European Parliament

Commission du marché intérieur et de la protection des consommateurs

Commission des libertés civiles, de la justice et des affaires intérieures

16/5/2023

KMB/DA/AS

Version : 1.1

PROJET d'amendements de compromis

sur le projet de rapport

Proposition de règlement du Parlement européen et du Conseil concernant des règles harmonisées sur l'intelligence artificielle (acte sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union

(COM(2021)0206 – C9 0146/2021 – 2021/0106(COD))

Rapporteurs:
Brando Benifei & Ioan-Dragoş Tudorache

(Procédure de commission mixte – article 58 du règlement)

Titre III, chapitre 4 et considérants 65 et 65 bis	CA 1

(65) Afin d'effectuer des évaluations de conformité par tierce partie lorsque cela est requis, les organismes notifiés devraient être désignés en vertu du présent règlement par les autorités nationales compétentes, à condition qu'ils respectent un ensemble d'exigences, notamment en matière d'indépendance, de compétence, d'absence de conflits des intérêts et des exigences minimales en matière de cybersécurité. Les États membres devraient encourager la désignation d'un nombre suffisant d'organismes d'évaluation de la conformité, afin de rendre la certification possible en temps utile. Les procédures d'évaluation, de désignation, de notification et de contrôle des organismes d'évaluation de la conformité devraient être mises en œuvre aussi uniformément que possible dans les États membres, en vue de supprimer les barrières administratives aux frontières et de garantir la réalisation du potentiel du marché intérieur.

(65 bis) Conformément aux engagements de l'Union dans le cadre de l'Organisation mondiale du commerce (OMC) accord sur les obstacles techniques au commerce (OTC), il convient de maximiser l'acceptation des résultats d'essais produits par des organismes d'évaluation de la conformité compétents, indépendamment du territoire sur lequel ils sont établis, lorsque cela est nécessaire pour démontrer la conformité aux exigences applicables du règlement. La Commission devrait explorer activement d'éventuels instruments internationaux à cette fin et, en particulier, rechercher la possibilité d'établir des accords de reconnaissance mutuelle avec des pays qui se trouvent à un niveau de développement technique comparable et qui ont une approche compatible en matière d'intelligence artificielle et d'évaluation de la conformité.

CHAPITRE 4

AUTORITÉS NOTIFIANTES ET ORGANISMES NOTIFIÉS

Article 30

Autorités notifiantes

1. Chaque État membre désigne ou établit une autorité notifiante chargée de mettre en place et de mettre en œuvre 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 désigner un organisme national d'accréditation visé dans le règlement (CE) no 765/2008 comme autorité notifiante.

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 préserver l'objectivité et l'impartialité de leurs activités.

4. Les autorités notifiantes sont organisées de manière à ce que les décisions relatives à la notification des organismes d'évaluation de la conformité soient prises par des personnes compétentes différentes de celles qui ont procédé à l'évaluation de ces organismes.

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

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

7. Les autorités notifiantes disposent d'un personnel compétent en nombre suffisant pour la bonne exécution de leurs tâches. Le cas échéant, le personnel compétent possède l'expertise nécessaire, telle qu'un diplôme dans un domaine juridique approprié, en matière de contrôle des droits fondamentaux consacrés dans la charte des droits fondamentaux de l'Union.

8. Les autorités notifiantes veillent à ce que les évaluations de la conformité soient réalisées de manière proportionnée et en temps utile, en évitant des charges inutiles pour les prestataires, et à ce que les organismes notifiés exercent leurs activités en tenant dûment compte de la taille d'une entreprise, du secteur dans lequel elle opère, de sa structure et le degré de complexité du système d'IA en question. Une attention particulière est accordée à la réduction des charges administratives et des coûts de mise en conformité pour les micro et petites entreprises telles que définies dans la recommandation 2003/361/CE de la Commission.

Article 31

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

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

2. La demande de notification est accompagnée d'une description des activités d'évaluation de la conformité, du ou des modules d'évaluation de la conformité et des technologies d'intelligence artificielle pour lesquels l'organisme d'évaluation de la conformité se déclare compétent, ainsi que d'un certificat d'accréditation, s'il en existe un, délivré par un organisme national d'accréditation attestant que l'organisme d'évaluation de la conformité satisfait aux exigences énoncées à l'article 33. Tout document valide lié aux désignations existantes de l'organisme notifié demandeur en vertu de toute autre législation d'harmonisation de l'Union est ajouté.

3. Lorsque l'organisme d'évaluation de la conformité concerné n'est pas en mesure de fournir un certificat d'accréditation, il fournit à l'autorité notifiante les pièces justificatives nécessaires à la vérification, à la reconnaissance et au contrôle régulier de sa conformité avec les exigences prévues à l'article 33. Pour les organismes notifiés qui sont désignés en vertu de toute autre législation d'harmonisation de l'Union, tous les documents et certificats liés à ces désignations peuvent être utilisés à l'appui de leur procédure de désignation au titre du présent règlement, le cas échéant.

Article 32

Procédure de notification

1. Les autorités notifiantes notifient uniquement les organismes d'évaluation de la conformité qui ont satisfait aux exigences prévues à l'article 33.

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

3. La notification visée au paragraphe 2 contient des détails complets sur les activités d'évaluation de la conformité, le ou les modules d'évaluation de la conformité et les technologies d'intelligence artificielle concernées, ainsi que l'attestation de compétence pertinente.

4. L'organisme d'évaluation de la conformité concerné ne peut exercer les activités d'un organisme notifié que si aucune objection n'est soulevée par la Commission ou les autres États membres dans les deux semaines suivant la validation de la notification lorsqu'elle comprend un certificat d'accréditation visé à l'article 31, paragraphe 2. , ou dans les deux mois suivant la notification lorsqu'elle comporte des pièces justificatives visées à l'article 31, paragraphe 3.

4a. En cas d'objections, la Commission engage sans délai une consultation avec les États membres concernés et l'organisme d'évaluation de la conformité.
Au vu de ces éléments, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre concerné et à l'organisme d'évaluation de la conformité compétent.

4b. Les États membres notifient à la Commission et aux autres États membres les organismes d'évaluation de la conformité.

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

Article 33

Organismes notifiés

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

2. Les organismes notifiés satisfont aux exigences en matière d'organisation, de gestion de la qualité, de ressources et de processus nécessaires à l'accomplissement de leurs tâches ainsi qu'aux exigences minimales en matière de cybersécurité fixées pour les entités de l'administration publique identifiées comme opérateurs de services essentiels conformément à la directive XXX concernant des mesures pour un haut niveau de niveau de cybersécurité dans l'Union (NIS2), abrogeant la directive (UE) 2016/1148.

3. La structure organisationnelle, la répartition des responsabilités, les voies hiérarchiques et le fonctionnement des organismes notifiés doivent être tels qu'il existe une confiance dans la performance et dans les résultats des activités d'évaluation de la conformité menées par les organismes notifiés.

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

4a. L'évaluation de la conformité en vertu du paragraphe 1 est effectuée par des employés d'organismes notifiés qui n'ont fourni aucun autre service lié à la question évaluée que l'évaluation de la conformité au fournisseur d'un système d'IA à haut risque ni à toute personne morale liée à ce fournisseur. dans la période de 12 mois précédant l'évaluation et se sont engagés à ne pas leur fournir de tels services dans la période de 12 mois suivant la fin de l'évaluation.

5. Les organismes notifiés sont organisés et fonctionnent de manière à garantir l'indépendance, l'objectivité et l'impartialité de leurs activités. Les organismes notifiés documentent et

mettre en place une structure et des procédures pour préserver l'impartialité et promouvoir et appliquer les principes d'impartialité dans l'ensemble de leur organisation, de leur personnel et de leurs activités d'évaluation.

6. Les organismes notifiés doivent avoir mis en place des procédures documentées garantissant que leur personnel, comités, filiales, sous-traitants et tout organisme associé ou personnel d'organismes externes respectent la confidentialité des informations qui entrent en leur possession au cours de l'exécution des activités d'évaluation de la conformité, sauf lorsque la divulgation est Requis par la loi. Le personnel des organismes notifiés est tenu au secret professionnel en ce qui concerne toutes les informations obtenues dans l'exercice de leurs missions en vertu du présent règlement, sauf en ce qui concerne les autorités notifiantes de l'État membre dans lequel leurs activités sont exercées. Toutes les informations et tous les documents obtenus par les organismes notifiés conformément aux dispositions du présent article sont traités dans le respect des obligations de confidentialité énoncées à l'article 70.

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

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

9. Les organismes notifiés sont capables d'accomplir toutes les tâches qui leur incombent en vertu du présent règlement avec la plus grande probité professionnelle et la compétence requise dans le domaine spécifique, que ces tâches soient exécutées par les organismes notifiés eux-mêmes ou en leur nom et sous leur responsabilité.

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

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

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

Article 34

Filiales et sous-traitance d'organismes notifiés

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

2. Les organismes notifiés assument l'entière responsabilité des tâches exécutées par les sous-traitants ou les filiales, où qu'ils soient établis.

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

4. Les organismes notifiés tiennent à la disposition de l'autorité notifiante les documents pertinents concernant la vérification des qualifications du sous-traitant ou de la filiale et les travaux effectués par eux dans le cadre du présent règlement.

Article 35

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

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

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

Article 36

Modifications des notifications

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

2. En cas de restriction, de suspension ou de retrait de la notification, ou lorsque l'organisme notifié a cessé ses activités, l'autorité notifiante prend les mesures appropriées pour garantir que les dossiers de cet organisme notifié sont soit repris par un autre organisme notifié, soit tenus à disposition pour les autorités notifiantes responsables et l'autorité de surveillance du marché à leur demande.

Article 37

Contestation de la compétence des organismes notifiés

1. La Commission enquête, si nécessaire, 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 et 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 de ses enquêtes en vertu du présent article soient traitées de manière confidentielle.

4. Lorsque la Commission constate qu'un organisme notifié ne satisfait pas ou plus aux exigences de sa notification, elle en informe l'État membre notifiant et lui demande de prendre les mesures correctives nécessaires, y compris la suspension ou le retrait de la notification si nécessaire. Si l'État membre ne prend pas les mesures correctives nécessaires, 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 74, paragraphe 2.

Article 38

Coordination des organismes notifiés

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

2. Les États membres veillent à ce que les organismes notifiés par eux participent aux travaux de ce groupe, directement ou par l'intermédiaire de représentants désignés.

2a. La Commission prévoit l'échange de connaissances et de bonnes pratiques entre les autorités nationales des États membres responsables de la politique de notification.

Article 39

Organismes d'évaluation de la conformité des pays tiers

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

(61) La normalisation devrait jouer un rôle clé pour fournir des solutions techniques aux fournisseurs afin de garantir la conformité avec le présent règlement. La conformité aux normes harmonisées telles que définies dans le règlement (UE) n° 1025/2012 du Parlement européen et du Conseil1 devrait être un moyen pour les prestataires de démontrer la conformité aux exigences du présent règlement. Afin de garantir l'efficacité des normes en tant qu'instrument politique de l'Union et compte tenu de l'importance des normes pour garantir la conformité aux exigences du présent règlement et pour la compétitivité des entreprises, il est nécessaire d'assurer une représentation équilibrée des intérêts en associant toutes les parties prenantes concernées aux l'élaboration de normes. Le processus de normalisation devrait être transparent en termes de personnes morales et physiques participant aux activités de normalisation.

(61 ter) Afin de faciliter la mise en conformité, les premières demandes de normalisation devraient être émises par la Commission au plus tard deux mois après l'entrée ~~en~~ vigueur du présent règlement. Cela devrait permettre d'améliorer la sécurité juridique, favorisant ainsi l'investissement et l'innovation dans le domaine de l'IA, ainsi que la compétitivité et la croissance du marché de l'Union, tout en renforçant la gouvernance multipartite représentant toutes les parties prenantes européennes concernées telles que l'Office de l'IA, les organisations et organismes européens de normalisation ou les groupes d' experts établi en vertu du droit sectoriel pertinent de l'Union ainsi que de l'industrie, des PME, des start-up, de la société civile, des chercheurs et des partenaires sociaux, et devrait, à terme, faciliter la coopération mondiale en matière de normalisation dans le domaine de l'IA d'une manière conforme aux valeurs de l'Union. Lors de la préparation de la demande de normalisation, la Commission devrait consulter l'Office AI et le forum consultatif AI afin de recueillir l'expertise pertinente.

(61 quater) Lorsque les systèmes d'IA sont destinés à être utilisés sur le lieu de travail, les normes harmonisées devraient se limiter aux spécifications et procédures techniques.

(61 quinquies) La Commission devrait pouvoir adopter des spécifications communes sous certaines conditions, lorsqu'il n'existe pas de norme harmonisée pertinente ou pour répondre à des préoccupations spécifiques en matière de droits fondamentaux. Tout au long du processus de rédaction, la Commission devrait consulter régulièrement l'Office AI et son forum consultatif, les organisations européennes de normalisation et les organes ou groupes d'experts établis en vertu du droit sectoriel pertinent de l'Union ainsi que les parties prenantes concernées, telles que l'industrie, les PME, les start-ups, la société civile la société, les chercheurs et les partenaires sociaux.

(61 sexies) Lors de l'adoption de spécifications communes, la Commission devrait s'efforcer d'aligner la réglementation sur l'IA avec des partenaires mondiaux partageant les mêmes idées, ce qui est essentiel pour favoriser l'innovation et les partenariats transfrontaliers dans le domaine de l'IA, car la coordination avec des partenaires partageant les mêmes idées au sein des organismes internationaux de normalisation est d'une grande importance .

(62) Afin de garantir un niveau élevé de fiabilité des systèmes d'IA à haut risque, ces systèmes devraient faire l'objet d'une évaluation de conformité avant leur mise sur le marché ou leur mise en service. Pour accroître la confiance dans la chaîne de valeur et donner de la certitude aux

[1] Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil et les directives 94/9/CE, 94/25/ CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil (JO L 316 du 14.11.2012, p. 12).

entreprises sur les performances de leurs systèmes, les tiers qui fournissent des composants d'IA peuvent demander volontairement une évaluation de la conformité par un tiers.

(63) Il convient que, afin de réduire au minimum la charge pesant sur les opérateurs et d'éviter tout double emploi éventuel, pour les systèmes d'IA à haut risque liés à des produits qui sont couverts par la législation d'harmonisation existante de l'Union conformément à l'approche du nouveau cadre législatif, la conformité de ces Les systèmes d'IA répondant aux exigences du présent règlement devraient être évalués dans le cadre de l'évaluation de la conformité déjà prévue par cette législation. L'applicabilité des exigences du présent règlement ne devrait donc pas affecter la logique, la méthodologie ou la structure générale spécifiques de l'évaluation de la conformité en vertu de la législation spécifique pertinente du nouveau cadre législatif. Cette approche se reflète pleinement dans l'interaction entre le présent règlement et le [règlement machines].
Alors que les risques de sécurité des systèmes d'IA assurant des fonctions de sécurité dans les machines sont traités par les exigences du présent règlement, certaines exigences spécifiques du [règlement sur les machines] garantiront l'intégration en toute sécurité du système d'IA dans l'ensemble de la machine, afin de ne pas compromettre la sécurité de la machinerie dans son ensemble. Le [règlement sur les machines] applique la même définition du système d'IA que le présent règlement.

(64) Compte tenu de la complexité des systèmes d'IA à haut risque et des risques qui leur sont associés, il est essentiel de développer une capacité plus adéquate pour l'application de l'évaluation de la conformité par un tiers aux systèmes d'IA à haut risque. Toutefois, compte tenu de l'expérience actuelle des certificateurs professionnels avant commercialisation dans le domaine de la sécurité des produits et de la nature différente des risques encourus, il convient de limiter, au moins dans une première phase d'application du présent règlement, le champ d'application des troisièmes -évaluation de la conformité des parties pour les systèmes d'IA à haut risque autres que ceux liés aux produits. Par conséquent, l'évaluation de la conformité de tels systèmes devrait être effectuée en règle générale par le fournisseur sous sa propre responsabilité, à la seule exception des systèmes d'IA destinés à être utilisés pour l'identification biométrique à distance de personnes, ou des systèmes d'IA destinés à être utilisés de faire des déductions sur les caractéristiques personnelles des personnes physiques sur la base de données biométriques ou fondées sur la biométrie, y compris les systèmes de reconnaissance des émotions pour lesquels la participation d'un organisme notifié à l'évaluation de la conformité devrait être prévue, dans la mesure où elles ne sont pas interdites.

