'éthique pour une IA digne de confiance;

b) l'évaluation et la réduction au minimum de l'incidence des systèmes d'IA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficaces de l'IA;

c) la promotion de la maîtrise de l'IA, en particulier chez les personnes chargées du développement, du fonctionnement et de l'utilisation de l'IA;

d) la facilitation d'une conception inclusive et diversifiée des systèmes d'IA, notamment par la mise en place d'équipes de développement inclusives et diversifiées et la promotion de la participation des parties prenantes à ce processus;

e) l'évaluation et la prévention de l'impact négatif des systèmes d'IA sur les personnes ou groupes de personnes vulnérables, y compris en ce qui concerne l'accessibilité pour les personnes handicapées, ainsi que sur l'égalité de genre.

3. Les codes de conduite peuvent être élaborés par des fournisseurs ou déployeurs individuels de systèmes d'IA ou par des organisations les représentant ou par les deux, y compris avec la participation de toute partie intéressée et de leurs organisations représentatives, y compris des organisations de la société civile et le monde universitaire. Les codes de conduite peuvent porter sur un ou plusieurs systèmes d'IA, compte tenu de la similarité de la destination des systèmes concernés.

4. Le Bureau de l'IA et les États membres prennent en considération les intérêts et les besoins spécifiques des PME, y compris les jeunes pousses, lorsqu'ils encouragent et facilitent l'élaboration de codes de conduite.

*Article 96*

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

1. La Commission élabore des lignes directrices sur la mise en œuvre pratique du présent règlement, et en particulier sur:

a) l'application des exigences et obligations visées aux articles 8 à 15 et à l'article 25;

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

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

d) la mise en œuvre pratique des obligations de transparence prévues à l'article 50;

e) des informations détaillées sur la relation entre le présent règlement et la législation d'harmonisation de l'Union dont la liste figure à l'annexe I ainsi que d'autres actes législatifs pertinents de l'Union, y compris en ce qui concerne la cohérence de leur application;

f) l'application de la définition d'un système d'IA telle qu'elle figure à l'article 3, point 1).

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

Les lignes directrices visées au premier alinéa du présent paragraphe tiennent dûment compte de l'état de la technique généralement reconnu en matière d'IA, ainsi que des normes harmonisées et spécifications communes pertinentes visées aux articles 40 et 41, ou des normes harmonisées ou spécifications techniques qui sont énoncées en vertu de la législation d'harmonisation de l'Union.

2. À la demande des États membres ou du Bureau de l'IA, ou de sa propre initiative, la Commission met à jour les lignes directrices précédemment adoptées lorsque cela est jugé nécessaire.

## CHAPITRE XI
## DÉLÉGATION DE POUVOIR ET PROCÉDURE DE COMITÉ

*Article 97*

### Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, est conféré à la Commission pour une durée de cinq ans à partir du 1er août 2024. La Commission élabore un rapport relatif à la délégation de pouvoir au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prorogation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 6, paragraphes 6 et 7, à l'article 7, paragraphes 1 et 3, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, à l'article 47, paragraphe 5, à l'article 51, paragraphe 3, à l'article 52, paragraphe 4, et à l'article 53, paragraphes 5 et 6, peut être révoquée à tout moment par le Parlement européen ou le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle ne porte pas atteinte à la validité des actes délégués déjà en vigueur.

4. Avant l'adoption d'un acte délégué, la Commission consulte les experts désignés par chaque État membre, conformément aux principes définis dans l'accord interinstitutionnel du 13 avril 2016«Mieux légiférer».

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

6. Un acte délégué adopté en vertu de l'article 6, paragraphe 6 ou 7, de l'article 7, paragraphe 1 ou 3, de l'article 11, paragraphe 3, de l'article 43, paragraphe 5 ou 6, de l'article 47, paragraphe 5, de l'article 51, paragraphe 3, de l'article 52, paragraphe 4, ou de l'article 53, paragraphe 5 ou 6, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la

Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

*Article 98*

**Comité**

1. La Commission est assistée par un comité. Ledit comité est un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 s'applique.

## CHAPITRE XII
## SANCTIONS

*Article 99*

**Sanctions**

1. Conformément aux conditions établies dans le présent règlement, les États membres déterminent le régime des sanctions et autres mesures d'exécution, qui peuvent également comprendre des avertissements et des mesures non monétaires, applicables aux violations du présent règlement commises par des opérateurs, et prennent toute mesure nécessaire pour veiller à la mise en œuvre correcte et effective de ces sanctions, tenant ainsi compte des lignes directrices publiées par la Commission en vertu de l'article 96. Ces sanctions doivent être effectives, proportionnées et dissuasives. Elles tiennent compte des intérêts des PME, y compris les jeunes pousses, et de leur viabilité économique.

2. Les États membres informent la Commission, sans retard et au plus tard à la date d'entrée en application, du régime des sanctions et des autres mesures d'exécution visées au paragraphe 1, de même que de toute modification apportée ultérieurement à ce régime ou à ces mesures.

3. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'amendes administratives pouvant aller jusqu'à 35 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 7 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

4. La non-conformité avec l'une quelconque des dispositions suivantes relatives aux opérateurs ou aux organismes notifiés, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 15 000 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 3 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu:

a) les obligations incombant aux fournisseurs en vertu de l'article 16;

b) les obligations incombant aux mandataires en vertu de l'article 22;

c) les obligations incombant aux importateurs en vertu de l'article 23;

d) les obligations incombant aux distributeurs en vertu de l'article 24;

e) les obligations incombant aux déployeurs en vertu de l'article 26;

f) les exigences et obligations applicables aux organismes notifiés en application de l'article 31, de l'article 33, paragraphes 1, 3 et 4, ou de l'article 34;

g) les obligations de transparence pour les fournisseurs et les déployeurs conformément à l'article 50.

5. La fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales compétentes en réponse à une demande fait l'objet d'une amende administrative pouvant aller jusqu'à 7 500 000 EUR ou, si l'auteur de l'infraction est une entreprise, jusqu'à 1 % de son chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, le montant le plus élevé étant retenu.

6. Dans le cas des PME, y compris les jeunes pousses, chaque amende visée au présent article s'élève au maximum aux pourcentages ou montants visés aux paragraphes 3, 4 et 5, le chiffre le plus faible étant retenu.

7. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et, le cas échéant, il est tenu compte des éléments suivants:

a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné, ainsi que, le cas échéant, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;

b) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités de surveillance du marché au même opérateur pour la même violation;

c) la question de savoir si des amendes administratives ont déjà été imposées par d'autres autorités au même opérateur pour des violations d'autres dispositions du droit de l'Union ou du droit national, lorsque ces violations résultent de la même activité ou omission constituant une violation pertinente au sens du présent règlement;

d) la taille, le chiffre d'affaires annuel et la part de marché de l'opérateur qui commet la violation;

e) toute autre circonstance aggravante ou atténuante applicable aux circonstances de l'espèce, telle que les avantages financiers obtenus ou les pertes évitées, directement ou indirectement, du fait de la violation;

f) le degré de coopération établi avec les autorités nationales compétentes en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs;

g) le degré de responsabilité de l'opérateur, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;

h) la manière dont les autorités nationales compétentes ont eu connaissance de la violation, notamment si, et dans quelle mesure, l'opérateur a notifié la violation;

i) le fait que la violation a été commise délibérément ou par négligence;

j) toute mesure prise par l'opérateur pour atténuer le préjudice subi par les personnes concernées.

8. Chaque État membre établit les règles déterminant dans quelle mesure des amendes administratives peuvent être imposées à des autorités et organismes publics établis sur son territoire.

9. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que les amendes sont imposées par les juridictions nationales compétentes ou par d'autres organismes, selon le cas prévu dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

10. L'exercice des pouvoirs conférés par le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et au droit national, y compris des recours juridictionnels effectifs et une procédure régulière.

11. Les États membres font rapport chaque année à la Commission sur les amendes administratives qu'ils ont infligées au cours de l'année concernée, conformément au présent article, ainsi que sur toute action en justice ou procédure judiciaire connexe.