(66) Conformément à la notion communément admise de modification substantielle pour les produits régis par la législation d'harmonisation de l'Union, il convient qu'un système d'IA à haut risque fasse l'objet d'une nouvelle évaluation de la conformité chaque fois qu'une modification imprévue se produit et va au-delà des modifications contrôlées ou prédéterminées par le fournisseur, y compris l'apprentissage continu et qui peuvent créer un nouveau risque inacceptable et affecter de manière significative la conformité du système d'IA à haut risque avec le présent règlement ou lorsque la finalité prévue du système change. En outre, en ce qui concerne les systèmes d'IA qui continuent à "apprendre" après avoir été mis sur le marché ou mis en service (c'est-à-dire qu'ils adaptent automatiquement la façon dont les fonctions sont exécutées), il est nécessaire de prévoir des règles établissant que les modifications de l'algorithme et de ses performances qui ont été prédéterminés par le fournisseur et évalués au moment de l'évaluation de la conformité ne doivent pas constituer une modification substantielle. Il devrait en être de même pour les mises à jour du système d'IA pour des raisons de sécurité en général et pour se protéger contre l'évolution des menaces de manipulation du système, tant qu'elles ne constituent pas une modification substantielle.

(67) Les systèmes d'IA à haut risque devraient porter le marquage CE pour indiquer leur conformité avec le présent règlement afin qu'ils puissent circuler librement au sein du marché intérieur. Pour les systèmes d'IA physiques à haut risque, un marquage CE physique doit être apposé et peut être complété

par un marquage CE numérique. Pour les systèmes d'IA à haut risque uniquement numériques, un marquage CE numérique doit être utilisé. Les États membres ne devraient pas créer d'obstacles injustifiés à la mise sur le marché ou à la mise en service de systèmes d'IA à haut risque conformes aux exigences énoncées dans le présent règlement et portant le marquage CE.

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

(69) Afin de faciliter le travail de la Commission et des États membres dans le domaine de l'intelligence artificielle et d'accroître la transparence vis-à-vis du public, les fournisseurs de systèmes d'IA à haut risque autres que ceux liés aux produits relevant du champ d'application de la législation d'harmonisation de l'Union existante pertinente, devraient être tenus d'enregistrer leur système d'IA à haut risque et leurs modèles de base dans une base de données de l'UE, qui sera créée et gérée par la Commission. Cette base de données doit être accessible librement et publiquement, facilement compréhensible et lisible par machine. La base de données devrait également être conviviale et facilement navigable, avec des fonctionnalités de recherche permettant au minimum au grand public de rechercher dans la base de données des systèmes à haut risque spécifiques, des emplacements, des catégories de risque au titre de l'annexe IV et des mots clés. Les déployeurs qui sont des autorités publiques ou des institutions, organes, offices et agences de l'Union européenne ou des déployeurs agissant en leur nom et les déployeurs qui sont des entreprises désignées comme contrôleur d'accès en vertu du règlement 2022/1925 devraient également s'inscrire dans la base de données de l'UE avant de mettre en service ou d'utiliser un système d'IA à risque pour la première fois et après chaque modification substantielle. Les autres déployeurs devraient être autorisés à le faire volontairement. Toute modification substantielle des systèmes d'IA à haut risque est également enregistrée dans la base de données de l'UE. La Commission devrait être le responsable du traitement de cette base de données, conformément au règlement (UE) 2018/1725 du Parlement européen et du Conseil2 .

Afin de garantir la pleine fonctionnalité de la base de données, une fois déployée, la procédure de configuration de la base de données devrait inclure l'élaboration de spécifications fonctionnelles par la Commission et un rapport d'audit indépendant. La Commission devrait tenir compte de la cybersécurité et des risques liés aux dangers lorsqu'elle s'acquitte de ses tâches en tant que responsable du traitement des données de la base de données de l'UE. Afin de maximiser la disponibilité et l'utilisation de la base de données par le public, la base de données, y compris les informations mises à disposition par son intermédiaire, devrait être conforme aux exigences de l'acte européen sur l'accessibilité.

CHAPITRE 5

NORMES, ÉVALUATION DE LA CONFORMITÉ, CERTIFICATS, ENREGISTREMENT

[2] 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).

Article 40
Normes harmonisées

1. Les systèmes d'IA à haut risque et les modèles de base qui sont conformes aux normes harmonisées ou à des parties de celles-ci dont les références ont été publiées au Journal officiel de l'Union européenne conformément au règlement 1025/2012 (AM 2122) sont présumés être en conformité avec les exigences énoncées au chapitre 2 du présent titre ou à l'article 28 ter, dans la mesure où ces normes couvrent ces exigences.

1a. La Commission émet des demandes de normalisation couvrant toutes les exigences du présent règlement, conformément à l'article 10 du règlement 1025/2012 au plus tard 2 mois après la date d'entrée en vigueur du présent règlement. Lors de la préparation de la demande de normalisation, la Commission consulte l'Office AI et le forum consultatif.

1b. Lorsqu'elle adresse une demande de normalisation aux organisations européennes de normalisation, la Commission précise que les normes doivent être cohérentes, y compris avec la législation sectorielle énumérée à l'annexe II, et viser à garantir que les systèmes d'IA ou les modèles de base mis sur le marché ou mis en service dans l'Union satisfaire aux exigences pertinentes du présent règlement ; posé bas dans

1c. Les acteurs impliqués dans le processus de normalisation tiennent compte des principes généraux pour une IA digne de confiance énoncés à l'article 4, point a), cherchent à promouvoir l'investissement et l'innovation dans l'IA ainsi que la compétitivité et la croissance du marché de l'Union, et contribuent au renforcement de la coopération en matière de normalisation et la prise en compte des normes internationales existantes dans le domaine de l'IA qui sont conformes aux valeurs, aux droits fondamentaux et aux intérêts de l'Union, et garantissent une représentation équilibrée des intérêts et une participation effective de toutes les parties prenantes concernées conformément aux articles 5, 6 et 7 du règlement (UE) n° 1025/2012.

Article 41
Spécifications communes

~~1. Lorsqu'il n'existe pas de normes harmonisées visées à l'article 40 ou lorsque la Commission estime que les normes harmonisées pertinentes sont insuffisantes ou qu'il est nécessaire de répondre à des préoccupations spécifiques en matière de sécurité ou de droits fondamentaux, la Commission peut, au moyen d'actes d'exécution, adopter des spécifications relatives aux exigences énoncées au chapitre 2 du présent titre. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 74, paragraphe 2.~~

1a. La Commission peut, au moyen d'un acte d'exécution adopté conformément à la procédure d'examen visée à l'article 74, paragraphe 2, et après consultation de l'Office AI et du forum consultatif AI, adopter des spécifications communes en ce qui concerne les exigences énoncées au chapitre 2 du présent titre ou à l'article 28 ter lorsque les conditions suivantes sont remplies:

a) il n'y a aucune référence à des normes harmonisées déjà publiées dans le Journal officiel de l'Union européenne relatives à la ou aux exigences essentielles, sauf si la norme harmonisée en question est une norme existante qui doit être révisée ; et

b) la Commission a demandé à une ou plusieurs organisations européennes de normalisation d'élaborer une norme harmonisée pour la ou les exigences essentielles énoncées au chapitre 2; et

c) la demande visée au point b) n'a été acceptée par aucune des organisations européennes de normalisation; ou il y a des retards injustifiés dans l'établissement d'une norme harmonisée appropriée; ou la norme fournie ne satisfait pas aux exigences de la législation européenne pertinente ou n'est pas conforme à la demande de la Commission.

1b. Lorsque la Commission estime qu'il est nécessaire de répondre à des préoccupations spécifiques en matière de droits fondamentaux, les spécifications communes adoptées par la Commission conformément au paragraphe 1 traitent également ces préoccupations spécifiques en matière de droits fondamentaux.

1c. La Commission élabore des spécifications communes pour la méthodologie permettant de satisfaire à l'exigence de déclaration et de documentation sur la consommation d'énergie et de ressources lors du développement, de la formation et du déploiement du système d'IA à haut risque.

2. La Commission, tout au long du processus d'élaboration des spécifications communes visées aux paragraphes 1 bis et 1 ter, consulte régulièrement l'Office AI et le forum consultatif, les organisations européennes de normalisation et les organes ou groupes d'experts établis en vertu du droit sectoriel pertinent de l'Union ainsi que d'autres les parties prenantes, organes ou groupes d'experts concernés établis en vertu du droit sect~~oriel pertinent de l'Union. La Commission remplit les objectifs visés à l'article 40, p~~aragraphe 1 quater, et justifie dûment sa décision de recourir à des spécifications communes. Lorsque la Commission a l'intention d'adopter des spécifications communes conformément au paragraphe 1 ter du présent article, elle identifie également clairement la préoccupation spécifique en matière de droits fondamentaux à traiter.

Lors de l'adoption de spécifications communes conformément aux paragraphes 1 bis et 1 ter du présent article, la Commission tient compte de l'avis émis par l'Office AI visé à l'article 56 sexies, point b), du présent règlement. Si la Commission décide de ne pas suivre l'avis de l'Office AI, elle fournit une explication motivée à l'Office AI.

3. Les systèmes d'IA à haut risque qui sont conformes aux spécifications communes visées aux paragraphes 1 bis et 1 ter so~~n~~t présumé~~s~~ conformes aux exigences énoncées au chapitre 2 du présent titre, dans la mesure où ces spécifications communes couvrent ces exigences.

3 bis Lorsqu'une norme harmonisée est adoptée par une organisation européenne de normalisation et proposée à la Commission pour la publication de sa référence au Journal officiel de l'Union européenne, la Commission évalue la norme harmonisée conformément au règlement (UE) n° 1025/2012 . Lorsqu'une référence à une norme harmonisée est publiée au Journal officiel de l'Union européenne, la Commission abroge les actes visés aux paragraphes 1 bis et 1 ter, ou des parties de ceux-ci qui couvrent les mêmes exigences énoncées au chapitre 2 du présent titre.

4. Lorsque les fournisseurs de systèmes d'IA à haut risque ne respectent pas les spécifications communes visées au paragraphe 1, ils justifient dûment qu'ils ont adopté des solutions techniques qui satisfont aux exigences visées au chapitre II à un niveau au moins équivalent.

Article 42

Présomption de conformité à certaines exigences

1. Compte tenu de leur destination, les systèmes d'IA à haut risque qui ont été formés et testés sur des données concernant le cadre géographique, comportemental, contextuel et fonctionnel spécifique dans lequel ils sont destinés à être utilisés sont présumés conformes aux exigences respectives. conformément à l'article 10, paragraphe 4.

2. 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 programme de cybersécurité conformément au règlement (UE) 2019/881 du Parlement européen et du Conseil3 et dont les références ont été publiées dans le Journal officiel de l'Union européenne est présumé conforme aux exigences de cybersécurité énoncées à l'article 15 du présent règlement dans la mesure où le certificat de cybersécurité ou la déclaration de conformité ou des parties de celui-ci couvrent ces exigences.

Article 43

Évaluation de la conformité

1. Pour les systèmes d'IA à haut risque énumérés à l'annexe III, point 1, lorsque, pour démontrer la conformité d'un système d'IA à haut risque aux exigences énoncées au chapitre 2 du présent Titre, le prestataire a appliqué les normes harmonisées visées à l'article 40, ou, le cas échéant, les spécifications communes visées à l'article 41, le prestataire opte pour l'une des procédures suivantes :

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

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

En démontrant la conformité d'un système d'IA à haut risque avec les exigences énoncées dans chapitre 2 du présent titre, le prestataire suit la procédure d'évaluation de la conformité prévue à l'annexe VII dans les cas suivants:

a) lorsqu'il n'existe pas de normes harmonisées visées à l'article 40, dont le numéro de référence a été publié au Journal officiel de l'Union européenne, couvrant toutes les exigences de sécurité pertinentes pour le système d'IA et les spécifications communes visées à l'article 41 ne sont pas disponibles;

3 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (l'Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et de la communication et abrogeant le règlement (UE) n° 526/2013 (loi sur la cybersécurité) (JO L 151 du 7.6.2019, p. 1).

b) lorsque les spécifications techniques visées au point a) existent mais que le fournisseur ne les a pas appliquées ou ne les a appliquées que partiellement ;

c) lorsqu'une ou plusieurs des spécifications techniques visées au point a) ont été publiées avec une restriction et uniquement sur la partie de la norme qui a été restreinte;

(d) lorsque le fournisseur considère que la nature, la conception, la construction ou la finalité du système d'IA nécessitent une vérification par une tierce partie, quel que soit son niveau de risque.

Aux fins de l'exécution de la procédure d'évaluation de la conformité visée à l'annexe VII, le prestataire peut choisir n'importe lequel des organismes notifiés. Toutefois, lorsque le système est destiné à être mis en service par les autorités répressives, les autorités chargées de l'immigration ou de l'asile ainsi que par les institutions, organes ou agences de l'Union, l'autorité de surveillance du marché visée à l'article 63, paragraphes 5 ou 6, selon le cas, agit en qualité d'organisme notifié.

2. Pour les systèmes d'IA à haut risque visés à l'annexe III, points 1 à 8, les fournisseurs suivent la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI, qui ne prévoit pas l'intervention d'un organisme notifié. Pour les systèmes d'IA à haut risque visés à l'annexe III, point 5 b), mis sur le marché ou mis en service par des établissements de crédit régis par la directive 2013/36/UE, l'évaluation de la conformité est effectuée dans le cadre de la procédure visée aux articles 97 à 101 de ladite directive.

3. Pour les systèmes d'IA à haut risque, auxquels s'appliquent les actes juridiques énumérés à l'annexe II, section A, le fournisseur suit l'évaluation de la conformité pertinente, comme l'exigent ces actes juridiques. Les exigences énoncées au chapitre 2 du présent titre s'appliquent à ces systèmes d'IA à haut risque et font partie de cette évaluation. Points 4.3., 4.4., 4.5. et le cinquième alinéa du point 4.6 de l'annexe VII s'appliquent également.

Aux fins de cette évaluation, les organismes notifiés qui ont été notifiés au titre de ces actes juridiques sont habilités à contrôler la conformité des systèmes d'IA à haut risque avec les exigences énoncées au chapitre 2 du présent titre, à condition que la conformité de ceux notifiés organismes soumis aux exigences énoncées à l'article 33, paragraphes 4, 9 et 10, a été évaluée dans le cadre de la procédure de notification prévue par ces actes juridiques.

Lorsque les actes juridiques énumérés à l'annexe II, section A, permettent au fabricant du produit de se soustraire à une évaluation de la conformité par une tierce partie, à condition que ce fabricant ait appliqué toutes les normes harmonisées couvrant toutes les exigences pertinentes, ce fabricant peut recourir à cette faculté que s'il a également appliqué les normes harmonisées ou, le cas échéant, les spécifications communes visées à l'article 41, couvrant les exigences énoncées au chapitre 2 du présent titre.

4. Les systèmes d'IA à haut risque qui ont déjà fait l'objet d'une procédure d'évaluation de la conformité sont soumis à une nouvelle procédure d'évaluation de la conformité chaque fois qu'ils sont substantiellement modifiés, que le système modifié soit destiné à être distribué ultérieurement ou continue d'être utilisé par le déployeur actuel.

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

4 un. Les intérêts et besoins spécifiques des PME sont pris en compte lors de la fixation des redevances pour l'évaluation de la conformité par un tiers au titre du présent article, en réduisant ces redevances proportionnellement à leur taille et à leur part de marché.

5. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 aux fins de mettre à jour les annexes VI et VII afin d'introduire des éléments des procédures d'évaluation de la conformité qui deviennent nécessaires à la lumière du progrès technique. Ce faisant, la Commission consulte l'Office AI et les parties prenantes concernées

6. La Commission est habilitée à adopter des actes délégués pour modifier les paragraphes 1 et 2 afin de soumettre les systèmes d'IA à haut risque visés aux points 2 à 8 de l'annexe III à la procédure d'évaluation de la conformité visée à l'annexe VII ou à des parties de celle-ci. La Commission adopte ces actes délégués en tenant compte de l'efficacité de la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI pour prévenir ou réduire au minimum les risques pour la santé et la sécurité et la protection des droits fondamentaux posés par ces systèmes ainsi que la disponibilité de capacités et de ressources adéquates parmi les organismes notifiés. Ce faisant, la Commission consulte l'Office AI et les parties prenantes concernées.

Article 44

Certificats

1. Les attestations délivrées par des organismes notifiés conformément à l'annexe VII sont rédigées dans une ou plusieurs langues officielles de l'Union déterminées par l'État membre dans lequel l'organisme notifié est établi ou dans une ou plusieurs langues officielles de l'Union autrement acceptées par l'organisme notifié.

2. Les certificats sont valables pour la période qu'ils indiquent, qui ne peut excéder quatre ans. À la demande du fournisseur, la validité d'un certificat peut être prolongée pour de nouvelles périodes, chacune n'excédant pas quatre ans, sur la base d'une réévaluation conformément aux procédures d'évaluation de la conformité applicables.