*Article 100*

**Amendes administratives imposées aux institutions, organes et organismes de l'Union**

1. Le Contrôleur européen de la protection des données peut imposer des amendes administratives aux institutions, organes et organismes de l'Union relevant du champ d'application du présent règlement. Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative dans chaque cas d'espèce, toutes les caractéristiques propres à chaque cas sont prises en considération et il est dûment tenu compte des éléments suivants:

a) la nature, la gravité et la durée de la violation et de ses conséquences, compte tenu de la finalité du système d'IA concerné ainsi que, s'il y a lieu, du nombre de personnes touchées et du niveau de dommage qu'elles ont subi;

b) le degré de responsabilité de l'institution, organe ou organisme de l'Union, compte tenu des mesures techniques et organisationnelles qu'il a mises en œuvre;

c) toute mesure prise par l'institution, organe ou organisme de l'Union pour atténuer les dommages subis par les personnes touchées;

d) le niveau de coopération établi avec le Contrôleur européen de la protection des données en vue de remédier à la violation et d'en atténuer les éventuels effets négatifs, y compris le respect de toute mesure précédemment ordonnée par le Contrôleur européen de la protection des données à l'encontre de l'institution, organe ou organisme de l'Union concerné pour le même objet;

e) toute violation similaire commise précédemment par l'institution, organe ou organisme de l'Union;

f) la manière dont le Contrôleur européen de la protection des données a eu connaissance de la violation, notamment si, et le cas échéant dans quelle mesure, l'institution, organe ou organisme de l'Union a notifié la violation;

g) le budget annuel de l'institution, organe ou organisme de l'Union.

2. Le non-respect de l'interdiction des pratiques en matière d'IA visées à l'article 5 fait l'objet d'une amende administrative pouvant aller jusqu'à 1 500 000 EUR.

3. La non-conformité du système d'IA avec les exigences ou obligations au titre du présent règlement, autres que celles énoncées à l'article 5, fait l'objet d'une amende administrative pouvant aller jusqu'à 750 000 EUR.

4. Avant de prendre des décisions en vertu du présent article, le Contrôleur européen de la protection des données donne à l'institution, organe ou organisme de l'Union faisant l'objet des procédures conduites par le Contrôleur européen de la protection des données la possibilité de faire connaître son point de vue sur l'éventuelle infraction. Le Contrôleur européen de la protection des données ne fonde ses décisions que sur les éléments et les circonstances au sujet desquels les parties concernées ont pu formuler des observations. Les éventuels plaignants sont étroitement associés à la procédure.

5. Les droits de la défense des parties concernées sont pleinement respectés dans le déroulement de la procédure. Les parties disposent d'un droit d'accès au dossier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou entreprises concernées en ce qui concerne la protection de leurs données à caractère personnel ou de leurs secrets commerciaux.

6. Les fonds collectés en imposant des amendes en vertu du présent article contribuent au budget général de l'Union. Les amendes ne compromettent pas le bon fonctionnement de l'institution, organe ou organisme de l'Union faisant l'objet d'une amende.

7. Le Contrôleur européen de la protection des données informe chaque année la Commission des amendes administratives qu'il a infligées en vertu du présent article ainsi que de toute action en justice ou procédure judiciaire qu'il a engagée.

*Article 101*

**Amendes applicables aux fournisseurs de modèles d'IA à usage général**

1. La Commission peut infliger aux fournisseurs de modèles d'IA à usage général des amendes n'excédant pas 3 % de leur chiffre d'affaires annuel mondial total réalisé au cours de l'exercice précédent, ou 15 000 000 EUR, le montant le plus élevé étant retenu, lorsque la Commission constate que le fournisseur, de manière délibérée ou par négligence:

a) a enfreint les dispositions pertinentes du présent règlement;

b) n'a pas donné suite à une demande de document ou d'informations au titre de l'article 91, ou a fourni des informations inexactes, incomplètes ou trompeuses;

c) ne s'est pas conformé à une mesure demandée au titre de l'article 93;

d) n'a pas donné à la Commission accès au modèle d'IA à usage général ou au modèle d'IA à usage général présentant un risque systémique en vue de procéder à une évaluation conformément à l'article 92.

Pour fixer le montant de l'amende ou de l'astreinte, il y a lieu de prendre en considération la nature, la gravité et la durée de la violation, tout en tenant dûment compte des principes de proportionnalité et d'adéquation. La Commission tient également compte des engagements pris conformément à l'article 93, paragraphe 3, ou pris dans les codes de bonne pratique pertinents conformément à l'article 56.

2. Avant d'adopter la décision en vertu du paragraphe 1, la Commission communique ses constatations préliminaires au fournisseur du modèle d'IA à usage général, et lui donne la possibilité d'être entendu.

3. Les amendes infligées conformément au présent article sont effectives, proportionnées et dissuasives.

4. Les informations relatives aux amendes infligées en vertu du présent article sont en outre communiquées au Comité IA, le cas échéant.

5. La Cour de justice de l'Union européenne statue avec compétence de pleine juridiction sur les recours formés contre les décisions par lesquelles la Commission a fixé une amende au titre du présent article. Elle peut supprimer, réduire ou majorer l'amende infligée.

6. La Commission adopte des actes d'exécution contenant les modalités détaillées des procédures et des garanties procédurales en vue de l'adoption éventuelle de décisions en vertu du paragraphe 1 du présent article. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 98, paragraphe 2.

## CHAPITRE XIII
## DISPOSITIONS FINALES

*Article 102*

### Modification du règlement (CE) nº 300/2008

À l'article 4, paragraphe 3, du règlement (CE) nº 300/2008, l'alinéa suivant est ajouté:

«Lors de l'adoption de mesures détaillées relatives aux spécifications techniques et aux procédures d'approbation et d'utilisation des équipements de sûreté en ce qui concerne les systèmes d'intelligence artificielle au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*1]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 103*

### Modification du règlement (UE) nº 167/2013

À l'article 17, paragraphe 5, du règlement (UE) nº 167/2013, l'alinéa suivant est ajouté:

«Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*2]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 104*

### Modification du règlement (UE) nº 168/2013

À l'article 22, paragraphe 5, du règlement (UE) nº 168/2013, l'alinéa suivant est ajouté:

«Lors de l'adoption d'actes délégués conformément au premier alinéa en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*3]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 105*

**Modification de la directive 2014/90/UE**

À l'article 8 de la directive 2014/90/UE, le paragraphe suivant est ajouté:

«5. Pour les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*4]), lorsqu'elle exerce ses activités conformément au paragraphe 1 et qu'elle adopte des spécifications techniques et des normes d'essai conformément aux paragraphes 2 et 3, la Commission tient compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 106*

**Modification de la directive (UE) 2016/797**

À l'article 5 de la directive (UE) 2016/797, le paragraphe suivant est ajouté:

«12. Lors de l'adoption d'actes délégués conformément au paragraphe 1 et d'actes d'exécution conformément au paragraphe 11 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*5]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 107*

**Modification du règlement (UE) 2018/858**

À l'article 5 du règlement (UE) 2018/858, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes délégués conformément au paragraphe 3 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*6]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 108*

**Modifications du règlement (UE) 2018/1139**

Le règlement (UE) 2018/1139 est modifié comme suit:

1) À l'article 17, le paragraphe suivant est ajouté:

«3. Sans préjudice du paragraphe 2, lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*7]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

([*7]) Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).»."

2) À l'article 19, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

3) À l'article 43, le paragraphe suivant est ajouté:

«4. Lors de l'adoption d'actes d'exécution conformément au paragraphe 1 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

4) À l'article 47, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

5) À l'article 57, le paragraphe suivant est ajouté:

«Lors de l'adoption de ces actes d'exécution en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

6) À l'article 58, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes délégués conformément aux paragraphes 1 et 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689, il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.».

*Article 109*

**Modification du règlement (UE) 2019/2144**

À l'article 11 du règlement (UE) 2019/2144, le paragraphe suivant est ajouté:

«3. Lors de l'adoption d'actes d'exécution conformément au paragraphe 2 en ce qui concerne les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) 2024/1689 du Parlement européen et du Conseil ([*8]), il est tenu compte des exigences énoncées au chapitre III, section 2, dudit règlement.

*Article 110*

**Modification de la directive (UE) 2020/1828**

À l'annexe I de la directive (UE) 2020/1828 du Parlement européen et du Conseil ([58]), le point suivant est ajouté:

«68)Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur

l'intelligence artificielle) (JO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

*Article 111*

**Systèmes d'IA déjà mis sur le marché ou mis en service et modèles d'IA à usage général déjà mis sur le marché**

1. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), les systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe X et mis sur le marché ou mis en service avant le 2 août 2027 sont mis en conformité avec le présent règlement au plus tard le 31 décembre 2030.

Il est tenu compte des exigences énoncées dans le présent règlement lors de l'évaluation de chaque système d'information à grande échelle établi par les actes juridiques énumérés à l'annexe X devant être effectuée conformément à ces actes juridiques et lorsque ces actes juridiques sont remplacés ou modifiés.

2. Sans préjudice de l'application de l'article 5 visée à l'article 113, paragraphe 3, point a), le présent règlement s'applique aux opérateurs de systèmes d'IA à haut risque, autres que les systèmes visés au paragraphe 1 du présent article, qui ont été mis sur le marché ou mis en service avant le 2 août 2026, uniquement si, à compter de cette date, ces systèmes subissent d'importantes modifications de leurs conceptions. En tout état de cause, les fournisseurs et les déployeurs de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques prennent les mesures nécessaires pour se conformer aux exigences et obligations du présent règlement au plus tard le 2 août 2030.

3. Les fournisseurs de modèles d'IA à usage général qui ont été mis sur le marché avant le 2 août 2025 prennent les mesures nécessaires pour se conformer aux obligations prévues par le présent règlement au plus tard le 2 août 2027.

*Article 112*

**Évaluation et réexamen**

1. La Commission évalue la nécessité de modifier la liste figurant à l'annexe III et la liste des pratiques d'IA interdites figurant à l'article 5, une fois par an après l'entrée en vigueur du présent règlement et jusqu'à la fin de la période de délégation de pouvoir énoncée à l'article 97. La Commission transmet les conclusions de cette évaluation au Parlement européen et au Conseil.

2. Au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission évalue le présent règlement et fait rapport au Parlement européen et au Conseil sur les éléments suivants:

a) la nécessité de modifications pour étendre des rubriques de domaine existantes ou ajouter de nouvelles rubriques de domaine dans l'annexe III;

b) les modifications de la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires au titre de l'article 50;

c) les modifications visant à renforcer l'efficacité du système de surveillance et de gouvernance.

3. Au plus tard le 2 août 2029 et tous les quatre ans par la suite, la Commission présente au Parlement européen et au Conseil un rapport sur l'évaluation et le réexamen du présent règlement.

Le rapport comprend une évaluation en ce qui concerne la structure de contrôle de l'application ainsi que l'éventuelle nécessité d'une agence de l'Union pour remédier aux lacunes identifiées. Sur la base des constatations, ce rapport est, le cas échéant, accompagné d'une proposition de modification du présent règlement. Les rapports sont publiés.

4. Les rapports visés au paragraphe 2 prêtent une attention particulière aux éléments suivants:

a) l'état des ressources financières, techniques et humaines dont les autorités nationales compétentes ont besoin pour mener efficacement à bien les missions qui leur sont dévolues par le présent règlement;

b) l'état des sanctions, notamment les amendes administratives visées à l'article 99, paragraphe 1, appliquées par les États membres en cas de violation du présent règlement;

c) les normes harmonisées adoptées et les spécifications communes élaborées à l'appui du présent règlement;

d) le nombre d'entreprises qui arrivent sur le marché après l'entrée en application du présent règlement, et combien d'entre elles sont des PME.

5. Au plus tard le 2 août 2028, la Commission évalue le fonctionnement du Bureau de l'IA, afin de déterminer si des pouvoirs et compétences suffisants lui ont été conférés pour s'acquitter de ses tâches, et s'il serait pertinent et nécessaire pour la bonne mise en œuvre et l'application correcte du présent règlement de renforcer le Bureau de l'IA et ses compétences d'exécution et d'accroître ses ressources. La Commission présente un rapport sur son évaluation au Parlement européen et au Conseil.

6. Au plus tard le 2 août 2028 et tous les quatre ans par la suite, la Commission présente un rapport sur l'examen de l'état d'avancement des travaux de normalisation concernant le développement économe en énergie de modèles d'IA à usage général, et évalue la nécessité de mesures ou d'actions supplémentaires, y compris de mesures ou d'actions contraignantes. Ce rapport est présenté au Parlement européen et au Conseil et il est rendu public.

7. Au plus tard le 2 août 2028 et tous les trois ans par la suite, la Commission évalue l'impact et l'efficacité des codes de conduite volontaires destinés à favoriser l'application des exigences énoncées au chapitre III, section 2, pour les systèmes d'IA autres que les systèmes d'IA à haut risque, et éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à haut risque, y compris en ce qui concerne la durabilité environnementale.

8. Aux fins des paragraphes 1 à 7, le Comité IA, les États membres et les autorités nationales compétentes fournissent des informations à la Commission à la demande de cette dernière et sans retard injustifié.

9. Lorsqu'elle procède aux évaluations et réexamens visés aux paragraphes 1 à 7, la Commission tient compte des positions et des conclusions du Comité IA, du Parlement européen, du Conseil et d'autres organismes ou sources pertinents.

10. La Commission soumet, si nécessaire, des propositions appropriées visant à modifier le présent règlement, notamment en tenant compte de l'évolution des technologies, de l'effet des systèmes d'IA sur la santé et la sécurité, ainsi que sur les droits fondamentaux, et à la lumière de l'état d'avancement de la société de l'information.

11. Pour orienter les évaluations et les réexamens visés aux paragraphes 1 à 7 du présent article, le Bureau de l'IA entreprend de mettre au point une méthode objective et participative pour l'évaluation des niveaux de risque fondée sur les critères décrits dans les articles pertinents et l'inclusion de nouveaux systèmes dans:

a) la liste figurant à l'annexe III, y compris l'extension des rubriques de domaine existantes ou l'ajout de nouvelles rubriques de domaine dans ladite annexe;

b) la liste des pratiques interdites figurant à l'article 5; et

c) la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires en application de l'article 50.

12. Toute modification du présent règlement en vertu du paragraphe 10, ou tout acte délégué ou acte d'exécution pertinent, qui concerne la législation d'harmonisation de l'Union dont la liste figure à l'annexe I, section B, tient compte des spécificités réglementaires de chaque secteur, ainsi et des mécanismes de gouvernance, d'évaluation de la conformité et d'applications existants et des autorités qui y sont établies.

13. Au plus tard le 2 août 2031, la Commission procède à une évaluation de sa mise en application dont elle fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte des premières années d'application du présent règlement. Sur la base des conclusions, ce rapport est accompagné, le cas échéant, d'une proposition de modification du présent règlement en ce qui concerne la structure de contrôle de l'application ainsi que la nécessité d'une agence de l'Union pour remédier aux lacunes identifiées.

*Article 113*

**Entrée en vigueur et application**

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Il est applicable à partir du 2 août 2026.

Toutefois:

a) les chapitres I et II sont applicables à partir du 2 février 2025;

b) le chapitre III, section 4, le chapitre V, le chapitre VII, le chapitre XII et l'article 78 s'appliquent à partir du 2 août 2025, à l'exception de l'article 101;

c) l'article 6, paragraphe 1, et les obligations correspondantes du présent règlement s'appliquent à partir du 2 août 2027.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Bruxelles, le 13 juin 2024.

*Par le Parlement européen*

*La présidente*

R. METSOLA

*Par le Conseil*

*Le président*

M. MICHEL

([1]) JO C 517 du 22.12.2021, p. 56.

([2]) JO C 115 du 11.3.2022, p. 5.

([3]) JO C 97 du 28.2.2022, p. 60.

([4]) Position du Parlement européen du 13 mars 2024 (non encore parue au Journal officiel) et décision du Conseil du 21 mai 2024.

([5]) Conseil européen, réunion extraordinaire du Conseil européen (1er et 2 octobre 2020) — Conclusions, EUCO 13/20, 2020, p. 6.

([6]) Résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes, 2020/2012 (INL).

([7]) Règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et abrogeant le règlement (CEE) nº 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

([8]) Décision nº 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil (JO L 218 du 13.8.2008, p. 82).