3. Lorsqu'un organisme notifié constate qu'un système d'IA ne satisfait plus aux exigences énoncées au chapitre 2 du présent titre, il doit, compte tenu du principe de proportionnalité, suspendre ou retirer le certificat délivré ou lui imposer toute restriction, à moins que le respect de ces exigences est assurée par des mesures correctives appropriées prises par le fournisseur du système dans un délai approprié fixé par l'organisme notifié.
L'organisme notifié motive sa décision.

Article 45

Recours contre les décisions des organismes notifiés

Les États membres veillent à ce qu'une procédure de recours contre les décisions des organismes notifiés, y compris concernant les certificats de conformité délivrés, soit accessible aux parties ayant un intérêt légitime à cette décision.

Article 46

Obligations d'information des organismes notifiés

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

a) tous les certificats d'évaluation de la documentation technique de l'Union, tous les suppléments à ces certificats, les approbations du système de gestion de la qualité délivrées conformément aux exigences de l'annexe VII;

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

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

demande d'informations qu'ils ont reçue de la surveillance du marché autorités 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 transfrontalières et la sous-traitance.

2. Chaque organisme notifié informe les autres organismes notifiés:

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

b) des attestations d'évaluation de la documentation technique de l'UE ou de tout complément à celles-ci qu'il a refusés, retirés, suspendus ou soumis à d'autres restrictions, et, sur demande, des attestations et/ou des compléments qu'il a délivrés.

3. Chaque organisme notifié fournit aux autres organismes notifiés menant des activités similaires d'évaluation de la conformité couvrant~~ les mêmes technologies d'intelligence artificielle des~~ informations pertinentes sur les questions liées aux résultats d'évaluation de la conformité négatifs et, sur demande, positifs.

Article 47

Dérogation à la procédure d'évaluation de la conformité

1. Par dérogation à l'article 43, toute autorité de contrôle nationale peut demander à une autorité judiciaire d'autoriser la mise sur le marché ou la mise en service de systèmes d'IA spécifiques à haut risque sur le territoire de l'État membre concerné, pour des raisons exceptionnelles de sécurité publique ou la protection de la vie et ~~de la santé des perso~~nnes, la protection de l'environnement et la protection des infrastructures critiques. Cette autorisation est valable pour une durée limitée, pendant que les procédures d'évaluation de la conformité nécessaires sont en cours, et prend fin une fois ces procédures achevées. L'achèvement de ces procédures est entrepris sans retard injustifié.

2. L'autorisation visée au paragraphe 1 n'est délivrée que si l'autorité nationale de contrôle et l'autorité judiciaire concluent que le système d'IA à haut risque ~~e~~st conforme aux exigences du chapitre 2 du présent titre. L'autorité de contrôle nationale informe la Commission, l'office AI et les autres États membres de toute demande présentée et de toute autorisation ultérieure délivrée en vertu du paragraphe 1.

3. Lorsque, dans les quinze jours calendaires suivant la réception des informations visées au paragraphe 2, aucune objection n'a été soulevée par un État membre ou la Commission à l'égard de la demande de l'autorité nationale de contrôle d'une autorisation délivrée par un

l'autorité nationale de contrôle d'un État membre conformément au paragraphe 1, cette autorisation est réputée justifiée.

4. Lorsque, dans les quinze jours civils suivant la réception de la notification visée au paragraphe 2, des objections sont soulevées par un État membre contre une demande émise par une autorité de contrôle nationale d'un autre État membre, ou lorsque la Commission considère que l'autorisation est contraire aux règles de l'Union loi ou la conclusion des États membres concernant la conformité du système visée au paragraphe 2 n'est pas fondée, la Commission engage sans délai une consultation avec l'État membre concerné et l'Office AI; le ou les opérateurs concernés sont consultés et ont la possibilité de présenter leur point de vue. Au vu de ces éléments, la Commission décide si l'autorisation est justifiée ou non. La Commission adresse sa décision à l'État membre concerné et au(x) opérateur(s) concerné(s) Si l'autorisation est jugée injustifiée, celle-ci est retirée par l'autorité nationale de surveillance

5. de l'État membre concerné.

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

Article 48

Déclaration de conformité UE

1. Le fournisseur établit une déclaration UE de conformité écrite, lisible par machine, physique ou électronique, pour chaque système d'IA à haut risque et la tient à la disposition de l'autorité nationale de surveillance et des autorités nationales compétentes pendant 10 ans après que le système d'IA à haut risque a été mis sur le marché ou mis en service. Une copie de la déclaration UE de conformité est soumise sur demande à l'autorité de contrôle nationale et aux autorités nationales compétentes concernées.

2. La déclaration UE de conformité indique que le système d'IA à haut risque en question satisfait aux exigences énoncées au chapitre 2 du présent titre. La déclaration UE de conformité contient les informations énoncées à l'annexe V et est traduite dans une version officielle Langue(s) de l'Union requise(s) par le ou les États membres dans lesquels le système d'IA à haut risque est mis sur le marché ou mis à disposition.

3. Lorsque les systèmes d'IA à haut risque sont soumis à une autre législation d'harmonisation de l'Union qui exige également une déclaration UE de conformité, une seule déclaration UE de conformité peut être établie pour toutes les législations 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. En établissant la déclaration UE de conformité, le fournisseur assume la responsabilité du respect des exigences énoncées au chapitre 2 du présent titre.
Le fournisseur tient à jour la déclaration UE de conformité en tant que de besoin.

5. Après consultation de l'office AI, la Commission est habilitée à adopter des actes délégués conformément à l'article 73 en vue de mettre à jour le contenu de la déclaration UE de conformité figurant à l'annexe V afin d'y introduire les éléments qui deviennent nécessaires à la lumière d'évolutions techniques progrès.

Article 49

Marquage CE de conformité

1. Le marquage CE physique doit être apposé de manière visible, lisible et indélébile pour les systèmes d'IA à haut risque avant que le système d'IA à haut risque ne soit mis sur le marché. Lorsque cela n'est pas possible ou ne se justifie pas en raison de la nature du système d'IA à haut risque, il est apposé sur l'emballage ou sur la documentation qui l'accompagne, selon le cas. Il peut être suivi d'un pictogramme ou de tout autre marquage indiquant un risque particulier de
utiliser.

1a. Pour les systèmes d'IA à haut risque uniquement numériques, un marquage CE numérique doit être utilisé, uniquement s'il est facilement accessible via l'interface à partir de laquelle le système d'intelligence artificielle est accessible ou via un code lisible par machine facilement accessible ou un autre dispositif électronique.
moyens.

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

3. Le cas échéant, le marquage CE est suivi du numéro d'identification de l'organisme notifié responsable des procédures d'évaluation de la conformité visées 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 représentant autorisé du fournisseur. Le numéro d'identification doit également être indiqué dans tout matériel promotionnel mentionnant que le système d'IA à haut risque satisfait aux exigences du marquage CE.

3a. Lorsque les systèmes d'IA à haut risque sont soumis à une autre législation de l'Union qui prévoit également l'apposition du marquage CE, le marquage CE indique que le système d'IA à haut risque satisfait également aux exigences de cette autre législation.

Article 50

Conservation des documents

Après la mise sur le marché ou la mise en service du système d'IA, le fournisseur tient à la disposition de l'autorité nationale de surveillance et des autorités nationales compétentes, pendant une période de 10 ans :

(un la documentation technique visée à l'article 11 ;

B) la documentation concernant le système de gestion de la qualité visée à l'article 17 ;

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

(d) et autres documents émis par les organismes notifiés le cas échéant ; la déclaration UE de

(e) conformité visée à l'article 48.

Article 51

Inscription

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

1a. Avant de mettre en service ou d'utiliser un système d'IA à haut risque conformément à l'article 6, paragraphe 2, les catégories suivantes de déployeurs enregistrent l'utilisation de ce système d'IA dans la base de données de l'UE visée à l'article 60:

a) les déployeurs qui sont des autorités publiques ou des institutions, organes, offices ou agences de l'Union ou des déployeurs agissant en leur nom
b) les déployeurs qui sont des entreprises désignées comme contrôleur d'accès en vertu du règlement 2022/1925 ;

1b. Les déployeurs qui ne relèvent pas de l'alinéa 1a. sont autorisés à enregistrer volontairement l'utilisation d'un système d'IA à haut risque visé à l'article 6, paragraphe 2, dans la base de données de l'UE visée à l'article 60;

1c. Une entrée d'enregistrement mise à jour doit être complétée immédiatement après chaque modification substantielle.

ANNEXE V

DÉCLARATION UE DE CONFORMITÉ

La déclaration UE de conformité visée à l'article 48 contient toutes les informations suivantes:

1. Nom et type du système IA et toute autre référence non ambiguë permettant identification et traçabilité du système d'IA ;

2. Nom et adresse du prestataire ou, le cas échéant, de son mandataire représentant;

3. Une mention indiquant que la déclaration UE de conformité est délivrée sous la seule responsabilité du fournisseur ;

4. une déclaration attestant que le système d'IA en question est conforme au présent règlement et, le cas échéant, à toute autre législation pertinente de l'Union prévoyant la délivrance d'une déclaration UE de conformité;

4a. Lorsqu'un système d'IA implique le traitement de données à caractère personnel, une déclaration indiquant que ce système d'IA est conforme aux règlements (UE) 2016/679 et (UE) 2018/1725 et à la directive (UE) 2016/680.

5. Références à toute norme harmonisée pertinente utilisée ou à toute autre norme commune spécification par rapport à laquelle la conformité est déclarée ;

6. Le cas échéant, le nom et le numéro d'identification de l'organisme notifié, une description de la procédure d'évaluation de la conformité effectuée et l'identification du certificat délivré ;

Lieu et date d'émission de la déclaration, signature, nom et fonction de la personne qui l'a signée ainsi qu'une indication pour et au nom de qui cette personne a signé.

ANNEXE VI

PROCÉDURE D'ÉVALUATION DE LA CONFORMITÉ BASÉE SUR LE CONTRÔLE INTERNE

1. La procédure d'évaluation de la conformité basée sur le contrôle interne est la procédure d'évaluation de la conformité basée sur les points 2 à 4.

2. Le prestataire vérifie que le système de management de la qualité mis en place 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 titre III, chapitre 2.

4. Le prestataire vérifie également que le processus de conception et de développement du système d'IA et son suivi post-commercialisation tel que visé à l'article 61 est conforme à la documentation technique.

ANNEXE VII

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

1. Introduction

La conformité basée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique est la procédure d'évaluation de la conformité basée sur les points 2 à 5.

2. Aperçu

Le système de gestion de la qualité approuvé pour la conception, le développement et les essais de systèmes d'IA conformément à l'article 17 est examiné conformément au point 3 et fait l'objet de la surveillance visée au point 5. La documentation technique du système d'IA est examinée en conformément au point 4.

3. Système de gestion de la qualité

3.1. La demande du fournisseur doit comprendre :

a) le nom et l'adresse du prestataire et, si la demande est introduite par le mandataire, ses nom et adresse également; (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 doit couvrir tous les aspects énumérés à l'article 17;

e) une description des procédures en place pour garantir que la gestion de la qualité le système reste adéquat et efficace ;

f) une déclaration écrite attestant 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 prestataire 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 doit continuer à être mis en œuvre et maintenu par le fournisseur afin qu'il reste 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 doit être portée à l'attention de l'organisme notifié par le prestataire.

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 informe le prestataire de sa décision. La notification contient les conclusions de l'examen des modifications et la décision d'évaluation motivée.

4. Maîtrise de la documentation technique.

4.1. Outre la demande visée au point 3, une demande auprès d'un organisme notifié de son choix est introduite par le fournisseur pour l'évaluation de la documentation technique relative au système d'IA que le fournisseur entend mettre sur le marché ou mettre en service et qui est couvert par le système de gestion de la qualité visé au point 3.

4.2. La demande doit comprendre :

(a) le nom et l'adresse du fournisseur; b) une

déclaration écrite attestant 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. À cette fin, l'organisme notifié se voit accorder un accès complet aux ensembles de données de formation et de test utilisés par le fournisseur, y compris par le biais d'interfaces de programmation d'applications (API) ou d'autres moyens et outils appropriés permettant un accès à distance.

4.4. Lors de l'examen de la documentation technique, l'organisme notifié peut exiger du prestataire qu'il fournisse des preuves supplémentaires ou qu'il procède à des essais supplémentaires afin de permettre une évaluation correcte de la conformité du système d'IA aux exigences énoncées au titre III, chapitre 2. Chaque fois que le organisme notifié n'est pas satisfait des essais effectués par le prestataire, l'organisme notifié procède directement, le cas échéant, aux essais adéquats.

4.5. S'il est nécessaire d'évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au titre III, chapitre 2, après que tous les autres moyens raisonnables de vérifier la conformité ont été épuisés et se sont révélés insuffisants, et sur demande motivée, le l'organisme notifié se voit également accorder l'accès à la formation et aux modèles formés du système d'IA, y compris ses paramètres pertinents. Cet accès doit

être soumis au droit de l'Union existant en matière de protection de la propriété intellectuelle et des secrets d'affaires. Ils prennent des mesures techniques et organisationnelles pour assurer la protection de la propriété intellectuelle et des secrets commerciaux.

4.6. La décision est notifiée au prestataire ou à son mandataire. La notification contient les conclusions de l'évaluation de la documentation technique et la décision d'évaluation motivée.

Lorsque le système d'IA est conforme aux exigences énoncées au titre III, chapitre 2, une attestation UE d'évaluation de la documentation technique est délivrée par l'organisme notifié. Le certificat indique le nom et l'adresse du fournisseur, les conclusions de l'examen, les conditions (le cas échéant) 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 pour permettre le contrôle du système d'IA en cours d'utilisation, le cas échéant.

Lorsque le système d'IA n'est pas conforme aux exigences énoncées au titre III, chapitre 2, l'organisme notifié refuse de délivrer une attestation UE d'évaluation de la documentation technique et en informe le demandeur en lui donnant les raisons détaillées de son refus.

Lorsque le système d'IA ne satisfait pas à l'exigence relative aux données utilisées pour l'entraîner, un nouvel entraînement du système d'IA sera nécessaire avant la demande d'une nouvelle évaluation de la conformité. Dans ce cas, la décision d'évaluation motivée de l'organisme notifié refusant de délivrer l'attestation UE d'évaluation de la documentation technique contient des considérations spécifiques sur les données de qualité utilisées pour former le système d'IA, notamment sur les raisons de la non-conformité.

4.7. Toute modification du système d'IA susceptible d'affecter la conformité du système d'IA aux exigences ou à sa destination doit être approuvée par l'organisme notifié qui a délivré l'attestation UE d'évaluation de la documentation technique. Le fournisseur informe cet organisme notifié de son intention d'introduire l'un des changements susmentionnés ou s'il prend connaissance de la survenance de tels changements. Les modifications envisagées sont évaluées par l'organisme notifié, qui décide si ces modifications nécessitent une nouvelle évaluation de la conformité conformément à l'article 43, paragraphe 4, ou si elles peuvent être traitées au moyen d'un supplément à l'attestation UE d'évaluation de la documentation technique. Dans ce dernier cas, l'organisme notifié évalue les modifications, notifie sa décision au fournisseur et, si les modifications sont approuvées, délivre au fournisseur un supplément à l'attestation UE d'évaluation de la documentation technique.

5. Surveillance du système de gestion de la qualité approuvé.

5.1. La surveillance exercée par l'organisme notifié visé au point 3 a pour objet de s'assurer que le prestataire remplit dûment les conditions et modalités du système de gestion de la qualité agréé.

5.2. À des fins d'évaluation, le fournisseur autorise l'organisme notifié à accéder aux locaux où se déroulent la conception, le développement et les essais des systèmes d'IA.
Le fournisseur partage en outre avec l'organisme notifié toutes les informations nécessaires.

5.3. L'organisme notifié effectue des audits périodiques pour s'assurer que le prestataire maintient et applique le système de gestion de la qualité et fournit au prestataire

avec un rapport d'audit. Dans le cadre de ces audits, l'organisme notifié peut effectuer des essais supplémentaires des systèmes d'IA pour lesquels une attestation UE d'évaluation de la documentation technique a été délivrée.

ANNEXE VIII

INFORMATIONS À SOUMETTRE LORS DE L'INSCRIPTION DU HIGH SYSTÈMES D'IA DU RISQUE CONFORMÉMENT À L'ARTICLE 51

Section A - Les informations suivantes sont fournies et ensuite tenues à jour en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 51, paragraphe 1.