([9]) Règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) nº 765/2008 et (UE) nº 305/2011 (JO L 169 du 25.6.2019, p. 1).

([10]) Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux (JO L 210 du 7.8.1985, p. 29).

([11]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([12]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([13]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

([14]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37).

([15]) Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) (JO L 277 du 27.10.2022, p. 1).

([16]) Directive (UE) 2019/882 du Parlement européen et du Conseil du 17 avril 2019 relative aux exigences en matière d'accessibilité applicables aux produits et services (JO L 151 du 7.6.2019, p. 70).

([17]) Directive nº 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) nº 2006/2004 du Parlement européen et du Conseil («directive sur les pratiques commerciales déloyales») (JO L 149 du 11.6.2005, p. 22).

([18]) Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres (JO L 190 du 18.7.2002, p. 1).

([19]) Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques, et abrogeant la directive 2008/114/CE du Conseil (JO L 333 du 27.12.2022, p. 164).

([20]) JO C 247 du 29.6.2022, p. 1.

([21]) 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).

([22]) 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).

([23]) Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24).

([24]) 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).

([25]) 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).

([26]) 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).

([27]) 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).

([28]) 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).

([29]) Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) n° 715/2007 et (CE) n° 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

([30]) Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1).

([31]) Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) n° 78/2009, (CE) n° 79/2009 et (CE) n° 661/2009 du Parlement européen et du Conseil et les règlements (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1).

([32]) Règlement (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).

([33]) Directive 2013/32/UE du Parlement européen et du Conseil du 26 juin 2013 relative à des procédures communes pour l'octroi et le retrait de la protection internationale (JO L 180 du 29.6.2013, p. 60).

([34]) Règlement (UE) 2024/900 du Parlement européen et du Conseil du 13 mars 2024 relatif à la transparence et au ciblage de la publicité à caractère politique (JO L, 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

([35]) Directive 2014/31/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des instruments de pesage à fonctionnement non automatique (JO L 96 du 29.3.2014, p. 107).

([36]) Directive 2014/32/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'instruments de mesure (JO L 96 du 29.3.2014, p. 149).

([37]) Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) (JO L 151 du 7.6.2019, p. 15).

([38]) Directive (UE) 2016/2102 du Parlement européen et du Conseil du 26 octobre 2016 relative à l'accessibilité des sites internet et des applications mobiles des organismes du secteur public (JO L 327 du 2.12.2016, p. 1).

([39]) Directive 2002/14/CE du Parlement européen et du Conseil du 11 mars 2002 établissant un cadre général relatif à l'information et la consultation des travailleurs dans la Communauté européenne (JO L 80 du 23.3.2002, p. 29).

([40]) Directive (UE) 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE (JO L 130 du 17.5.2019, p. 92).

([41]) 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 ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

([42]) Règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) (JO L 152 du 3.6.2022, p. 1).

([43]) Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données) (JO L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

([44]) 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).

([45]) Décision de la Commission du 24 janvier 2024 créant le Bureau européen de l'intelligence artificielle (C/2024/390).

([46]) Règlement (UE) n° 575/2013 du Parlement européen et du Conseil du 26 juin 2013 concernant les exigences prudentielles applicables aux établissements de crédit et aux entreprises d'investissement et modifiant le règlement (UE) n° 648/2012 (JO L 176 du 27.6.2013, p. 1).

([47]) Directive 2008/48/CE du Parlement européen et du Conseil du 23 avril 2008 concernant les contrats de crédit aux consommateurs et abrogeant la directive 87/102/CEE du Conseil (JO L 133 du 22.5.2008, p. 66).

([48]) Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II) (JO L 335 du 17.12.2009, p. 1).

([49]) 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).

([50]) Directive 2014/17/UE du Parlement européen et du Conseil du 4 février 2014 sur les contrats de crédit aux consommateurs relatifs aux biens immobiliers à usage résidentiel et modifiant les directives 2008/48/CE et 2013/36/UE et le règlement (UE) n° 1093/2010 (JO L 60 du 28.2.2014, p. 34).

([51]) Directive (UE) 2016/97 du Parlement européen et du Conseil du 20 janvier 2016 sur la distribution d'assurances (JO L 26 du 2.2.2016, p. 19).

([52]) Règlement (UE) n° 1024/2013 du Conseil du 15 octobre 2013 confiant à la Banque centrale européenne des missions spécifiques ayant trait aux politiques en matière de surveillance prudentielle des établissements de crédit (JO L 287 du 29.10.2013, p. 63).

([53]) Règlement (UE) 2023/988 du Parlement européen et du Conseil du 10 mai 2023 relatif à la sécurité générale des produits, modifiant le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil et la directive (UE) 2020/1828 du Parlement européen et du Conseil, et abrogeant la directive 2001/95/CE du Parlement européen et du Conseil et la directive 87/357/CEE du Conseil (JO L 135 du 23.5.2023, p. 1).

([54]) Directive (UE) 2019/1937 du Parlement européen et du Conseil du 23 octobre 2019 sur la protection des personnes qui signalent des violations du droit de l'Union (JO L 305 du 26.11.2019, p. 17).

([55]) JO L 123 du 12.5.2016, p. 1.

([56]) 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).

([57]) Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites (JO L 157 du 15.6.2016, p. 1).

([58]) Directive (UE) 2020/1828 du Parlement européen et du Conseil du 25 novembre 2020 relative aux actions représentatives visant à protéger les intérêts collectifs des consommateurs et abrogeant la directive 2009/22/CE (JO L 409 du 4.12.2020, p. 1).

## ANNEXE I

### Liste de la législation d'harmonisation de l'Union

### Section A. Liste de la législation d'harmonisation de l'Union fondée sur le nouveau cadre législatif

1. Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24);
2. Directive 2009/48/CE du Parlement européen et du Conseil du 18 juin 2009 relative à la sécurité des jouets (JO L 170 du 30.6.2009, p. 1);
3. Directive 2013/53/UE du Parlement européen et du Conseil du 20 novembre 2013 relative aux bateaux de plaisance et aux véhicules nautiques à moteur et abrogeant la directive 94/25/CE (JO L 354 du 28.12.2013, p. 90);
4. Directive 2014/33/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les ascenseurs et les composants de sécurité pour ascenseurs (JO L 96 du 29.3.2014, p. 251);
5. Directive 2014/34/UE du Parlement européen et du Conseil du 26 février 2014 relative à l'harmonisation des législations des États membres concernant les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles (JO L 96 du 29.3.2014, p. 309);
6. Directive 2014/53/UE du Parlement européen et du Conseil du 16 avril 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché d'équipements radioélectriques et abrogeant la directive 1999/5/CE (JO L 153 du 22.5.2014, p. 62);
7. Directive 2014/68/UE du Parlement européen et du Conseil du 15 mai 2014 relative à l'harmonisation des législations des États membres concernant la mise à disposition sur le marché des équipements sous pression (JO L 189 du 27.6.2014, p. 164);
8. Règlement (UE) 2016/424 du Parlement européen et du Conseil du 9 mars 2016 relatif aux installations à câbles et abrogeant la directive 2000/9/CE (JO L 81 du 31.3.2016, p. 1);
9. Règlement (UE) 2016/425 du Parlement européen et du Conseil du 9 mars 2016 relatif aux équipements de protection individuelle et abrogeant la directive 89/686/CEE du Conseil (JO L 81 du 31.3.2016, p. 51);
10. Règlement (UE) 2016/426 du Parlement européen et du Conseil du 9 mars 2016 concernant les appareils brûlant des combustibles gazeux et abrogeant la directive 2009/142/CE (JO L 81 du 31.3.2016, p. 99);
11. Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et

le règlement (CE) nº 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE (JO L 117 du 5.5.2017, p. 1);

12. Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

**Section B. Liste des autres législations d'harmonisation de l'Union**

13. Règlement (CE) nº 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile et abrogeant le règlement (CE) nº 2320/2002 (JO L 97 du 9.4.2008, p. 72);
14. Règlement (UE) nº 168/2013 du Parlement européen et du Conseil du 15 janvier 2013 relatif à la réception et à la surveillance du marché des véhicules à deux ou trois roues et des quadricycles (JO L 60 du 2.3.2013, p. 52);
15. Règlement (UE) nº 167/2013 du Parlement européen et du Conseil du 5 février 2013 relatif à la réception et à la surveillance du marché des véhicules agricoles et forestiers (JO L 60 du 2.3.2013, p. 1);
16. Directive 2014/90/UE du Parlement européen et du Conseil du 23 juillet 2014 relative aux équipements marins et abrogeant la directive 96/98/CE du Conseil (JO L 257 du 28.8.2014, p. 146);
17. Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44);
18. Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, modifiant les règlements (CE) nº 715/2007 et (CE) nº 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1);
19. Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions applicables à la réception par type des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques distinctes destinés à ces véhicules, en ce qui concerne leur sécurité générale et la protection des occupants des véhicules et des usagers vulnérables de la route, modifiant le règlement (UE) 2018/858 du Parlement européen et du Conseil et abrogeant les règlements (CE) nº 78/2009, (CE) nº 79/2009 et (CE) nº 661/2009 du Parlement européen et du Conseil et les règlements (CE) nº 631/2009, (UE) nº 406/2010, (UE) nº 672/2010, (UE) nº 1003/2010, (UE) nº 1005/2010, (UE) nº 1008/2010, (UE) nº 1009/2010, (UE) nº 19/2011, (UE) nº 109/2011, (UE) nº 458/2011, (UE) nº 65/2012, (UE) nº 130/2012, (UE) nº 347/2012, (UE) nº 351/2012, (UE) nº 1230/2012 et (UE) 2015/166 de la Commission (JO L 325 du 16.12.2019, p. 1);
20. Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) nº 2111/2005, (CE) nº 1008/2008, (UE) nº 996/2010, (UE) nº 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les

règlements (CE) nº 552/2004 et (CE) nº 216/2008 du Parlement européen et du Conseil et le règlement (CEE) nº 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1), dans la mesure où il concerne la conception, la production et la mise sur le marché des aéronefs visés à son article 2, paragraphe 1, points a) et b), lorsque cela concerne des aéronefs sans équipage à bord et leurs moteurs, hélices, pièces et équipements de contrôle à distance.

## ANNEXE II

### Liste des infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii)

Infractions pénales visées à l'article 5, paragraphe 1, premier alinéa, point h) iii):

— terrorisme,

— traite des êtres humains,

— exploitation sexuelle des enfants et pédopornographie,

— trafic de stupéfiants ou de substances psychotropes,

— trafic d'armes, de munitions ou d'explosifs,

— homicide volontaire, coups et blessures graves,

— trafic d'organes ou de tissus humains,

— trafic de matières nucléaires ou radioactives,

— enlèvement, séquestration ou prise d'otage,

— crimes relevant de la compétence de la Cour pénale internationale,

— détournement d'avion ou de navire,

— viol,

— criminalité environnementale,

— vol organisé ou à main armée,

— sabotage,

— participation à une organisation criminelle impliquée dans une ou plusieurs des infractions énumérées ci-dessus.

## ANNEXE III

### Systèmes d'IA à haut risque visés à l'article 6, paragraphe 2

Les systèmes d'IA à haut risque au sens de l'article 6, paragraphe 2, sont les systèmes d'IA répertoriés dans l'un des domaines suivants:

1. Biométrie, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

   a) systèmes d'identification biométrique à distance.

      Cela n'inclut pas les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique dont la seule finalité est de confirmer qu'une personne physique spécifique est

la personne qu'elle prétend être;

b) systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique, en fonction d'attributs ou de caractéristiques sensibles ou protégés, sur la base de la déduction de ces attributs ou de ces caractéristiques;

c) systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions.

2. Infrastructures critiques: systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité.

3. Éducation et formation professionnelle:

a) systèmes d'IA destinés à être utilisés pour déterminer l'accès, l'admission ou l'affectation de personnes physiques à des établissements d'enseignement et de formation professionnelle, à tous les niveaux;

b) systèmes d'IA destinés à être utilisés pour évaluer les acquis d'apprentissage, y compris lorsque ceux-ci sont utilisés pour orienter le processus d'apprentissage de personnes physiques dans les établissements d'enseignement et de formation professionnelle, à tous les niveaux;

c) systèmes d'IA destinés à être utilisés pour évaluer le niveau d'enseignement approprié qu'une personne recevra ou sera en mesure d'atteindre, dans le contexte ou au sein d'établissements d'enseignement et de formation professionnelle à tous les niveaux;

d) systèmes d'IA destinés à être utilisés pour surveiller et détecter des comportements interdits chez les étudiants lors d'examens dans le contexte d'établissements d'enseignement et de formation ou en leur sein à tous les niveaux;

4. Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant:

a) systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, en particulier pour publier des offres d'emploi ciblées, analyser et filtrer les candidatures et évaluer les candidats;

b) systèmes d'IA destinés à être utilisés pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalité ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations.

5. Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels:

a) systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soins de santé, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services;

b) systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières;

c) systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie;

d) systèmes d'IA destinés à évaluer et hiérarchiser les appels d'urgence émanant de personnes physiques ou à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par la police, les pompiers et l'assistance médicale, ainsi que pour les systèmes de tri des patients admis dans les services de santé d'urgence.

6. Répression, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

a) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives ou en leur nom pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales;

b) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives, en tant que polygraphes ou outils similaires;

c) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales;

d) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer le risque qu'une personne physique commette une infraction ou récidive, sans se fonder uniquement sur le profilage des personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes;

e) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre de la détection d'infractions pénales, d'enquêtes ou de poursuites en la matière ou de l'exécution de sanctions pénales.

7. Migration, asile et gestion des contrôles aux frontières, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable:

a) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, en tant que polygraphes et outils similaires;

b) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour évaluer un risque, y compris un risque pour la sécurité, un risque de migration irrégulière ou un risque pour la santé, posé par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre;

c) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, pour aider les autorités

publiques compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, y compris les évaluations connexes de la fiabilité des éléments de preuve;

d) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou par les institutions, organes ou organismes de l'Union, ou en leur nom, dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques, à l'exception de la vérification des documents de voyage.

8. Administration de la justice et processus démocratiques:

a) systèmes d'IA destinés à être utilisés par les autorités judiciaires ou en leur nom, pour les aider à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits, ou à être utilisés de manière similaire lors du règlement extrajudiciaire d'un litige;

b) systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums. Sont exclus les systèmes d'IA aux sorties desquels les personnes physiques ne sont pas directement exposées, tels que les outils utilisés pour organiser, optimiser ou structurer les campagnes politiques sous l'angle administratif ou logistique.

## ANNEXE IV

### Documentation technique visée à l'article 11, paragraphe 1

La documentation technique visée à l'article 11, paragraphe 1, contient au moins les informations ci-après, selon le système d'IA concerné:

1. une description générale du système d'IA, y compris:

a) la destination, le nom du fournisseur et la version du système, faisant apparaître sa relation aux versions précédentes;

b) la manière dont le système d'IA interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels, y compris avec d'autres systèmes d'IA, qui ne font pas partie du système d'IA lui-même, le cas échéant;

c) les versions des logiciels ou des micrologiciels pertinents et toute exigence relative aux mises à jour de la version;

d) la description de toutes les formes sous lesquelles le système d'IA est mis sur le marché ou mis en service, telles que les packs logiciels intégrés dans du matériel informatique, les téléchargements ou les API;

e) la description du matériel informatique sur lequel le système d'IA est destiné à être exécuté;

f) lorsque le système d'IA est un composant de produits, des photographies ou des illustrations montrant les caractéristiques externes, le marquage et la disposition interne de ces produits;

g) une description de base de l'interface utilisateur fournie au déployeur;

h) une notice d'utilisation à l'intention du déployeur et une description de base de l'interface utilisateur fournie au déployeur, le cas échéant;