1. Nom, adresse et coordonnées du fournisseur ; 2. Lorsque la soumission d'informations est effectuée par une autre personne au nom du fournisseur, le nom, l'adresse et les coordonnées de cette personne ; 3. Nom, adresse et coordonnées du mandataire, le cas échéant ; 4. Nom commercial du système d'IA et toute autre référence non ambiguë permettant identification et traçabilité du système d'IA ;

4a. Dénomination commerciale du modèle de fondation et toute référence complémentaire dénuée d'ambiguïté permettant l'identification et la traçabilité

5. Une description simple et compréhensible de a. l'objectif visé du système d'IA ; b. les composants et les fonctions pris en charge par l'IA c. une explication de base de la logique du système d'IA

5a. le cas échéant, les catégories et la nature des données susceptibles ou envisagées d'être traitées par le système d'IA ; 6. Statut du système d'IA (sur le marché ou en service ; n'est plus mis sur le marché/en service, rappelé);

7. Type, numéro et 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 ; 8. Une copie scannée du certificat visé au point 7, le cas échéant ; 9. États membres dans lesquels le système d'IA est ou a été mis sur le marché, mis en service ou mis à disposition dans l'Union ;

10. Une copie de la déclaration UE de conformité visée à l'article 48 ; 11. Mode d'emploi électronique ; ces informations ne sont pas fournies pour les systèmes d'IA à haut risque dans les domaines de l'application de la loi et de la gestion des migrations, de l'asile et du contrôle des frontières visés à l'annexe III, points 1, 6 et 7.

12. URL pour des informations supplémentaires (facultatif).

PARTIE B - Les informations suivantes sont fournies et ensuite tenues à jour en ce qui concerne les systèmes d'IA à haut risque à enregistrer conformément à l'article 51, paragraphes 1 bis, points a) et 1 ter)

1. le nom, l'adresse et les coordonnées du déployeur 2. le nom, l'adresse et les coordonnées de la personne qui soumet les informations en son nom du déployeur

3. le nom commercial du système d'IA à haut risque et toute référence complémentaire non équivoque permettant l'identification et la traçabilité du système d'IA utilisé 4. a. Une description simple et compréhensible de l'utilisation prévue du système d'IA, y compris les résultats spécifiques recherchés par l'utilisation du système, la portée géographique et temporelle de l'application b. Le cas échéant, les catégories et la nature des données à traiter par le système d'IA ; c. Dispositions pour la surveillance humaine et la gouvernance d. Le cas échéant, les organes ou personnes physiques responsables des décisions prises ou appuyées par le système d'IA.

5. un résumé des conclusions de l'étude d'impact sur les droits fondamentaux réalisée conformément à l'article 29 bis 6.

L'URL de l'entrée du système d'IA dans la base de données de l'UE par son fournisseur 7. un résumé de l'analyse d'impact sur la protection des données réalisée conformément à l'article 35 du règlement (UE) 2016/679 ou à l'article 27 de la directive (UE) 2016/680 tel que spécifié au paragraphe 6 de l'article 29 du présent règlement, le cas échéant

Section C - Les informations suivantes doivent être fournies et ensuite tenues à jour en ce qui concerne les modèles de fondation à enregistrer conformément à l'article 28b (e).

1. Nom, adresse et 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. Nom, adresse et coordonnées du mandataire, le cas échéant ; 4. Nom commercial et toute référence supplémentaire non ambiguë permettant l'identification du modèle de base 5. Description des sources de données utilisées dans le développement du modèle de base 6. Description des capacités et des limites du modèle de base, y compris les risques raisonnablement prévisibles et les mesures qui ont été prises pour les atténuer ainsi que les risques restants non atténués avec une explication sur la raison pour laquelle ils ne peuvent pas être atténués 7. Description des ressources de formation utilisées par le modèle de base, y compris la puissance de calcul requise, le temps de formation et d'autres informations pertinentes liées à la taille et à la puissance du modèle

8. Description des performances du modèle, y compris sur des benchmarks publics ou sur l'état les références de l'industrie de l'art
9. Description des résultats des tests et optimisations internes et externes pertinents du modèle
10. États membres dans lesquels le modèle de fondation est ou a été mis sur le marché, mis en service ou mis à disposition dans l'Union ; 11. URL pour des informations supplémentaires (facultatif).

Articles 16 à 29 bis et considérants associés	CA 3

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

(53 bis) En tant que signataires de la convention des Nations unies relative aux droits des personnes handicapées (CNUDPH), l'Union européenne et tous 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 l'accès, sur la base de l'égalité avec les autres, aux technologies et systèmes d'information et de communication, et d'assurer le respect de la vie privée des personnes handicapées. 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 tous les nouveaux services devrait garantir un accès complet, égal et illimité à toute personne potentiellement affectée par ou utilisant les technologies d'IA, y compris les personnes handicapées, d'une manière qui tient pleinement compte de leur dignité et de leur diversité inhérentes. Il est donc essentiel que les fournisseurs garantissent le plein respect des exigences en matière d'accessibilité, y compris la directive 2019/882 et la directive 2016/2102 du Parlement européen et du Conseil. Les fournisseurs doivent garantir la conformité à ces exigences dès la conception. Par conséquent, les mesures nécessaires doivent être intégrées autant que possible dans la conception du système d'IA à haut risque.

(54) Le fournisseur devrait mettre en place un système de gestion de la qualité solide, assurer l'accomplissement de la procédure d'évaluation de la conformité requise, établir la documentation pertinente et mettre en place un solide système de suivi après commercialisation. Pour les fournisseurs qui ont déjà mis en place des systèmes de gestion de la qualité basés sur des normes telles que ISO 9001 ou d'autres normes pertinentes, il ne faut pas s'attendre à un système de gestion de la qualité dupliqué dans son intégralité, mais plutôt à une adaptation de leurs systèmes existants à certains aspects liés au respect d'exigences spécifiques de présent règlement. Cela devrait également se refléter dans les futures activités de normalisation ou dans les orientations adoptées par la Commission à cet égard. Les autorités publiques qui mettent en service des systèmes d'IA à haut risque pour leur propre usage peuvent adopter et mettre en œuvre les règles du système de gestion de la qualité dans le cadre du système de gestion de la qualité adopté au niveau national ou régional, selon le cas, en tenant compte des spécificités de le secteur ainsi que les compétences et l'organisation de l'autorité publique en question.

(55) Lorsqu'un système d'IA à haut risque qui est un composant de sécurité d'un produit couvert par une législation sectorielle pertinente du nouveau cadre législatif n'est pas mis sur le marché ou mis en service indépendamment du produit, le fabricant du produit final tels que définis dans la législation pertinente du nouveau cadre législatif devraient respecter les obligations du fournisseur établies dans le présent règlement et notamment garantir que le système d'IA intégré dans le produit final est conforme aux exigences du présent règlement.

(56) Afin de permettre l'application du présent règlement et de créer des conditions de concurrence équitables pour les opérateurs, et compte tenu des différentes formes de mise à disposition de produits numériques, il est important de veiller à ce qu'en toutes circonstances, une personne établie dans l'Union peut 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 lorsqu'un importateur ne~~ peut être identifié, les fournisseurs établis en dehors de l'Union désignent, par mandat écrit, un représentant autorisé établi dans l'Union.

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

(58) Compte tenu de la nature des systèmes d'IA et des risques pour la sécurité et les droits fondamentaux éventuellement associés à leur utilisation, y compris en ce qui concerne la nécessité d'assurer un contrôle adéquat des performances d'un système d'IA dans un environnement réel, il convient de définir des responsabilités spécifiques pour les déployeurs. Les déployeurs devraient en particulier utiliser des systèmes d'IA à haut risque conformément aux instructions d'utilisation et certaines autres obligations devraient être prévues en ce qui concerne la surveillance du fonctionnement des systèmes d'IA et en ce qui concerne la tenue de registres, le cas échéant.

(58 bis) Si les risques liés aux systèmes d'IA peuvent résulter de la manière dont ces systèmes sont conçus, des risques peuvent également découler 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 garantir la protection des droits fondamentaux, en complément des 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 ainsi identifier des risques significatifs potentiels qui n'étaient pas prévus dans la phase de développement, grâce à une connaissance plus précise du contexte d'utilisation, des personnes ou des groupes de personnes susceptibles d'être touchées, y compris les groupes marginalisés et vulnérables. Les déployeurs doivent identifier les structures de gouvernance appropriées dans ce contexte d'utilisation spécifique, telles que les dispositifs de surveillance humaine, les procédures de traitement des plaintes et les procédures de recours, car les choix dans les structures de gouvernance peuvent contribuer à atténuer les risques pour les droits fondamentaux dans des cas d'utilisation concrets. Afin de garantir efficacement la protection des droits fondamentaux, le déployeur de systèmes d'IA à haut risque devrait donc procéder à une évaluation de l'impact sur les droits fondamentaux avant de les mettre en service. L'analyse d'impact devrait être accompagnée d'un plan détaillé décrivant les mesures ou les outils qui contribueront à atténuer les risques pour les droits fondamentaux identifiés au plus tard au moment de sa mise en œuvre. Si un tel plan ne peut être identifié, le déployeur doit s'abstenir de mettre le système en service. Lors de la réalisation de cette analyse d'impact, le déployeur doit informer l'autorité de contrôle nationale et, dans la mesure du possible, les parties prenantes concernées ainsi que les représentants des groupes de personnes susceptibles d'être affectées par le système d'IA afin de collecter les informations pertinentes jugées nécessaires pour effectuer l'analyse d'impact et sont encouragés à rendre le résumé de leur analyse d'impact sur les droits fondamentaux accessible au public sur leur site web en ligne. Ces obligations ne devraient pas s'appliquer aux PME qui, compte tenu du manque de ressources, pourraient rencontrer des difficultés pour effectuer une telle consultation. et la nécessité d'un contrôle et d'un contrôle démocratiques, les déployeurs de systèmes d'IA à haut risque qui sont des autorités publiques ou des institutions, organes, offices et agences de l'Union, ainsi que les déployeurs qui sont des entreprises désignées comme gardiennes en vertu du règlement 2022/1925 devraient être tenus de s'enregistrer l'utilisation de tout système d'IA à haut risque dans une base de données publique. D'autres déployeurs peuvent s'inscrire volontairement.

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

(60) Au sein de la chaîne de valeur de l'IA, plusieurs entités fournissent souvent des outils et des services, mais également des composants ou des processus qui sont ensuite intégrés par le fournisseur dans le système d'IA, y compris en ce qui concerne la collecte et le prétraitement des données, la formation au modèle, le recyclage du modèle, le test et évaluation, intégration dans un logiciel ou autres aspects du développement de modèles. Les entités concernées peuvent rendre leur offre commercialement disponible directement ou indirectement, par le biais d'interfaces, telles que des interfaces de programmation d'applications (API), et distribuées sous des licences libres et open source, mais aussi de plus en plus par des plateformes de main-d'œuvre d'IA, la revente de paramètres entraînés, des kits de bricolage pour construire des modèles ou offrir un accès payant à un modèle au service de l'architecture pour développer et former des modèles. Compte tenu de cette complexité de la chaîne de valeur de l'IA, tous les tiers concernés, notamment ceux qui sont impliqués dans le développement, la vente et la fourniture commerciale d'outils logiciels, de composants, de modèles pré-entraînés ou de données incorporées dans le système d'IA, ou les fournisseurs de services de réseau, devraient, sans compromettre leurs propres droits de propriété intellectuelle ou secrets commerciaux, mettre à disposition les informations, la formation ou l'expertise requises et coopérer, le cas échéant, avec les fournisseurs pour leur permettre de contrôler tous les aspects pertinents de la conformité du système d'IA qui relève de présent règlement. Pour permettre une gouvernance de la chaîne de valeur de l'IA rentable, le niveau de contrôle doit être explicitement divulgué par chaque tiers qui fournit au fournisseur un outil, un service, un composant ou un processus qui est ensuite intégré par le fournisseur dans le système d'IA.

(60 bis) Lorsqu'une partie se trouve dans une position de négociation plus forte, il existe un risque qu'elle tire parti de cette position au détriment de l'autre partie contractante lors de la négociation de la fourniture d'outils, de services, de composants ou de processus qui sont utilisés ou intégrés dans un système d'IA à haut risque ou les recours en cas de violation ou de résiliation des obligations connexes. De tels déséquilibres contractuels nuisent particulièrement aux micro, petites et moyennes entreprises ainsi qu'aux start-ups, à moins qu'elles ne soient détenues ou sous-traitées par une entreprise qui est en mesure de rémunérer le sous-traitant de manière appropriée, car elles sont dépourvues d'une véritable capacité de négociation les conditions de l'accord contractuel et ne peut avoir d'autre choix que d'accepter les conditions contractuelles "à prendre ou à laisser". Par conséquent, les clauses contractuelles abusives régissant la fourniture d'outils, de services, de composants ou de processus qui sont utilisés ou intégrés dans un système d'IA à haut risque ou les recours en cas de violation ou de résiliation des obligations connexes ne devraient pas être contraignantes pour ces micro, petites ou moyennes petites entreprises et start-up lorsqu'elles leur ont été imposées unilatéralement.

(60 ter) Les règles relatives aux clauses contractuelles devraient tenir compte du principe de la liberté contractuelle en tant que concept essentiel dans les relations interentreprises. Par conséquent, toutes les clauses contractuelles ne devraient pas être soumises à un test de caractère abusif, mais uniquement les clauses imposées unilatéralement aux micro, petites et moyennes entreprises et aux start-up. Cela concerne les situations "à prendre ou à laisser" dans lesquelles une partie fournit une certaine clause contractuelle et la micro, petite ou moyenne entreprise et la start-up ne peuvent pas influencer le contenu de cette clause malgré une tentative de négociation. Une clause contractuelle qui est simplement fournie par une partie et acceptée par la micro, petite ou moyenne entreprise ou une start-up ou une clause qui est négociée puis convenue de manière modifiée entre les parties contractantes ne doit pas être considérée comme imposée unilatéralement .

(60 quater) En outre, les règles relatives aux clauses contractuelles abusives ne devraient s'appliquer qu'aux éléments d'un contrat liés à la fourniture d'outils, de services, de composants ou

processus utilisés ou intégrés dans un système d'IA à haut risque ou les recours en cas de violation ou de résiliation des obligations connexes. Les autres parties du même contrat, sans rapport avec ces éléments, ne devraient pas être soumises au critère du caractère abusif prévu par le présent règlement.

(60 quinquies) Les critères permettant d'identifier les clauses contractuelles abusives ne devraient être appliqués qu'aux clauses contractuelles excessives, lorsqu'il y a abus d'une position de négociation plus forte. La grande majorité des clauses contractuelles qui sont commercialement plus favorables à une partie qu'à l'autre, y compris celles qui sont normales dans les contrats entre entreprises, sont une expression normale du principe de liberté contractuelle et continuent de s'appliquer. Si une clause contractuelle n'est pas incluse dans la liste des clauses qui sont toujours considérées comme abusives, la disposition générale sur l'abus s'applique. À cet égard, les clauses répertoriées comme clauses abusives devraient servir de référence pour interpréter la disposition générale relative à l'abus d'équité.

(60 sexies) Les modèles de base sont un développement récent, dans lequel des modèles d'IA sont développés à partir d'algorithmes conçus pour optimiser la généralité et la polyvalence des résultats. Ces modèles sont souvent formés sur un large éventail de sources de données et de grandes quantités de données pour accomplir un large éventail de tâches en aval, y compris certaines pour lesquelles ils n'ont pas été spécifiquement développés et formés. Ces systèmes peuvent être unimodaux ou multimodaux, entraînés par diverses méthodes telles que l'apprentissage supervisé ou l'apprentissage renforcé. Les systèmes d'IA avec un objectif spécifique ou des systèmes d'IA à usage général peuvent être une implémentation d'un modèle de base, ce qui signifie que chaque modèle de base peut être réutilisé dans d'innombrables systèmes d'IA en aval ou à usage général. Ces modèles revêtent une importance croissante pour de nombreuses applications et systèmes en aval.

(60 septies) Dans le cas de modèles de base fournis en tant que service, par exemple via un accès API, la coopération avec les fournisseurs en aval devrait s'étendre tout au long de la période pendant laquelle ce service est fourni et pris en charge, afin de permettre une atténuation appropriée des risques, à moins que le fournisseur de le modèle de base transfère le modèle de formation ainsi que des informations complètes et appropriées sur les ensembles de données et le processus de développement du système ou restreint le service, tel que l'accès à l'API, de manière à ce que le fournisseur en aval soit en mesure de s'y conformer pleinement Régulation sans autre soutien de la part du fournisseur d'origine du modèle de fondation.