2. une description détaillée des éléments du système d'IA et de son processus de développement, y compris:

a) les méthodes et étapes suivies pour le développement du système d'IA, y compris, le cas échéant, le recours à des systèmes ou outils pré-entraînés fournis par des tiers et la manière dont ceux-ci ont été utilisés, intégrés ou modifiés par le fournisseur;

b) les spécifications de conception du système, à savoir la logique générale du système d'IA et des algorithmes; les principaux choix de conception, y compris le raisonnement et les hypothèses retenues, y compris en ce qui concerne les personnes ou les groupes de personnes à l'égard desquels le système est destiné à être utilisé; les principaux choix de classification; ce que le système est conçu pour optimiser, ainsi que la pertinence des différents paramètres; la description des sorties attendues du système et de leur qualité; les décisions relatives aux compromis éventuels en ce qui concerne les solutions techniques adoptées pour se conformer aux exigences énoncées au chapitre III, section 2;

c) la description de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global; les ressources informatiques utilisées pour développer, entraîner, mettre à l'essai et valider le système d'IA;

d) le cas échéant, les exigences relatives aux données en ce qui concerne les fiches décrivant les méthodes et techniques d'entraînement et les jeux de données d'entraînement utilisés, y compris une description générale de ces jeux de données et des informations sur leur provenance, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées; les procédures d'étiquetage (par exemple pour l'apprentissage supervisé), les méthodes de nettoyage des données (par exemple la détection des valeurs aberrantes);

e) l'évaluation des mesures de contrôle humain nécessaires conformément à l'article 14, y compris une évaluation des mesures techniques nécessaires pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA, conformément à l'article 13, paragraphe 3, point d);

f) le cas échéant, une description détaillée des modifications prédéterminées du système d'IA et de ses performances, ainsi que toutes les informations pertinentes relatives aux solutions techniques adoptées pour garantir que continue d'être assurée la conformité du système d'IA aux les exigences pertinentes énoncées au chapitre III, section 2;

g) les procédures de validation et d'essai utilisées, y compris les informations sur les données de validation et d'essai utilisées et leurs principales caractéristiques; les indicateurs utilisés pour mesurer l'exactitude, la robustesse et le respect des autres exigences pertinentes énoncées au chapitre III, section 2, ainsi que les éventuelles incidences discriminatoires; les journaux de test et tous les rapports de test datés et signés par les personnes responsables, y compris en ce qui concerne les modifications prédéterminées visées au point f);

h) les mesures de cybersécurité qui ont été prises;

3. des informations détaillées sur la surveillance, le fonctionnement et le contrôle du système d'IA, en particulier en ce qui concerne: les capacités et les limites du système sur le plan de sa performance, y compris le degré d'exactitude pour des personnes ou des groupes de personnes spécifiques à l'égard desquels le système est destiné à être utilisé et le niveau global d'exactitude prévu par rapport à sa destination; les résultats non intentionnels et sources de risques prévisibles pour la santé et la sécurité, les droits fondamentaux et en termes de discrimination compte tenu de la destination du système d'IA; les mesures de contrôle humain nécessaires conformément à l'article 14, y compris les mesures techniques mises en place pour faciliter l'interprétation par les déployeurs des sorties des systèmes d'IA; les spécifications concernant les données d'entrée, le cas échéant;
4. une description de l'adéquation des indicateurs de performance à ce système d'IA spécifique;
5. une description détaillée du système de gestion des risques conformément à l'article 9;
6. une description des modifications pertinentes apportées par le fournisseur au système tout au long de son cycle de vie;
7. une liste des normes harmonisées appliquées, en totalité ou en partie, dont les références ont été publiées au *Journal officiel de l'Union européenne*; lorsqu'aucune norme harmonisée de ce type n'a été appliquée, une description détaillée des solutions adoptées pour satisfaire aux exigences énoncées au chapitre III, section 2, y compris une liste des autres normes pertinentes et spécifications techniques appliquées;
8. une copie de la déclaration UE de conformité visée à l'article 47;
9. une description détaillée du système en place pour évaluer les performances du système d'IA après la commercialisation conformément à l'article 72, y compris le plan de surveillance après commercialisation visé à l'article 72, paragraphe 3.

## ANNEXE V

### Déclaration UE de conformité

La déclaration UE de conformité visée à l'article 47 contient l'ensemble des informations suivantes:

1. le nom et le type du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
2. le nom et l'adresse du fournisseur ou, le cas échéant, de son mandataire;
3. une attestation certifiant que la déclaration UE de conformité visée à l'article 47 est établie sous la seule responsabilité du fournisseur;
4. une déclaration attestant que le système d'IA respecte le présent règlement et, le cas échéant, toute autre législation de l'Union applicable prévoyant l'établissement de la déclaration UE de conformité visée à l'article 47;
5. lorsqu'un système d'IA nécessite le traitement de données à caractère personnel, une déclaration qui atteste que ledit système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 ainsi qu'à la directive (UE) 2016/680;
6. des références aux éventuelles normes harmonisées pertinentes utilisées ou aux éventuelles autres spécifications communes par rapport auxquelles la conformité est déclarée;

7. le cas échéant, le nom et le numéro d'identification de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré;

8. le lieu et la date de délivrance de la déclaration, le nom et la fonction du signataire ainsi que la mention de la personne pour le compte de laquelle ce dernier a signé, et une signature.

## ANNEXE VI

### Procédure d'évaluation de la conformité fondée sur le contrôle interne

1. La procédure d'évaluation de la conformité fondée sur le contrôle interne est la procédure d'évaluation de la conformité décrite aux points 2, 3 et 4.

2. Le fournisseur vérifie que le système de gestion de la qualité établi est conforme aux exigences de l'article 17.

3. Le fournisseur examine les informations contenues dans la documentation technique afin d'évaluer la conformité du système d'IA aux exigences essentielles pertinentes énoncées au chapitre III, section 2.

4. Le fournisseur vérifie également que le processus de conception et de développement du système d'IA et son système de surveillance après commercialisation prévu à l'article 72 sont cohérents avec la documentation technique.

## ANNEXE VII

### Conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique

#### 1. Introduction

La conformité fondée sur une évaluation du système de gestion de la qualité et une évaluation de la documentation technique est la procédure d'évaluation de la conformité décrite aux points 2 à 5.

#### 2. Vue d'ensemble

Le système de gestion de la qualité approuvé pour la conception, le développement et les essais des systèmes d'IA conformément à l'article 17 est examiné conformément au point 3 et soumis à la surveillance spécifiée au point 5. La documentation technique du système d'IA est examinée conformément au point 4.

#### 3. Système de gestion de la qualité

3.1. La demande du fournisseur comprend:

a) le nom et l'adresse du fournisseur, ainsi que le nom et l'adresse d'un mandataire si la demande est introduite par celui-ci;

b) la liste des systèmes d'IA couverts par le même système de gestion de la qualité;

c) la documentation technique de chaque système d'IA couvert par le même système de gestion de la qualité;

d) la documentation relative au système de gestion de la qualité qui couvre tous les aspects énumérés à l'article 17;

e) une description des procédures en place pour garantir que le système de gestion de la qualité reste adéquat et efficace;

f) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié.

3.2. Le système de gestion de la qualité est évalué par l'organisme notifié, qui détermine s'il satisfait aux exigences visées à l'article 17.

La décision est notifiée au fournisseur ou à son mandataire.

La notification contient les conclusions de l'évaluation du système de gestion de la qualité et la décision d'évaluation motivée.

3.3. Le système de gestion de la qualité tel qu'approuvé continue d'être mis en œuvre et adapté par le fournisseur afin de rester adéquat et efficace.

3.4. Toute modification envisagée du système de gestion de la qualité approuvé ou de la liste des systèmes d'IA couverts par ce dernier est portée à l'attention de l'organisme notifié par le fournisseur.

Les modifications proposées sont examinées par l'organisme notifié, qui décide si le système de gestion de la qualité modifié continue de satisfaire aux exigences visées au point 3.2, ou si une réévaluation est nécessaire.

L'organisme notifié notifie sa décision au fournisseur. La notification contient les conclusions de l'examen des modifications et la décision d'évaluation motivée.

**4. Contrôle de la documentation technique**

4.1. Outre la demande visée au point 3, une demande est déposée par le fournisseur auprès d'un organisme notifié de son choix pour l'évaluation de la documentation technique relative au système d'IA que le fournisseur prévoit de mettre sur le marché ou de mettre en service et qui est couvert par le système de gestion de la qualité visé au point 3.

4.2. La demande comprend:

a) le nom et l'adresse du fournisseur;

b) une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié;

c) la documentation technique visée à l'annexe IV.

4.3. La documentation technique est examinée par l'organisme notifié. Lorsque cela est pertinent et dans les limites de ce qui est nécessaire à l'accomplissement de ses tâches, l'organisme notifié se voit accorder un accès complet aux jeux de données d'entraînement, de validation et d'essai utilisés, y compris, lorsque cela est approprié et sous réserve de garanties de sécurité, par l'intermédiaire d'API ou d'autres moyens et outils techniques pertinents permettant un accès à distance.

4.4. Lors de l'examen de la documentation technique, l'organisme notifié peut exiger que le fournisseur apporte des preuves supplémentaires ou effectue des essais supplémentaires afin de permettre une évaluation correcte de la conformité du système d'IA avec les exigences énoncées au chapitre III, section 2. Lorsque l'organisme notifié n'est pas satisfait

des essais effectués par le fournisseur, l'organisme notifié effectue directement des essais adéquats, le cas échéant.

4.5. Lorsque cela est nécessaire pour évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au chapitre III, section 2, après que tous les autres moyens raisonnables de vérifier la conformité ont été épuisés et se sont révélés insuffisants, et sur demande motivée, l'accès aux modèles d'entraînement et aux modèles entraînés du système d'IA, y compris à ses paramètres pertinents, est aussi accordé à l'organisme notifié. Cet accès est soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires.

4.6. La décision de l'organisme notifié est notifiée au fournisseur ou à son mandataire. La notification contient les conclusions de l'évaluation de la documentation technique et la décision d'évaluation motivée.

Lorsque le système d'IA est conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié délivre un certificat d'évaluation UE de la documentation technique. Le certificat indique le nom et l'adresse du fournisseur, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du système d'IA.

Le certificat et ses annexes contiennent toutes les informations pertinentes pour permettre l'évaluation de la conformité du système d'IA et le contrôle du système d'IA pendant son utilisation, le cas échéant.

Lorsque le système d'IA n'est pas conforme aux exigences énoncées au chapitre III, section 2, l'organisme notifié refuse de délivrer un certificat d'évaluation UE de la documentation technique et en informe le demandeur, en lui précisant les raisons de son refus.

Lorsque le système d'IA ne satisfait pas à l'exigence relative aux données utilisées pour l'entraîner, il devra être entraîné à nouveau avant l'introduction d'une nouvelle demande d'évaluation de la conformité. Dans ce cas, la décision d'évaluation motivée de l'organisme notifié refusant de délivrer le certificat d'évaluation UE de la documentation technique contient des considérations spécifiques sur la qualité des données utilisées pour entraîner le système d'IA, en particulier sur les raisons de la non-conformité.

4.7. Les éventuelles modifications du système d'IA susceptibles d'avoir une incidence sur la conformité du système d'IA avec les exigences ou sur sa destination sont évaluées par l'organisme notifié qui a délivré le certificat d'évaluation UE de la documentation technique. Le fournisseur informe cet organisme notifié de son intention d'introduire une telle modification ou s'il prend autrement connaissance de l'existence de telles modifications. Les modifications envisagées sont évaluées par l'organisme notifié, qui décide si elles nécessitent une nouvelle évaluation de la conformité conformément à l'article 43, paragraphe 4, ou si elles peuvent faire l'objet d'un document complémentaire au certificat d'évaluation UE de la documentation technique. Dans ce dernier cas, l'organisme notifié évalue les modifications, informe le fournisseur de sa décision et, lorsque les modifications sont approuvées, lui fournit un document complémentaire au certificat d'évaluation UE de la documentation technique.

**5. Surveillance du système de gestion de la qualité approuvé**

5.1. Le but de la surveillance effectuée par l'organisme notifié visé au point 3 est de s'assurer que le fournisseur se conforme dûment aux conditions du système de gestion de la qualité

approuvé.

5.2. À des fins d'évaluation, le fournisseur autorise l'organisme notifié à accéder aux locaux où les systèmes d'IA sont conçus, développés ou mis à l'essai. Le fournisseur partage en outre avec l'organisme notifié toutes les informations nécessaires.

5.3. L'organisme notifié effectue périodiquement des audits pour s'assurer que le fournisseur maintient et applique le système de gestion de la qualité; il transmet un rapport d'audit au fournisseur. Dans le cadre de ces audits, l'organisme notifié peut effectuer des essais supplémentaires des systèmes d'IA pour lesquels un certificat d'évaluation UE de la documentation technique a été délivré.

## ANNEXE VIII

## Informations à fournir lors de l'enregistrement d'un système d'IA à haut risque conformément à l'article 49

### Section A - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 1

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 1:

1. le nom, l'adresse et les coordonnées du fournisseur;
2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;
3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;
4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
5. une description de la destination du système d'IA ainsi que des composants et fonctions gérées au moyen de ce système d'IA;
6. une description de base et concise des informations utilisées par le système (données, entrées) et de sa logique de fonctionnement;
7. le statut du système d'IA (sur le marché ou en service; plus mis sur le marché/en service, rappelé);
8. le type, le numéro et la date d'expiration du certificat délivré par l'organisme notifié et le nom ou le numéro d'identification de cet organisme notifié, le cas échéant;
9. une copie numérisée du certificat visé au point 8, le cas échéant;
10. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union;
11. une copie de la déclaration UE de conformité visée à l'article 47;
12. une notice d'utilisation en format électronique; ces informations ne sont pas à fournir pour les systèmes d'IA à haut risque dans les domaines des activités répressives ou de la migration, de l'asile et de la gestion des contrôles aux frontières visés à l'annexe III, points 1, 6 et 7;
13. une adresse URL vers des informations supplémentaires (facultatif).

**Section B - Informations à fournir par les fournisseurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 2**

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à enregistrer conformément à l'article 49, paragraphe 2:

1. le nom, l'adresse et les coordonnées du fournisseur;
2. lorsque la soumission d'informations est effectuée par une autre personne pour le compte du fournisseur, le nom, l'adresse et les coordonnées de cette personne;
3. le nom, l'adresse et les coordonnées du mandataire, le cas échéant;
4. la dénomination commerciale du système d'IA et toute référence supplémentaire non équivoque permettant l'identification et la traçabilité du système d'IA;
5. une description de la destination du système d'IA;
6. la ou les conditions visées à l'article 6, paragraphe 3, sur la base desquelles le système d'IA est considéré comme n'étant pas à haut risque;
7. un résumé succinct des motifs pour lesquels le système d'IA est considéré comme n'étant pas à haut risque en application de la procédure prévue à l'article 6, paragraphe 3;
8. le statut du système d'IA (sur le marché ou en service; plus sur le marché/en service, rappelé);
9. tout État membre dans lequel le système d'IA a été mis sur le marché, mis en service ou mis à disposition dans l'Union.

**Section C - Informations à fournir par les déployeurs de systèmes d'IA à haut risque conformément à l'article 49, paragraphe 3**

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 49, paragraphe 3:

1. le nom, l'adresse et les coordonnées du déployeur;
2. le nom, l'adresse et les coordonnées de toute personne qui soumet des informations au nom du déployeur;
3. l'adresse URL de l'entrée du système d'IA dans la base de données de l'UE par son fournisseur;
4. une synthèse des conclusions de l'analyse d'impact sur les droits fondamentaux réalisée conformément à l'article 27;
5. un résumé de l'analyse d'impact relative à la protection des données réalisée en application de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, comme précisé à l'article 26, paragraphe 8, du présent règlement, le cas échéant.

## ANNEXE IX

## Informations à fournir lors de l'enregistrement de systèmes d'IA à haut risque énumérés à l'annexe III en ce qui concerne les essais en conditions réelles conformément à l'article 60

Les informations ci-après sont fournies et mises à jour par la suite en ce qui concerne les essais en conditions réelles à enregistrer conformément à l'article 60:

1. un numéro d'identification unique à l'échelle de l'Union des essais en conditions réelles;

2. le nom et les coordonnées du fournisseur ou du fournisseur potentiel et des déployeurs participant aux essais en conditions réelles;
3. une brève description du système d'IA et de sa destination, ainsi que d'autres informations nécessaires à l'identification du système;
4. une synthèse des caractéristiques principales du plan d'essais en conditions réelles;
5. des informations sur la suspension ou la cessation des essais en conditions réelles.