(60 octies) Compte tenu de la nature et de la complexité de la chaîne de valeur des systèmes d'IA, il est essentiel de clarifier le rôle des acteurs contribuant au développement des systèmes d'IA. Il existe une grande incertitude quant à l'évolution des modèles de fondation, tant en termes de typologie des modèles qu'en termes d'autonomie. Il est donc essentiel de clarifier la situation juridique des fournisseurs de modèles de fondation. Combiné avec leur complexité et leur impact inattendu, le manque de contrôle du fournisseur d'IA en aval sur le développement du modèle de base et le déséquilibre de pouvoir qui en résulte et afin d'assurer un partage équitable des responsabilités tout au long de la chaîne de valeur de l'IA, ces modèles devraient faire l'objet d'un contrôle proportionné et plus exigences et obligations spécifiques en vertu du présent règlement, à savoir que les modèles de base devraient évaluer et atténuer les risques et les préjudices éventuels grâce à une conception, des tests et des analyses appropriés, devraient mettre en œuvre des mesures de gouvernance des données, y compris l'évaluation des biais, et devraient se conformer aux exigences de conception technique pour garantir des niveaux appropriés de performance, prévisibilité, interprétabilité, corrigibilité, sûreté et cybersécurité et doivent être conformes aux normes environnementales. Ces obligations doivent s'accompagner de

normes. En outre, les modèles de fondation devraient avoir des obligations d'information et préparer toute la documentation technique nécessaire pour que les fournisseurs potentiels en aval puissent se conformer à leurs obligations au titre du présent règlement. Les modèles de base génératifs devraient garantir la transparence sur le fait que le contenu est généré par un système d'IA, et non par des humains. Ces exigences et obligations spécifiques ne reviennent pas à considérer les modèles de base comme des systèmes d'IA à haut risque, mais devraient garantir que les objectifs du présent règlement visant à assurer un niveau élevé de protection des droits fondamentaux, de la santé et de la sécurité, de l'environnement, de la démocratie et de l'État de droit sont atteint. Les modèles pré-entraînés développés pour un ensemble d'applications plus étroit, moins général et plus limité qui ne peuvent pas être adaptés à un large éventail de tâches telles que les systèmes d'IA polyvalents simples ne devraient pas être considérés comme des modèles de base aux fins du présent règlement, en raison de leur plus grande interprétabilité qui rend leur comportement moins imprévisible.

(60 nonies) Compte tenu de la nature des modèles de base, l'expertise en matière d'évaluation de la conformité fait défaut et les méthodes d'audit par des tiers sont encore en cours de développement . Le secteur lui-même développe donc de nouvelles façons d'évaluer les modèles fondamentaux qui remplissent en partie l'objectif de l'audit (comme l'évaluation des modèles, le red-teaming ou les techniques de vérification et de validation de l'apprentissage automatique). Ces évaluations internes pour les modèles de base devraient être largement applicables (par exemple, indépendamment des canaux de distribution, des modalités, des méthodes de développement), pour traiter les risques spécifiques à ces modèles en tenant compte des pratiques de pointe de l'industrie et se concentrer sur le développement de capacités techniques suffisantes. la compréhension et le contrôle du modèle, la gestion des risques raisonnablement prévisibles, et une analyse et un test approfondis du modèle par des mesures appropriées, telles que la participation d'évaluateurs indépendants.
Étant donné que les modèles de base constituent un développement nouveau et en évolution rapide dans le domaine de l'intelligence artificielle, il convient que la Commission et l'Office de l'IA surveillent et évaluent périodiquement le cadre législatif et de gouvernance de ces modèles, et en particulier des systèmes d'IA générative basés sur de tels modèles, qui soulèvent des questions importantes liées à la génération de contenus en violation du droit de l'Union, des règles de droit d'auteur et des utilisations abusives potentielles.

Il convient de préciser que le présent règlement devrait être sans préjudice du droit de l'Union sur le droit d'auteur et les droits voisins, y compris les directives 2001/29/CE, 2004/48/ECR et (UE) 2019/790 du Parlement européen et du Conseil.
Il convient de préciser que le présent règlement devrait être sans préjudice du droit de l'Union sur le droit d'auteur et les droits voisins, y compris les directives 2001/29/CE, 2004/48/ECR et (UE) 2019/790 du Parlement européen et du Conseil.

CHAPITRE 3

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

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

Article 16

Obligations des fournisseurs de systèmes d'IA à haut risque

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

(un) s'assurer que leurs systèmes d'IA à haut risque sont conformes aux exigences énoncées dans chapitre 2 du présent titre avant de les mettre sur le marché ou de les mettre en service ;

(aa) indiquer leur nom, leur raison sociale ou leur marque déposée, ainsi que leur adresse et leurs coordonnées sur le système d'IA à haut risque ou, lorsque cela n'est pas possible, sur la documentation qui l'accompagne, selon le cas ;

(un B) veiller à ce que les personnes physiques à qui est confiée la surveillance humaine des systèmes d'IA à haut risque soient spécifiquement sensibilisées au risque de biais d'automatisation ou de confirmation ; (ac)

fournir des spécifications pour les données d'entrée, ou toute autre information pertinente en termes d'ensembles de données utilisés, y compris leurs limites et hypothèses, en tenant compte de l'objectif visé et des utilisations abusives prévisibles et raisonnablement prévisibles des système d'IA ;

avoir mis en place un système de gestion de la qualité conforme à l'article 17 ; établir et

(avant JC) conserver la documentation technique du système d'IA à haut risque mentionné à l'article 11 ;

(d) lorsqu'ils sont sous leur contrôle, conserver les journaux générés automatiquement par leurs systèmes d'IA à haut risque qui sont nécessaires pour assurer et démontrer la conformité avec cette Règlement, conformément à l'article 20 ; veillent à ce

(C'est) que le système d'IA à haut risque soit soumis à la procédure d'évaluation de la conformité appropriée, avant sa mise sur le marché ou sa mise en service, conformément à l'article 43;

e bis) établit une déclaration UE de conformité conformément à l'article 48;

(eb) apposer le marquage CE sur le système d'IA à haut risque pour indiquer la conformité avec ce règlement, conformément à l'article 49 ; respecter les

(F) obligations d'enregistrement visées à l'article 51 ;

(g) prend les mesures correctives nécessaires visées à l'article 21 et fournit des informations à cet égard, si le système d'IA à haut risque n'est pas conforme aux exigences énoncées au chapitre 2 du présent titre; informer les autorités nationales compétentes des États

(h) membres dans lesquels elles ont mis à disposition ou en service le système d'IA et, le cas échéant, l'organisme notifié de la non-conformité et de toute action corrective entreprise

(je) apposer le marquage CE sur le système d'IA à haut risque pour indiquer la conformité avec le présent règlement, conformément à l'article 49; sur demande

(j) motivée d'une autorité nationale de surveillance, démontrer la conformité du système d'IA à haut risque avec les exigences énoncées au chapitre 2 du présent titre.

(k) veiller à ce que le système d'IA à haut risque soit conforme aux exigences d'accessibilité.

Article 17

Système de gestion de la qualité

1. Les fournisseurs de systèmes d'IA à haut risque doivent mettre en place un système de gestion de la qualité garantissant le respect du présent règlement. Elle doit être documentée de manière systématique et ordonnée sous la forme de politiques, de procédures ou d'instructions écrites, et peut être intégrée dans un système de gestion de la qualité existant en vertu de la législation sectorielle. Il comprend au moins les aspects suivants: a) une stratégie de conformité réglementaire, y compris

~~le respect des procédures d'évaluation de la conformité et des procédures de gestion des modifications du système d'IA à haut risque~~

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

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

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

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

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

g) le système de gestion des risques visé à l'article 9; h) la mise en place,

la mise en œuvre et la maintenance d'un système de surveillance après commercialisation, conformément à l'article 61;

(i) les procédures relatives au signalement des incidents graves et des dysfonctionnements dans conformément à l'article 62;

(j) le traitement de la communication avec les autorités compétentes concernées, y compris les autorités sectorielles, fourni~~ssant ou soutenant l'accès aux données, les organismes notifiés, les autres opérateurs, les clients ou les autres parties intéressées~~

(k) des systèmes et des procédures d'archivage de tous les documents pertinents et information;

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

(m) un cadre de responsabilité définissant les responsabilités de la direction 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 prestataire. Les fournisseurs respectent en tout état de cause le degré de rigueur et le niveau de protection requis pour assurer la conformité de leurs systèmes d'IA avec le présent règlement.

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

~~Article 18~~

~~Obligation de rédiger une documentation technique~~

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

~~2. Les prestataires qui sont des établissements de crédit régis par la directive 2013/36/UE conservent la documentation technique dans le cadre de la documentation concernant la gouvernance interne, les dispositifs, les processus et les mécanismes conformément à l'article 74 de ladite directive.~~

~~Article 19~~

~~Évaluation de la conformité~~

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

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

Article 20

Journaux générés automatiquement

1. Les fournisseurs de systèmes d'IA à haut risque doivent conserver les journaux générés automatiquement par leurs systèmes d'IA à haut risque, dans la mesure où ces journaux sont sous leur ~~contrôle en vertu d'un accord contractuel avec l'utilisateur ou autrement par la loi. Sans préju~~dice du droit de l'Union ou du droit national applicable, les registres sont conservés pendant une période d'au moins 6 mois. La période de conservation est conforme aux normes du secteur et adaptée à l'objectif visé par le système d'IA à haut risque et aux obligations légales applicables en vertu du droit de l'Union ~~ou du droit national.~~

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

Article 21
Mesures correctives

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

1a. Dans les cas visés au paragraphe 1, les prestataires informent immédiatement :

un. les distributeurs,
b. les importateurs,
c. les autorités nationales compétentes des États membres dans lesquels elles ont mis à disposition ou mis en service le système d'IA; et d.
le déployeur, si possible.

1b. Les fournisseurs informent également le mandataire, s'il en a été désigné conformément à l'article 25, et l'organisme notifié si le système d'IA à haut risque a dû faire l'objet d'une évaluation de conformité par un tiers conformément à l'article 43.
Le cas échéant, ils doivent également rechercher les causes en collaboration avec le déployeur.

Article 22
Devoir d'information

1. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 65, paragraphe 1, et ~~que ce risque est connu~~ du fournisseur du système qui prend connaissance de ce risque, ce fournisseur informe immédiatement les autorités de surveillance nationales de l'État membre Les États dans lesquels il a mis le système à disposition et, le cas échéant, l'organisme notifié qui a délivré un certificat pour le système d'IA à haut risque, en particulier la nature de la non-conformité et de toute action corrective pertinente entreprise.

1a. Dans les cas visés au paragraphe 1, les fournisseurs du système d'IA à haut risque informent immédiatement:

un. les distributeurs,
b. les importateurs,
c. les autorités nationales compétentes des États membres dans lesquels elles ont mis à disposition ou mis en service le système d'IA; et d. les
déployeurs, si possible,

1b. Les prestataires informent également le mandataire, s'il a été désigné conformément à l'article 25.

Article 23

Coopération avec les autorités compétentes, l'Office et la Commission

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

Sur demande motivée d'une autorité nationale compétente ou, le cas échéant, de la Commission, les fournisseurs et, le cas échéant, les déployeurs donnent également à l'autorité nationale compétente requérante ou à la Commission, selon le cas, l'accès aux journaux générés automatiquement par le système d'IA à risque, dans la mesure où ces journaux sont sous leur contrôle.

Toute information obtenue par une autorité nationale compétente ou par la Commission conformément aux dispositions du présent article est considérée comme un secret d'affaires et traitée dans le respect des obligations de confidentialité énoncées à l'article 70 .

Article 24

Obligations des fabricants de produits

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

Article 25

Représentants autorisés

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

1a. Le mandataire réside ou est établi dans l'un des États membres où se déroulent les activités visées à l'article 2, paragraphe 1, point c ter).

1b. Le prestataire dote son mandataire des pouvoirs et ressources nécessaires pour s'acquitter de ses missions au titre du présent règlement.

2. Le mandataire exécute les tâches précisées dans le mandat reçu du prestataire. Elle fournit une copie du mandat aux autorités de surveillance du marché sur demande, dans une langue officielle de l'Union déterminée par l'autorité nationale compétente. Aux fins du présent règlement, le mandat habilite le mandataire à accomplir les tâches suivantes :

a) s'assurer que la déclaration UE de conformité et la documentation technique ont été établies et qu'une procédure appropriée d'évaluation de la conformité a été effectuée par le fournisseur;

a bis) tient à la disposition des autorités nationales compétentes et des autorités nationales visées à l'article 63, paragraphe 7, une copie de la déclaration UE de conformité, la documentation technique et, le cas échéant, l'attestation délivrée par l'organisme notifié;

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

c) coopère avec les autorités nationales de surveillance, sur demande motivée, à toute mesure prise par l'autorité pour réduire et atténuer les risques posés par le système d'IA à haut risque.

c bis) le cas échéant, se conformer aux obligations d'enregistrement visées à l'article 51 ou, si l'enregistrement est effectué par le prestataire lui-même, s'assurer que les informations visées à l'annexe VIII, point 3, sont correctes.

2a. Le mandataire est mandaté pour être contacté, en plus ou à la place du prestataire, notamment par l'autorité nationale de contrôle ou les autorités nationales compétentes, sur toutes les questions liées au respect du présent règlement.

2b. Le mandataire met fin au mandat s'il considère ou a des raisons de considérer que le prestataire agit contrairement à ses obligations au titre du présent règlement. Dans ce cas, il informe également immédiatement l'autorité de contrôle nationale de l'État membre dans lequel il est établi, ainsi que, le cas échéant, l'organisme notifié compétent, de la résiliation du mandat et des motifs de celle-ci.

Article 26

Obligations des importateurs

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

a) la procédure d'évaluation de la conformité pertinente visée à l'article 43 a été effectué par le fournisseur de ce système d'IA

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

c) le système porte le marquage de conformité requis et est accompagné de la documentation et des instructions d'utilisation requises;

c bis) le cas échéant, le prestataire a désigné un mandataire conformément à l'article 25, paragraphe 1.

2. Lorsqu'un importateur considère ou a des raisons de considérer qu'un système d'IA à haut risque n'est pas conforme au présent règlement, est contrefait ou accompagné de documents falsifiés, il ne met pas ce système sur le marché tant que ce système d'IA n'a pas été mis en service. conformité. Lorsque le système d'IA à haut risque présente un risque au sens de l'article 65, paragraphe 1, l'importateur en informe le fournisseur du système d'IA et les autorités de surveillance du marché.

3. Les importateurs indiquent leur nom, leur raison sociale ou leur 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 la documentation qui l'accompagne, le cas échéant.

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

5. Les importateurs fournissent aux autorités nationales compétentes, sur demande motivée, toutes les informations et tous les documents nécessaires pour démontrer la conformité d'un système d'IA à haut risque avec les exigences énoncées au chapitre 2 du présent titre dans une langue facilement compréhensible par y compris l'accès aux journaux générés automatiquement par le système d'IA à haut risque dans la mesure où ces journaux sont sous le contrôle du fournisseur conformément à l'article 20.

5a. Les importateurs coopèrent avec les autorités nationales compétentes sur toute mesure que ces autorités prennent pour réduire et atténuer les risques posés par le système d'IA à haut risque.

Article 27

Obligations des distributeurs

1. Avant de mettre un système d'IA à haut risque à disposition sur le marché, les distributeurs vérifient que le système d'IA à haut risque porte le marquage CE de conformité requis, qu'il est accompagné de la documentation et des instructions d'utilisation requises, et que le fournisseur et l'importateur du système, selon le cas, ont respecté leurs obligations énoncées dans le présent règlement respectivement à l'article 16 et à l'article 26.

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 au chapitre 2 du présent titre, il ne rend pas le système à haut risque système d'IA disponible sur le marché tant que ce système n'a pas été mis en conformité avec ces exigences. En outre, lorsque le système présente un risque au sens de l'article 65, paragraphe 1, le distributeur en informe le fournisseur ou l'importateur du système, ainsi que l'autorité nationale compétente concernée, selon le cas. Les distributeurs veillent à ce que, tout en un système d'IA à haut risque

3. est sous leur responsabilité, le cas échéant, les conditions de stockage ou de transport ne compromettent pas la conformité du système aux exigences prévues au chapitre 2 du présent titre.

4. Un distributeur qui 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 au chapitre 2 du présent titre prend les mesures correctives nécessaires pour mettre ce système en conformité avec ces exigences, le retirer ou le rappeler ou veille à ce que le fournisseur, l'importateur ou tout opérateur concerné, selon le cas, prenne ces mesures correctives. Où le

système d'IA à haut risque présente un risque au sens de l'article 65, paragraphe 1, le distributeur informe immédiatement le fournisseur ou l'importateur du système et les autorités nationales compétentes des États membres dans lesquels il a mis le produit à disposition à cet effet , précisant notamment la non-conformité et les éventuelles actions correctives entreprises.

5. Sur demande motivée d'une autorité nationale compétente, les distributeurs de systèmes d'IA à haut risque fournissent à cette autorité toutes les informations et tous les documents en leur possession ou à leur disposition, conformément aux obligations des distributeurs telles que décrites au paragraphe 1, qui sont nécessaires pour démontrer la conformité d'un système à haut risque avec les exigences énoncées au chapitre 2 du présent titre. Les distributeurs coopèrent également avec cette autorité nationale compétente sur toute mesure prise par cette autorité.

5a. Les distributeurs coopèrent avec les autorités nationales compétentes sur toute mesure que ces autorités prennent pour réduire et atténuer les risques posés par le système d'IA à haut risque.

Article 28

Responsabilités tout au long de la chaîne de valeur de l'IA des fournisseurs, distributeurs, importateurs, déployeurs ou autres tiers

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 du fournisseur en vertu de l'article 16, dans l'une des circonstances suivantes:

(a) ils apposent leur nom ou leur marque sur un système d'IA à haut risque déjà mis sur le marché ou mis en service

b) ils apportent 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 reste un système d'IA à haut risque conformément à l'article 6;

b bis) ils apportent une modification substantielle à un système d'IA, y compris un système d'IA à usage général, qui n'a pas été classé comme à haut risque et a déjà été mis sur le marché ou mis en service de telle manière que le système d'IA devient un système d'IA à haut risque conformément à l'article 6

2. Lorsque les circonstances visées au paragraphe 1, points a) à b bis), se produisent, le fournisseur qui a initialement mis le système d'IA sur le marché ou l'a mis en service n'est plus considéré comme un fournisseur de ce système d'IA spécifique aux fins du présent règlement. Cet ancien fournisseur fournira au nouveau fournisseur la documentation technique et toutes les autres capacités d'information pertinentes et raisonnablement attendues du système d'IA, l'accès technique ou toute autre assistance basée sur l'état de la technique généralement reconnu qui sont nécessaires pour l'exécution des obligations fixées dans le présent règlement.

Le paragraphe 2 s'applique également aux fournisseurs de modèles de fondation tels que définis à l'article 3 lorsque le modèle de fondation est directement intégré dans un système d'IA à haut risque.

2a. Le fournisseur d'un système d'IA à haut risque et le tiers qui fournit des outils, des services, des composants ou des processus qui sont utilisés ou intégrés dans le système d'IA à haut risque doivent, par accord écrit, spécifier les informations, les capacités, l'accès technique et/ou

autre assistance, basée sur l'état de la technique généralement reconnu, que le tiers doit fournir afin de permettre au fournisseur du système d'IA à haut risque de se conformer pleinement aux obligations prévues par le présent règlement.

La Commission élabore et recommande des clauses contractuelles types non contraignantes 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 des systèmes d'IA à haut risque afin d'aider les deux parties à rédiger et négocier des contrats avec des droits et obligations contractuels équilibrés, cohérents avec le niveau de contrôle de chaque partie. Lors de l'élaboration de clauses contractuelles types non contraignantes, la Commission tient compte des éventuelles exigences contractuelles applicables dans des secteurs ou des cas commerciaux spécifiques.

Les clauses contractuelles non contraignantes sont publiées et disponibles gratuitement dans un format électronique facilement utilisable sur le site Internet de l'Office AI.

2b. Aux fins du présent article, les secrets d'affaires sont préservés et ne sont divulgués qu'à condition que toutes les mesures spécifiques nécessaires en vertu de la directive (UE) 2016/943 soient prises au préalable pour préserver leur confidentialité, notamment à l'égard des tiers. Si nécessaire, des dispositions techniques et organisationnelles appropriées peuvent être convenues pour protéger les droits de propriété intellectuelle ou les secrets commerciaux.

Article 28(a)

Clauses contractuelles abusives imposées unilatéralement à une PME ou une startup

1. Une clause contractuelle concernant la fourniture d'outils, de services, de composants ou de processus qui sont utilisés ou intégrés dans un système d'IA à haut risque ou les recours en cas de violation ou de résiliation d'obligations connexes imposées unilatéralement par une entreprise à une PME ou la création ne lie pas cette dernière entreprise si elle est déloyale.

2. Une clause contractuelle n'est pas considérée comme abusive lorsqu'elle découle
Droit syndical.

3. Une clause contractuelle est abusive si elle est d'une nature telle qu'elle porte objectivement atteinte à la capacité de la partie à laquelle la clause a été unilatéralement imposée de protéger son intérêt commercial légitime dans l'information en question ou si son utilisation s'écarte manifestement ~~d~~des bonnes pratiques commerciales. pratique dans la fourniture d'outils, de services, de composants ou de processus utilisés ou intégrés dans un système d'IA à haut risque, contraire à la bonne foi et à la loyauté ou créant un déséquilibre significatif entre les droits et les obligations des parties au contrat. Une clause contractuelle est également abusive si elle a pour effet de transférer les sanctions visées à l'article 71 ou les frais de justice associés entre les parties au contrat, comme indiqué à l'article 71, paragraphe 8 (nouveau).

4. Une clause contractuelle est abusive au sens du présent article si son objet ou son effet est de :

(un) exclure ou limiter la responsabilité de la partie qui a unilatéralement imposé le terme pour des actes intentionnels ou une négligence grave ; exclure

(b) les recours dont dispose la partie à qui le terme a été imposé unilatéralement en cas d'inexécution des obligations contractuelles

obligations ou la responsabilité de la partie qui a unilatéralement imposé le terme en cas de manquement à ces obligations ; donner à la partie qui

(c) a imposé unilatéralement la clause le droit exclusif de déterminer si la documentation technique, les informations fournies sont conformes au contrat ou d'interpréter toute clause du contrat.

5. Une clause contractuelle est considérée comme imposée unilatéralement au sens du présent article si elle a été fournie par une partie contractante et si l'autre partie contractante n'a pas pu influencer son contenu malgré une tentative de négociation. La partie contractante qui a fourni une clause contractuelle a la charge de prouver que cette clause n'a pas été imposée unilatéralement.

6. Lorsque la clause contractuelle abusive est dissociable des clauses restantes du contrat, ces clauses restantes restent contraignantes. La partie qui a fourni la clause contestée ne peut faire valoir que la clause est une clause abusive.

7. Le présent article s'applique à tous les nouveaux contrats entrés en vigueur après le ... [date d'entrée en vigueur du présent règlement]. Les entreprises disposent d'un délai de trois ans à compter de cette date pour réexaminer les obligations contractuelles existantes soumises au présent règlement.

8. Compte tenu de la rapidité avec laquelle les innovations se produisent sur les marchés, la liste des clauses contractuelles abusives visée à l'article 28 bis est réexaminée régulièrement par la Commission et, si nécessaire, mise à jour en fonction des nouvelles pratiques commerciales.

Article 28 ter

Obligations du fournisseur d'un modèle de fondation

1. Le fournisseur d'un modèle de base s'assure, avant de le mettre à disposition sur le marché ou de le mettre en service, qu'il est conforme aux exigences énoncées dans le présent article, qu'il soit fourni en tant que modèle autonome ou intégré. dans un système d'IA ou un produit, ou fournis sous des licences libres et open source, en tant que service, ainsi que d'autres canaux de distribution.

2. Aux fins du paragraphe 1, le fournisseur d'un modèle de fondation:

(un) démontrer par une conception, des essais et une analyse appropriés que l'identification, la réduction et l'atténuation des risques raisonnablement prévisibles pour la santé, la sécurité, les droits fondamentaux, l'environnement, la démocratie et l'état de droit avant et tout au long du développement avec des méthodes appropriées telles que la participation de experts indépendants, ainsi que la documentation des risques restants non atténuables après le développement ;

(b) traiter et incorporer uniquement les ensembles de données qui sont soumis à des mesures de gouvernance des données appropriées pour les modèles de base, en particulier des mesures pour examiner la pertinence des sources de données et les biais éventuels et les mesures d'atténuation appropriées ;

c) concevoir et développer le modèle de base afin d'atteindre tout au long de son cycle de vie des niveaux appropriés de performance, de prévisibilité, d'interprétabilité,

la corrigibilité, la sûreté et la cybersécurité évaluées par des méthodes appropriées telles que l'évaluation de modèles avec la participation d'experts indépendants, une analyse documentée et des tests approfondis lors de la conceptualisation, de la conception et du développement ;

(d) concevoir et développer le modèle de base, en utilisant les normes applicables pour réduire la consommation d'énergie, l'utilisation des ressources et les déchets, ainsi que pour augmenter l'efficacité énergétique et l'efficacité globale du système. Cela s'entend sans préjudice du droit de l'Union et du droit national en vigueur et cette obligation ne s'applique pas avant la publication des normes visées à l'article 40. Ils doivent être conçus avec des capacités permettant de mesurer et d'enregistrer la consommation d'énergie et de ressources et, lorsque cela est techniquement faisable, d'autres impacts environnementaux que le déploiement et l'utilisation des systèmes peuvent avoir sur l'ensemble de leur cycle de vie ;

(e) établir une documentation technique complète et des instructions d'utilisation compréhensibles afin de permettre aux fournisseurs en aval de se conformer à leurs obligations en vertu des articles 16 et 28.1. ;

(F) établir un système de gestion de la qualité pour assurer et documenter le respect du présent article, avec la possibilité d'expérimenter le respect de cette exigence,

(g) enregistrer ce modèle de fondation dans la base de données de l'UE visée à l'article 60, conformément aux instructions énoncées à l'annexe VIII, paragraphe C.

Pour satisfaire à ces exigences, il est tenu compte de l'état de la technique généralement reconnu, y compris tel qu'il ressort des normes harmonisées ou des spécifications communes pertinentes, ainsi que des méthodes d'évaluation et de mesure les plus récentes, reflétées notamment dans les orientations et les capacités d'analyse comparative visées à l'article 58a (nouveau).

3. Les fournisseurs de modèles de fondation tiennent, pendant une période se terminant dix ans après la mise sur le marché ou la mise en service de leurs modèles de fondation, la documentation technique visée au paragraphe 1, point c), à la disposition des autorités nationales compétentes;

4. Les fournisseurs de modèles de base utilisés dans les systèmes d'IA spécifiquement destinés à générer, avec des niveaux d'autonomie variables, des contenus tels que du texte, des images, de l'audio ou de la vidéo complexes ("IA générative") et les fournisseurs qui spécialisent un modèle de base dans un système d'IA générative, devra en plus

un) respecter les obligations de transparence visées à l'article 52, paragraphe 1,

b) former et, le cas échéant, concevoir et développer le modèle de fondation de manière à garantir des garanties adéquates contre la génération de contenu en violation du droit de l'Union, conformément à l'état de la technique généralement reconnu, et sans préjudice des droits fondamentaux, y compris la liberté d'expression,

c) sans préjudice de la législation nationale ou de l'Union sur le droit d'auteur, documenter et mettre à la disposition du public un résumé suffisamment détaillé de l'utilisation des données de formation protégées par le droit d'auteur.

Article 29

Obligations des déployeurs de systèmes d'IA à haut risque

1. Les déployeurs de systèmes d'IA à haut risque prennent les mesures techniques et organisationnelles appropriées pour garantir qu'ils utilisent ces systèmes conformément aux instructions d'utilisation accompagnant les systèmes, conformément aux paragraphes 2 et 5 du présent article.

1a. Dans la mesure où les déployeurs exercent un contrôle sur le système d'IA à haut risque, ils doivent

je) mettre en œuvre une surveillance humaine selon les exigences énoncées dans le présent Régulation

(ii) veiller à ce que les personnes physiques chargées d'assurer la surveillance humaine des systèmes d'IA à haut risque soient compétentes, dûment qualifiées et formées, et disposent des ressources nécessaires pour assurer la surveillance efficace du système d'IA conformément à l'article 14

(iii) veiller à ce que l'efficacité des mesures de robustesse et de cybersécurité pertinentes et appropriées fasse l'objet d'un contrôle régulier et soit régulièrement ajustée ou mise à jour.

2. Les obligations visées aux paragraphes 1, 1a, 1b et 1c sont sans préjudice des autres obligations du déployeur en vertu du droit de l'Union ou du droit national et du pouvoir discrétionnaire du déployeur d'organiser ses propres ressources et activités aux fins de la mise en œuvre des mesures de surveillance humaine indiquées par le fournisseur.

3. Sans préjudice des paragraphes 1, 1a, 1b et 1c, dans la mesure où le déployeur exerce un contrôle sur les données d'entrée, ce déployeur veille à ce que les données d'entrée soient pertinentes et suffisamment représentatives au regard de la finalité du système d'IA à haut risque.

4. Les déployeurs surveillent le fonctionnement du système d'IA à haut risque sur la base des instructions d'utilisation et, le cas échéant, informent les prestataires conformément à l'article 61. Lorsqu'ils ont des raisons de penser que l'utilisation conformément aux instructions d'utilisation peut entraîner dans le système d'IA présentant un risque au sens de l'article 65, paragraphe 1, ils informent, sans retard injustifié, le fournisseur ou le distributeur et les autorités de surveillance nationales compétentes et suspendent l'utilisation du système. Ils informent également immédiatement d'abord le fournisseur, puis l'importateur ou le distributeur et les autorités nationales de surveillance compétentes lorsqu'ils ont identifié un incident grave ou un dysfonctionnement au sens de l'article 62 et interrompent l'utilisation du système d'intelligence artificielle. Si le déployeur n'est pas en mesure de joindre le fournisseur, l'article 62 s'applique mutatis mutandis.

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

5. Les déployeurs de systèmes d'IA à haut risque conservent les journaux générés automatiquement par ce système d'IA à haut risque, dans la mesure où ces journaux sont sous leur contrôle et sont

nécessaires pour garantir et démontrer le respect du présent règlement, pour les audits ex post de tout dysfonctionnement, incident ou mauvaise utilisation raisonnablement prévisible du système, ou pour garantir et surveiller le bon fonctionnement du système tout au long de son cycle de vie. Sans préjudice du droit de l'Union ou du droit national applicable, les registres sont conservés pendant une période d'au moins 6 mois. La période de conservation est conforme aux normes du secteur et adaptée à l'objectif visé par le système d'IA à haut risque et aux obligations légales applicables en vertu du droit de l'Union ou du droit national.

Les déployeurs qui sont des établissements de crédit régis par la directive 2013/36/UE conservent les journaux dans le cadre de la documentation concernant les dispositifs, processus et mécanismes de gouvernance interne conformément à l'article 74 de ladite directive.

5a. Avant de mettre en service ou d'utiliser un système d'IA à haut risque sur le lieu de travail, les déployeurs consultent les représentants des travailleurs en vue de parvenir à un accord conformément à la directive 2002/14/CE et informent les employés concernés qu'ils seront soumis à la système.

5b. Les déployeurs de systèmes d'IA à haut risque qui sont des autorités publiques ou des institutions, organes, offices et agences ou entreprises de l'Union visés à l'article 51, paragraphe 1 bis, point b), se conforment aux obligations d'enregistrement visées à l'article 51.

6. Le cas échéant, les déployeurs de systèmes d'IA à haut risque utilisent les informations fournies en vertu de l'article 13 pour se conformer à leur obligation d'effectuer une analyse d'impact sur la protection des données en vertu de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive (UE) 2016/680, dont un résumé sera publié, eu égard à l'utilisation spécifique et au contexte spécifique dans lequel le système d'IA est destiné à fonctionner. Les déployeurs peuvent recourir en partie à ces analyses d'impact sur la protection des données pour remplir certaines des obligations énoncées dans le présent article, dans la mesure où l'analyse d'impact sur la protection des données remplit ces obligations.

6a. Sans préjudice de l'article 52, les déployeurs de systèmes d'IA à haut risque visés à l'annexe III, qui prennent des décisions ou aident à prendre des décisions concernant des personnes physiques, informent les personnes physiques qu'elles sont soumises à l'utilisation du système d'IA à haut risque . Ces informations doivent inclure l'objectif visé et le type de décisions prises. Le déployant informe également la personne physique de son droit à une explication visée à l'article 68 quater.

6c. Les déployeurs coopèrent avec les autorités nationales compétentes concernées sur toute action que ces autorités prennent en relation avec le système à haut risque afin de mettre en œuvre le présent règlement.