## ANNEXE X

## Actes législatifs de l'Union relatifs aux systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

### 1. Système d'information Schengen

a) Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).

b) Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) nº 1987/2006 (JO L 312 du 7.12.2018, p. 14).

c) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) nº 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

### 2. Système d'information sur les visas

a) Règlement (UE) 2021/1133 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (UE) nº 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 et (UE) 2019/818 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système d'information sur les visas (JO L 248 du 13.7.2021, p. 1).

b) Règlement (UE) 2021/1134 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) nº 767/2008, (CE) nº 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 et (UE) 2019/1896 du Parlement européen et du Conseil et abrogeant les décisions 2004/512/CE et 2008/633/JAI du Conseil, aux fins de réformer le système d'information sur les visas (JO L 248 du 13.7.2021, p. 11).

### 3. Eurodac

Règlement (UE) 2024/1358 du Parlement européen et du Conseil du 14 mai 2024 relatif à la création d'«Eurodac» pour la comparaison des données biométriques aux fins de l'application efficace des règlements (UE) 2024/1315, (UE) 2024/1350 du Parlement européen et du Conseil et de la directive 2001/55/CE du Conseil et aux fins de l'identification des ressortissants de pays tiers et apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, modifiant les règlements (UE) 2018/1240 et (UE) 2019/818 du Parlement européen et du Conseil et abrogeant le règlement (UE) nº 603/2013 du Parlement européen et du Conseil (JO L, 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

**4. Système d'entrée/de sortie**

Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) nº 767/2008 et (UE) nº 1077/2011 (JO L 327 du 9.12.2017, p. 20).

**5. Système européen d'information et d'autorisation concernant les voyages**

a) Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) nº 1077/2011, (UE) nº 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1).

b) Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) (JO L 236 du 19.9.2018, p. 72).

**6. Système européen d'information sur les casiers judiciaires concernant des ressortissants de pays tiers et des apatrides**

Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

**7. Interopérabilité**

a) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI (JO L 135 du 22.5.2019, p. 27).

b) Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019, p. 85).

## ANNEXE XI

## Documentation technique visée à l'article 53, paragraphe 1, point a) – documentation technique pour les fournisseurs de modèles d'IA à usage général

### Section 1

### Informations devant être fournies par tous les fournisseurs de modèles d'IA à usage général

La documentation technique visée à l'article 53, paragraphe 1, point a), contient au moins les informations ci-après, en fonction de la taille et du profil de risque du modèle:

1. Une description générale du modèle d'IA à usage général, y compris:
   a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;
   b) les politiques applicables en matière d'utilisation acceptable;
   c) la date de publication et les méthodes de distribution;
   d) l'architecture et le nombre de paramètres;
   e) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;
   f) la licence.
2. Une description détaillée des éléments du modèle visés au point 1, et des informations pertinentes sur le processus de développement, y compris les éléments suivants:
   a) les moyens techniques (p. ex.: notice d'utilisation, infrastructure, outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;
   b) les spécifications de conception du modèle et du processus d'entraînement, y compris les méthodes et techniques d'entraînement, les principaux choix de conception, y compris le raisonnement et les hypothèses retenues; ce que le modèle est conçu pour optimiser, ainsi que la pertinence des différents paramètres, le cas échéant;
   c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation (p. ex.: nettoyage, filtrage, etc.), le nombre de points de données, leur portée et leurs principales caractéristiques; la manière dont les données ont été obtenues et sélectionnées, ainsi que toutes les autres mesures visant à détecter l'inadéquation des sources de données et les méthodes permettant de détecter les biais identifiables, le cas échéant;
   d) les ressources informatiques utilisées pour entraîner le modèle (p. ex.: nombre d'opérations en virgule flottante), le temps d'entraînement et d'autres détails pertinents liés à l'entraînement;

e) la consommation d'énergie connue ou estimée du modèle.

En ce qui concerne le point e), lorsque la consommation d'énergie du modèle est inconnue, la consommation d'énergie peut être estimée en s'appuyant sur des informations concernant les ressources informatiques utilisées.

**Section 2**

**Informations devant être fournies par les fournisseurs de modèles d'IA à usage général présentant un risque systémique**

1. Une description détaillée des stratégies d'évaluation, y compris les résultats de l'évaluation, sur la base des protocoles et outils d'évaluation publics disponibles ou d'autres méthodes d'évaluation. Les stratégies d'évaluation comprennent des critères, des indicateurs et les méthodes d'évaluation pour l'identification des limites.
2. Le cas échéant, une description détaillée des mesures mises en place pour effectuer des essais contradictoires internes et/ou externes (p. ex.: méthode de l'équipe rouge), des adaptations de modèles, y compris l'alignement et le réglage fin.
3. Le cas échéant, une description détaillée de l'architecture du système expliquant la manière dont les composants logiciels s'utilisent et s'alimentent les uns les autres ou s'intègrent dans le traitement global.

## ANNEXE XII

## Informations relatives à la transparence visées à l'article 53, paragraphe 1, point b) – documentation technique pour les fournisseurs de modèles d'IA à usage général aux fournisseurs en aval qui intègrent le modèle dans leur système d'IA

Les informations visées à l'article 53, paragraphe 1, point b) comprennent au moins:

1. Une description générale du modèle d'IA à usage général, y compris:
   a) les tâches que le modèle est censé accomplir ainsi que le type et la nature des systèmes d'IA dans lesquels il peut être intégré;
   b) les politiques applicables en matière d'utilisation acceptable;
   c) la date de publication et les méthodes de distribution;
   d) la manière dont le modèle interagit ou peut être utilisé pour interagir avec du matériel informatique ou des logiciels qui ne font pas partie du modèle lui-même, le cas échéant;
   e) les versions des logiciels pertinents liés à l'utilisation du modèle d'IA à usage général, le cas échéant;
   f) l'architecture et le nombre de paramètres;
   g) les modalités (p. ex.: texte, image) et le format des entrées et des sorties;
   h) la licence pour le modèle.
2. Une description des éléments du modèle et de son processus de développement, notamment:
   a) les moyens techniques (p. ex.: la notice d'utilisation, l'infrastructure, les outils) nécessaires à l'intégration du modèle d'IA à usage général dans les systèmes d'IA;

b) les modalités (p. ex.: texte, image, etc.) et le format des entrées et des sorties, ainsi que leur taille maximale (p. ex.: taille de la fenêtre de contexte, etc.);

c) des informations sur les données utilisées pour l'entraînement, les essais et la validation, le cas échéant, y compris le type et la provenance des données et les méthodes d'organisation.

## ANNEXE XIII

## Critères de désignation des modèles d'IA à usage général présentant un risque systémique visés à l'article 51

Aux fins de déterminer si un modèle d'IA à usage général a des capacités ou un impact équivalents à ceux énoncés à l'article 51, paragraphe 1, point a), la Commission tient compte des critères suivants:

a) le nombre de paramètres du modèle;

b) la qualité ou la taille du jeu de données, par exemple mesurée en tokens;

c) la quantité de calcul utilisée pour l'entraînement du modèle, mesurée en nombre d'opérations en virgule flottante ou indiquée par une combinaison d'autres variables telles que le coût estimé de l'entraînement, le temps estimé nécessaire à l'entraînement ou la consommation d'énergie estimée pour l'entraînement;

d) les modalités d'entrée et de sortie du modèle, telles que la conversion de texte en texte (grands modèles de langage), la conversion de texte en image, la multimodalité et les seuils de l'état de l'art pour déterminer les capacités à fort impact pour chaque modalité, ainsi que le type spécifique d'entrées et de sorties (p. ex.: séquences biologiques);

e) les critères de référence et les évaluations des capacités du modèle, y compris en tenant compte du nombre de tâches ne nécessitant pas d'entraînement supplémentaire, sa capacité d'adaptation à apprendre de nouvelles tâches distinctes, son niveau d'autonomie et d'extensibilité, ainsi que les outils auxquels il a accès;

f) si le modèle a un impact important sur le marché intérieur en raison de sa portée, qui est présumée lorsqu'il a été mis à la disposition d'au moins 10 000 utilisateurs professionnels enregistrés établis dans l'Union;

g) le nombre d'utilisateurs finaux inscrits.

ELI: http://data.europa.eu/eli/reg/2024/1689/oj

ISSN 1977-0693 (electronic edition)