Article 29 bis

Évaluation de l'impact sur les droits fondamentaux des systèmes d'IA à haut risque

1. Avant de mettre en service un système d'IA à haut risque tel que défini à l'article 6, paragraphe 2, à l'exception des systèmes d'IA destinés à être utilisés dans le domaine 2 de l'annexe III, les déployeurs procèdent à une évaluation de l'impact des systèmes dans le domaine spécifique contexte d'utilisation. Cette évaluation comprendra, au minimum, les éléments suivants :

(un) un aperçu clair de l'objectif pour lequel le système sera utilisé ;

(b) un aperçu clair de la portée géographique et temporelle prévue de l'utilisation du système ; les

(c) catégories de personnes physiques et les groupes susceptibles d'être affectés par l'utilisation du système ;

(d) la vérification que l'utilisation du système est conforme au droit de l'Union et au droit national applicables en matière de droits

(C'est) fondamentaux ; l'impact raisonnablement prévisible sur les droits fondamentaux de la mise en service du système d'IA à haut risque ;

(F) les risques spécifiques de préjudice susceptibles d'affecter les personnes marginalisées ou les groupes

(g) vulnérables ; l'impact négatif raisonnablement prévisible de l'utilisation du système sur l'environnement ; −

(h) un plan détaillé indiquant comment les dommages et l'impact négatif sur les droits fondamentaux identifiés seront atténués.

(j) le système de gouvernance que le déployeur mettra en place, y compris la surveillance humaine, le traitement des plaintes et les recours.

2. Si un plan détaillé d'atténuation des risques décrits au cours de l'évaluation décrite au paragraphe 1 ne peut être identifié, le déployeur s'abstient d'utiliser le système d'IA à haut risque et informe le fournisseur et l'autorité de contrôle nationale sans retard injustifié. Les autorités nationales de surveillance, conformément aux articles 65 et 67, tiennent compte de ces informations lorsqu'elles enquêtent sur des systèmes qui présentent un risque au niveau national.

3. L'obligation visée 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 une évaluation d'impact sur les droits fondamentaux effectuée précédemment ou sur une évaluation existante effectuée par des fournisseurs. Si, lors de l'utilisation du système d'IA à haut risque, le déployeur estime que les critères énumérés au paragraphe 1 ne sont plus remplis, il procède à une nouvelle analyse d'impact sur les droits fondamentaux.

4. Au cours de l'analyse d'impact, le déployeur, à l'exception des PME, informe l'autorité de contrôle nationale et les parties prenantes concernées et associe, dans la mesure du possible, des représentants des personnes ou des groupes de personnes susceptibles d'être affectés par le système d'IA à haut risque, tel qu'identifié au paragraphe 1, y compris, mais sans s'y limiter: les organismes de promotion de l'égalité, les agences de protection des consommateurs, les partenaires sociaux et les agences de protection des données, en vue de recevoir des contributions à l'analyse d'impact. Le déployeur doit prévoir un délai de six semaines pour que les organismes répondent.
Les PME peuvent appliquer volontairement les dispositions prévues au présent paragraphe.

Dans le cas visé à l'article 47, paragraphe 1, les autorités publiques peuvent être exemptées de ces obligations.

5. Le déployeur qui est une autorité publique ou une entreprise visée à l'article 51, paragraphe 1 bis, point b), publie un résumé des résultats de l'analyse d'impact dans le cadre de l'enregistrement de l'utilisation conformément à son obligation au titre de l'article 51, paragraphe 2.

6. Lorsque le déployeur est déjà tenu d'effectuer une analyse d'impact sur la protection des données en vertu de l'article 35 du règlement (UE) 2016/679 ou de l'article 27 de la directive

(UE) 2016/680, l'analyse d'impact sur les droits fondamentaux visée au paragraphe 1 est menée conjointement avec l'analyse d'impact sur la protection des données. L'analyse d'impact relative à la protection des données est publiée sous forme d'addendum.

(71) L'intelligence artificielle est une famille de technologies en développement rapide qui nécessite une surveillance réglementaire et un espace d'expérimentation sûr et contrôlé, tout en garantissant une innovation responsable et l'intégration de garanties appropriées et de mesures d'atténuation des risques. Afin de garantir un cadre juridique qui favorise l'innovation, est à l'épreuve du temps et résilient aux perturbations, les États membres devraient établir au moins un bac à sable réglementaire d'intelligence artificielle pour faciliter le développement et le test de systèmes d'IA innovants sous une surveillance réglementaire stricte avant que ces systèmes ne soient mis sur le marché. commercialiser ou autrement mis en service. Il est en effet souhaitable que la mise en place de bacs à sable réglementaires, dont la mise en place est actuellement laissée à la discrétion des États membres, soit rendue obligatoire dans une prochaine étape avec des critères établis. Ce bac à sable obligatoire pourrait également être établi conjointement avec un ou plusieurs autres États membres, pour autant que ce bac à sable couvre le niveau national respectif des États membres concernés. Des bacs à sable supplémentaires peuvent également être établis à différents niveaux, y compris entre les États membres, afin de faciliter la coopération et les synergies transfrontalières. À l'exception du bac à sable obligatoire au niveau national, les États membres devraient également pouvoir établir des bacs à sable virtuels ou hybrides. Tous les bacs à sable réglementaires doivent pouvoir accueillir à la fois des produits physiques et virtuels. Les autorités d'établissement devraient également veiller à ce que les bacs à sable réglementaires disposent des ressources financières et humaines adéquates pour leur fonctionnement.

(72) Les objectifs des bacs à sable réglementaires devraient être les suivants : permettre aux autorités d'établissement d'accroître leur compréhension des évolutions techniques, d'améliorer les méthodes de surveillance et de fournir des orientations aux développeurs et aux fournisseurs de systèmes d'IA pour parvenir à la conformité réglementaire avec le présent règlement ou, le cas échéant, avec d'autres réglementations applicables de l'Union ; et la législation des États membres, ainsi qu'avec la Charte des droits fondamentaux ; pour les fournisseurs potentiels de permettre et de faciliter le test et le développement de solutions innovantes liées aux systèmes d'IA dans la phase de pré-commercialisation afin d'améliorer la sécurité juridique, de permettre un apprentissage plus réglementaire en établissant des autorités dans un environnement contrôlé pour développer de meilleures orientations et identifier d'éventuelles améliorations futures du cadre juridique par le biais de la procédure législative ordinaire. Tout risque important identifié lors du développement et des tests de ces systèmes d'IA devrait entraîner une atténuation immédiate et, à défaut, la suspension du processus de développement et de test jusqu'à ce que cette atténuation ait lieu. Afin de garantir une mise en œuvre uniforme dans l'ensemble de l'Union et des économies d'échelle, il convient d'établir des règles communes pour la mise en œuvre des bacs à sable réglementaires et un cadre de coopération entre les autorités compétentes impliquées dans la surveillance des bacs à sable. Les États membres devraient veiller à ce que les bacs à sable réglementaires soient largement disponibles dans toute l'Union, tandis que la participation devrait rester volontaire. Il est particulièrement important de veiller à ce que les PME et les startups puissent facilement accéder à ces bacs à sable, soient activement impliquées et participent au développement et aux tests de systèmes d'IA innovants, afin de pouvoir apporter leur savoir-faire et leur expérience.

(72 bis) Le présent règlement devrait fournir la base juridique de l'utilisation des données à caractère personnel collectées à d'autres fins pour développer certains systèmes d'IA dans l'intérêt public au sein de la Bac à sable réglementaire de l'IA uniquement dans des conditions spécifiées conformément à l'article 6, paragraphe 4, de

Règlement (UE) 2016/679 et article 6 du règlement (UE) 2018/1725, et sans préjudice de l'article 4, paragraphe 2, de la directive (UE) 2016/680. Les fournisseurs potentiels dans le bac à sable devraient assurer des garanties appropriées et coopérer avec les autorités compétentes, notamment en suivant leurs conseils et en agissant rapidement et de bonne foi pour atténuer tout risque élevé pour la sécurité, la santé et l'environnement et les droits fondamentaux qui pourraient survenir au cours du développement. et l'expérimentation dans le bac à sable. Le comportement des fournisseurs potentiels dans le bac à sable devrait être pris en compte lorsque les autorités compétentes décident de suspendre temporairement ou définitivement leur participation au bac à sable ou d'infliger une amende administrative en vertu de l'article 83, paragraphe 2, du règlement 2016/679 et de l'article 57. de la directive 2016/680.

(72 ter) Pour garantir que l'intelligence artificielle aboutisse à des résultats bénéfiques sur le plan social et environnemental, les États membres devraient soutenir et promouvoir la recherche et le développement de l'IA à l'appui de résultats bénéfiques sur le plan social et environnemental en allouant des ressources suffisantes, y compris des financements publics et de l'Union, et en accordant un accès prioritaire aux bacs à sable réglementaires aux projets menés par la société civile. De tels projets devraient être basés sur le principe d'une coopération interdisciplinaire entre les développeurs d'IA, des experts en matière d'inégalité et de non-discrimination, d'accessibilité, de droits des consommateurs, environnementaux et numériques, ainsi que des universitaires.

TITRE V

MESURES EN FAVEUR DE L'INNOVATION

Article 53

Bacs à sable réglementaires de l'IA

1. Les États membres établissent au moins un bac à sable réglementaire de l'IA au niveau national, qui est opérationnel au plus tard le jour de l'entrée en application du présent règlement. Ce bac à sable peut également être établi conjointement avec un ou plusieurs autres États membres.

1a. Des bacs à sable réglementaires supplémentaires en matière d'IA aux niveaux régional ou local ou conjointement avec d'autres États membres peuvent également être créés.

1b. La Commission et le Contrôleur européen de la protection des données, seuls, conjointement ou en collaboration avec un ou plusieurs États membres, peuvent également établir des bacs à sable réglementaires en matière d'IA au niveau de l'Union.

1c. Les autorités d'établissement allouent des ressources suffisantes pour se conformer efficacement et en temps utile au présent article.

1d. Les bacs à sable réglementaires de l'IA prévoient, conformément aux critères énoncés à l'article 53 bis, un environnement contrôlé qui favorise l'innovation et facilite le développement, 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 à un plan spécifique convenu entre les prestataires potentiels et l'autorité d'établissement.

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

a) aux autorités compétentes de fournir des orientations aux fournisseurs potentiels de systèmes d'IA pour se conformer à la réglementation avec le présent règlement ou, le cas échéant, avec d'autres législations applicables de l'Union et des États membres
b) pour les fournisseurs potentiels afin de permettre et de faciliter le test et le développement de solutions innovantes liées aux systèmes d'IA c)
l'apprentissage réglementaire dans un environnement contrôlé

1e. Les autorités d'établissement fournissent des orientations et une supervision au sein du bac à sable en vue d'identifier les risques, en particulier pour les droits fondamentaux, la démocratie et l'état de droit, la santé et la sécurité et l'environnement, testent et démontrent les mesures d'atténuation des risques identifiés, ainsi que leur efficacité et garantissent le respect des exigences du présent règlement et, le cas échéant, d'autres législations de l'Union et des États membres.

1f. Les autorités d'établissement fournissent aux fournisseurs potentiels bac à sable qui développent des systèmes d'IA à haut risque des orientations et une supervision sur la manière de satisfaire aux exigences énoncées dans le présent règlement, de sorte que les systèmes d'IA puissent sortir du bac à sable en présumant qu'ils sont conformes aux exigences spécifiques du présent règlement. qui ont été évalués dans le bac à sable. Dans la mesure où le système d'IA respecte les exigences en sortie du bac à sable, il est présumé conforme au présent règlement. À cet égard, les rapports de sortie établis par l'autorité d'établissement sont pris en compte par les autorités de surveillance du marché ou les organismes notifiés, selon le cas, dans le cadre des procédures d'évaluation de la conformité ou des contrôles de surveillance du marché.

2. Les autorités d'établissement veillent à ce que, dans la mesure où les systèmes d'IA innovants impliquent le traitement de données à caractère personnel ou relèvent de la compétence de surveillance d'autres autorités nationales ou autorités compétentes fournissant ou soutenant l'accès aux données à caractère personnel, les autorités nationales de protection des données, ou dans les cas visés au paragraphe 1 ter, le CEPD et ces autres autorités nationales sont associés au fonctionnement du bac à sable réglementaire de l'IA et participent à la surveillance de ces aspects dans toute la mesure de leurs tâches et pouvoirs respectifs.

3. Les bacs à sable réglementaires de l'IA n'affectent pas les pouvoirs de surveillance et de correction des autorités compétentes, y compris au niveau régional ou local. Tout risque significatif pour les droits fondamentaux, la démocratie et l'état de droit, la santé et la sécurité ou l'environnement identifié lors du développement et des tests de ces systèmes d'IA doit entraîner une atténuation immédiate et adéquate. Les autorités compétentes doivent avoir le pouvoir de suspendre temporairement ou définitivement le processus de test ou la participation au bac à sable si aucune atténuation efficace n'est possible et d'informer le bureau AI de cette décision.

4. Les fournisseurs potentiels du bac à sable réglementaire de l'IA restent responsables, en vertu de la législation applicable en matière de responsabilité de l'Union et des États membres, de tout préjudice infligé à des tiers du fait de l'expérimentation qui se déroule dans le bac à sable. Toutefois, à condition que le ou les prestataires potentiels respectent le plan spécifique visé au paragraphe 1 quater et les conditions de leur participation et suivent de bonne foi les orientations données par les autorités d'établissement, aucune amende administrative ne sera infligée par les autorités pour infractions au présent règlement.

5. Les autorités d'établissement coordonnent leurs activités et coopèrent dans le cadre de l'office AI.

5a. Les autorités chargées de l'établissement informent le bureau AI de la création d'un bac à sable et peuvent demander de l'aide et des conseils. Une liste des bacs à sable prévus et existants doit être rendue publique par le bureau de l'IA et tenue à jour afin d'encourager une plus grande interaction dans les bacs à sable réglementaires et la coopération transnationale.

5b. Les autorités d'établissement soumettent au bureau AI et, à moins que la Commission ne soit la seule autorité d'établissement, à la Commission, des rapports annuels, commençant un an après l'établissement du bac à sable, puis chaque année jusqu'à sa clôture, ainsi qu'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 meilleures pratiques, les incidents, les enseignements tirés et les recommandations sur leur mise en place et, le cas échéant, sur l'application et la révision éventuelle du présent règlement et d'autres actes législatifs de l'Union faisant l'objet d'une surveillance au sein de le bac à sable Ces rapports annuels ou leurs résumés sont mis à la disposition du public en ligne.

6. La Commission met en place une interface unique et dédiée contenant toutes les informations pertinentes relatives aux bacs à sable, ainsi qu'un point de contact unique au niveau de l'UE pour interagir avec les bacs à sable réglementaires et permettre aux parties prenantes de poser des questions aux autorités compétentes et de solliciter des informations non pertinentes. des orientations contraignantes sur la conformité des produits, services et modèles commerciaux innovants intégrant des technologies d'IA. La Commission assure une coordination proactive avec les autorités nationales, régionales et locales, le cas échéant.

6a. Aux fins des paragraphes 1 et 1 bis, la Commission joue un rôle complémentaire, permettant aux États membres de tirer parti de leur expertise et, d'autre part, d'aider et de fournir une compréhension technique et des ressources aux États membres qui demandent des conseils sur l'ensemble- mise en place et fonctionnement de ces bacs à sable réglementaires.

Article 53 bis

Modalités et fonctionnement des bacs à sable réglementaires de l'IA

1. Afin d'éviter une fragmentation dans l'ensemble de l'Union, la Commission, en consultation avec l'office de l'IA, adopte un acte délégué détaillant les modalités d'établissement, de développement, de mise en œuvre, de fonctionnement et de supervision des bacs à sable réglementaires de l'IA, y compris les critères d'éligibilité et la procédure pour la candidature, la sélection, la participation et la sortie du bac à sable, ainsi que les droits et obligations des participants, sur la base des dispositions énoncées dans le présent article

2. La Commission est habilitée à adopter des actes délégués conformément à la procédure visée à l'article 73 au plus tard 12 mois après l'entrée en vigueur du présent règlement et veille à ce que:

a) les bacs à sable réglementaires sont ouverts à tout fournisseur potentiel candidat d'un système d'IA qui remplit les critères d'éligibilité et de sélection. Les critères d'accès au bac à sable réglementaire doivent être transparents et équitables.
Les autorités d'établissement informent les demandeurs de leur décision dans les 3 mois suivant la demande;

b) les bacs à sable réglementaires permettent un accès large et égal et suivent demande de participation;

c) l'accès aux bacs à sable réglementaires de l'IA est gratuit pour les PME et les start-up sans préjudice des coûts exceptionnels que les autorités peuvent récupérer de manière équitable et proportionnée ;

d) les bacs à sable réglementaires facilitent l'implication d'autres acteurs pertinents au sein de l'écosystème de l'IA, tels que les organismes notifiés et les organismes de normalisation (PME, start-ups, entreprises, innovateurs, installations de test et d'expérimentation, laboratoires de recherche et d'expérimentation et pôles d'innovation numérique, centres de l'excellence, les chercheurs individuels, afin de permettre et de faciliter la coopération avec le secteur public et privé ;

e) ils permettent aux fournisseurs potentiels de remplir, dans un environnement contrôlé, les obligations d'évaluation de la conformité du présent règlement ou l'application volontaire des codes de conduite visés à l'article 69 ;

f) les procédures, processus et exigences administratives pour la candidature, la sélection, la participation et la sortie du bac à sable sont simples, facilement intelligibles, clairement communiqués afin de faciliter la participation des
PME et start-up aux capacités juridiques et administratives limitées et rationalisées dans l'ensemble de l'Union, afin d'éviter la fragmentation et que la participation à un bac à sable réglementaire établi par un État membre, par le
Commission ou par le CEPD est mutuellement et uniformément reconnu et produit les mêmes effets juridiques dans toute l'Union;

g) la participation au bac à sable réglementaire de l'IA est limitée à une période adapté à la complexité et à l'ampleur du projet ;

h) les bacs à sable facilitent le développement d'outils et d'infrastructures pour tester, comparer, évaluer et expliquer les dimensions des systèmes d'IA pertinentes pour les bacs à sable, telles que la précision, la robustesse et la cybersécurité, ainsi que la minimisation des risques pour les droits fondamentaux, l'environnement et la société à grand.

3. Les fournisseurs potentiels dans les bacs à sable, en particulier les PME et les start-ups, bénéficient d'un accès facilité aux services de pré-déploiement tels que des conseils sur la mise en œuvre du présent règlement, à d'autres services à valeur ajoutée tels que l'aide pour les documents de normalisation et la certification et consultation, et à d'autres initiatives du marché unique numérique telles que les installations de test et d'expérimentation, les hubs numériques, les centres d'excellence et les capacités d'analyse comparative de l'UE.

Article 54

Traitement ultérieur des données personnelles pour développer certains systèmes d'IA dans l'intérêt public dans le bac à sable réglementaire de l'IA

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

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

la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la sauvegarde

~~contre et la prévention des menaces à la sécurité publique, sous le contrôle et la responsabilité des autorités compétentes. Le traitement est fondé sur le droit de l'État membre ou de l'Union ;~~

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

(iii) un niveau élevé de protection et d'amélioration de la qualité de l'environnement, de protection de la biodiversité, des pollutions ainsi que d'atténuation et d'adaptation au changement climatique ;

(iii bis) la sécurité et la résilience des systèmes de transport, des infrastructures critiques et réseaux.

b) les données traitées sont nécessaires pour se conformer à une ou plusieurs des exigences visées au titre III, chapitre 2, lorsque ces exigences ne peuvent être effectivement remplies par le traitement de données anonymisées, synthétiques ou d'autres données non personnelles;

c) il existe des mécanismes de surveillance efficaces pour identifier s'il existe des risques élevés pour ~~les libertés et d~~roits fondamentaux des personnes concernées, comme indiqué à l'article 35 du règlement (UE) 2016/679 et à l'article 35 du règlement (UE) 2018/ 1725 peuvent survenir pendant l'expérimentation du bac à sable ainsi qu'un mécanisme de réponse pour atténuer rapidement ces risques et, si nécessaire, arrêter le traitement ;

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

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

f) tout traitement de données à caractère personnel dans le cadre du bac à sable n'entraîne pas de mesures ou de décisions affectant les personnes concernées ni n'affecte l'application de leurs droits prévus par le droit de l'Union sur la protection des données à caractère personnel ;

(g) toutes les données personnelles traitées dans le cadre du bac à sable sont protégées au moyen de mesures techniques et organisationnelles appropriées et supprimées une fois la participation au bac à sable terminée ou les données personnelles ont atteint la fin de leur période de conservation ;

(h) les journaux du traitement des données personnelles dans le cadre du bac à sable sont conservés pendant la durée de la participation au bac à sable et 1 an après sa fi~~n, uniquement dans le but et uniquement aussi longtemps que nécessaire pour s'acquitter de la responsabilité et obligations de documentation en vertu du présent article ou d'une autre application de la législation de l'Union ou des États membres ;~~

i) une description complète et détaillée du processus et de la justification de la formation, des tests et de la validation du système d'IA est conservée avec les résultats des tests dans le cadre de la documentation technique à l'annexe IV;

(j) un bref résumé du système d'IA développé dans le bac à sable, ses objectifs, hypothèses et résultats attendus, publié sur le site internet des autorités compétentes.

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

Article 54 bis

Promotion de la recherche et du développement en matière d'IA à l'appui de résultats bénéfiques pour la société et l'environnement

1. Les États membres encouragent la recherche et le développement de solutions d'IA qui favorisent des résultats bénéfiques sur le plan social et environnemental, y compris, mais sans s'y limiter, le développement de solutions basées sur l'IA pour accroître l'accessibilité pour les personnes handicapées, lutter contre les inégalités socio-économiques et atteindre les objectifs de durabilité et d'environnement, par:

a) accorder aux projets concernés un accès prioritaire aux bacs à sable réglementaires de l'IA dans la mesure où ils remplissent les conditions d'éligibilité; (b) allouer des fonds publics, y compris des fonds pertinents de l'UE, à la recherche et au développement en matière d'intelligence artificielle afin d'obtenir des résultats bénéfiques sur le plan social et environnemental ;

(c) organiser des activités spécifiques de sensibilisation à l'application du présent règlement, à la disponibilité et aux procédures de demande de financements dédiés, adaptées aux besoins de ces projets ; d) le cas échéant, établir des canaux dédiés accessibles, y compris au sein des bacs à sable, pour la communication avec les projets afin de fournir des orientations et de répondre aux questions concernant la mise en œuvre du présent règlement.

2. Les États membres aident la société civile et les acteurs sociaux à mener ou à participer à de tels projets.

Articles 8 à 12, annexe IV et considérants 42 à 46 ter CA 5

(42) Afin d'atténuer les risques liés aux systèmes d'IA à haut risque placés ou autrement mis en service sur le marché de l'Union pour les déployeurs et les personnes concernées, certaines exigences obligatoires devraient s'appliquer, compte tenu de la finalité prévue, de l'utilisation abusive raisonnablement prévisible du système et selon le système de gestion des risques à mettre en place par le prestataire. Ces exigences devraient être axées sur des objectifs, adaptées à l'objectif, raisonnables et efficaces, sans ajouter de charges réglementaires ou de coûts indus aux opérateurs.

(43) Des exigences devraient s'appliquer aux systèmes d'IA à haut risque en ce qui concerne la qualité et la pertinence des ensembles de données utilisés, la documentation technique et l'archivage, la transparence et la fourniture d'informations aux déployeurs, la surveillance humaine, ainsi que la robustesse, l'exactitude et la cybersécurité. Ces exigences sont nécessaires pour atténuer efficacement les risques pour la santé, la sécurité et les droits fondamentaux, ainsi que pour l'environnement, la démocratie et l'État de droit, selon qu'ils sont applicables à la lumière de l'objectif visé ou de l'utilisation abusive raisonnablement prévisible du système, et pas moins des mesures commerciales restrictives sont raisonnablement disponibles, évitant ainsi des restrictions injustifiées au commerce.

(44) L'accès à des données de haute qualité joue un rôle essentiel pour structurer et garantir les performances de nombreux systèmes d'IA, en particulier lorsque des techniques impliquant la formation de modèles sont utilisées, en vue de garantir que le système d'IA à haut risque fonctionne aussi bien que intentionnel et en toute sécurité et qu'il ne devienne pas une source de discrimination interdite par le droit de l'Union. Des ensembles de données de formation, de validation et de test de haute qualité nécessitent la mise en œuvre de pratiques appropriées de gouvernance et de gestion des données. Les ensembles de données de formation et, le cas échéant, de validation et de test, y compris les étiquettes, doivent être suffisamment pertinents, représentatifs, dûment contrôlés pour détecter les erreurs et aussi complets que possible compte tenu de l'objectif visé par le système. Ils devraient également avoir les propriétés statistiques appropriées, y compris en ce qui concerne les personnes ou les groupes de personnes vis-à-vis desquels le système d'IA à haut risque est destiné à être utilisé, en accordant une attention particulière à l'atténuation des biais éventuels dans les ensembles de données, qui pourraient conduire à à des risques pour les droits fondamentaux ou à des résultats discriminatoires pour les personnes concernées par le système d'IA à haut risque. Les biais peuvent par exemple être inhérents aux ensembles de données sous-jacents, en particulier lorsque des données historiques sont utilisées, introduites par les développeurs des algorithmes ou générées lorsque les systèmes sont mis en œuvre dans des contextes réels Les résultats fournis par les systèmes d'IA sont influencés par ces biais inhérents qui sont susceptibles d'augmenter progressivement et ainsi de perpétuer et d'amplifier les discriminations existantes, en particulier pour les personnes appartenant à certains groupes vulnérables ou ethniques, ou à des communautés racisées. En particulier, les ensembles de données de formation, de validation et d'essai devraient tenir compte, dans la mesure nécessaire à la lumière de leur destination, des caractéristiques, caractéristiques ou éléments qui sont particuliers au cadre ou au contexte géographique, contextuel, comportemental ou fonctionnel spécifique au sein de lequel le système d'IA est destiné à être utilisé. Afin de protéger le droit d'autrui de la discrimination qui pourrait résulter de la partialité des systèmes d'IA, les fournisseurs devraient, à titre exceptionnel et après application de toutes les conditions applicables prévues par le présent règlement et le règlement (UE) 2016/679, la directive 2016/680 et le règlement (UE) 2018/1725, être en mesure de traiter également des catégories particulières de données personnelles,

comme une question d'intérêt public substantiel, afin d'assurer la détection et la correction des biais négatifs liés aux systèmes d'IA à haut risque. Le biais négatif doit être compris comme un biais qui crée un effet discriminatoire direct ou indirect à l'encontre d'une personne physique. Les exigences liées à la gouvernance des données peuvent être respectées en ayant recours à des tiers qui offrent des services de conformité certifiés, y compris la vérification de la gouvernance des données, l'intégrité des ensembles de données, et les pratiques de formation, de validation et de test des données.

(45) Aux fins du développement et de l'évaluation des systèmes d'IA à haut risque, certains acteurs, tels que les fournisseurs, les organismes notifiés et d'autres entités concernées, telles que les pôles d'innovation numérique, les installations d'expérimentation de test et les chercheurs, devraient pouvoir accéder et utiliser des ensembles de données dans leurs domaines d'activité respectifs qui sont liés au présent règlement. Les espaces européens communs de données établis par la Commission et la facilitation du partage de données entre les entreprises et avec le gouvernement dans l'intérêt public seront déterminants pour fournir un accès fiable, responsable et non discriminatoire à des données de haute qualité pour la formation, la validation et le test 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 la formation d'algorithmes d'intelligence artificielle sur ces ensembles de données, d'une manière préservant la vie privée, sécurisée, opportune, transparente et digne de confiance, et avec une méthode appropriée gouvernance institutionnelle. Les autorités compétentes concernées, y compris celles sectorielles, fournissant ou soutenant l'accès aux données peuvent également soutenir la fourniture de données de haute qualité pour la formation, la validation et le test de

(45 bis) 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 des données et de protection des données dès la conception et par défaut, tels qu'énoncés dans la législation de l'Union sur la protection des données, sont essentiels lorsque le traitement des données comporte des risques importants pour les droits fondamentaux des personnes. Les fournisseurs et les utilisateurs de systèmes d'IA devraient mettre en œuvre des mesures techniques et organisationnelles de pointe afin de protéger ces droits. Ces mesures devraient inclure non seulement l'anonymisation et le cryptage, mais également l'utilisation d'une technologie de plus en plus disponible qui permet d'appliquer des algorithmes aux données et d'obtenir des informations précieuses sans transmission entre les parties ni copie inutile des données brutes ou structurées elles-mêmes.

(46) Il est essentiel de disposer d'informations compréhensibles sur la manière dont les systèmes d'IA à haut risque ont été développés et sur leurs performances tout au long de leur durée de vie pour vérifier le respect des exigences prévues par le présent règlement. 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 aux exigences applicables. Ces informations devraient inclure les caractéristiques générales, les capacités et les limites du système, les algorithmes, les données, les processus de formation, de test et de validation utilisés ainsi que la documentation sur le système de gestion des risques pertinent. La documentation technique doit être tenue à jour de manière appropriée tout au long du cycle de vie du système d'IA. Les systèmes d'IA peuvent avoir un impact environnemental important et une consommation d'énergie élevée au cours de leur cycle de vie. Afin de mieux appréhender l'impact des systèmes d'IA sur l'environnement, la documentation technique rédigée par les prestataires doit inclure des informations sur la consommation énergétique du système d'IA, y compris la consommation lors du développement et la consommation attendue lors de l'utilisation. Ces informations devraient tenir compte de la législation de l'Union et de la législation nationale applicables.
Ces informations communiquées doivent être compréhensibles, comparables et vérifiables et

à cette fin, la Commission devrait élaborer des lignes directrices sur une méthodologie harmonisée pour le calcul et la communication de ces informations. Afin de garantir qu'une documentation unique est possible, les termes et définitions liés à la documentation requise et à toute documentation requise dans la législation pertinente de l'Union devraient être alignés autant que possible. (46 bis) Les systèmes d'IA devraient

tenir compte des méthodes les plus récentes et des normes pertinentes applicables pour réduire la consommation d'énergie, l'utilisation des ressources et les déchets, ainsi que pour accroître leur efficacité énergétique et l'efficacité globale du système. Les aspects environnementaux des systèmes d'IA qui sont importants aux fins du présent règlement sont la consommation d'énergie du système d'IA pendant la phase de développement, de formation et de déploiement ainsi que l'enregistrement, la communication et le stockage de ces données. La conception des systèmes d'IA doit permettre de mesurer et d'enregistrer la consommation d'énergie et de ressources à chaque étape du développement, de la formation et du déploiement. La surveillance et la déclaration des émissions des systèmes d'IA doivent être robustes, transparentes, cohérentes et précises. Afin de garantir l'application uniforme du présent règlement et un écosystème juridique stable pour les fournisseurs et les déployeurs dans le marché unique, la Commission devrait élaborer une spécification commune pour la méthodologie permettant de satisfaire à l'exigence de déclaration et de documentation sur la consommation d'énergie et de ressources pendant le développement, formation et déploiement. De telles spécifications communes sur la méthodologie de mesure peuvent développer une base sur laquelle la Commission peut mieux décider si de futures interventions réglementaires sont nécessaires, après avoir mené une analyse d'impact qui tient compte de la législation existante ; (46 ter) Afin d'atteindre les objectifs du présent

règlement et de contribuer aux objectifs environnementaux de l'UE tout en garantissant le bon fonctionnement du marché intérieur, il peut être nécessaire d'établir des recommandations et des lignes directrices et, éventuellement, des objectifs de durabilité. À cette fin, la Commission est habilitée à développer une méthodologie pour contribuer à disposer d'indicateurs de performance clés (KPI) et d'une référence pour les objectifs de développement durable (ODD). L'objectif devrait être en premier lieu de permettre une comparaison équitable entre les choix de mise en œuvre de l'IA en incitant à promouvoir l'utilisation de technologies d'IA plus efficaces répondant aux préoccupations en matière d'énergie et de ressources. Pour atteindre cet objectif, le présent règlement devrait fournir les moyens d'établir une collecte de référence des données communiquées sur les émissions résultant du développement et de la formation et du déploiement.

EXIGENCES POUR LES SYSTÈMES D'IA À HAUT RISQUE

Article 8
Conformité aux exigences

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

1a. Pour se conformer à l'exigence établie dans le présent chapitre, il est dûment tenu compte des lignes directrices élaborées conformément à l'article 82 ter, de l'état de la technique généralement reconnu, y compris tel qu'il ressort des normes harmonisées pertinentes et des spécifications communes visées aux articles 40 et 41 ou ceux déjà prévus dans la législation d'harmonisation syndicale.

2. La finalité du système d'IA à haut risque, les utilisations abusives raisonnablement prévisibles et le système de gestion des risques visés à l'article 9 sont pris en compte pour garantir le respect de ces exigences.

2a. Tant que les exigences du titre III, chapitres 2 et 3 ou du titre VIII, chapitres 1, 2 et 3 pour les systèmes d'IA à haut risque sont traitées par la législation d'harmonisation de l'Union énumérée à l'annexe II, section A, les exigences ou obligations de ces chapitres du présent règlement sont réputées remplies, pour autant qu'elles incluent la composante IA. Les exigences des chapitres 2 et 3 du titre III ou du titre VIII, chapitres 1, 2 et 3 pour les systèmes d'IA à haut risque non couverts par la législation d'harmonisation de l'Union énumérée à l'annexe II, section A, sont intégrées dans ladite législation d'harmonisation de l'Union, le cas échéant. L'évaluation de la conformité pertinente est effectuée dans le cadre des procédures prévues par la législation d'harmonisation de l'Union énumérées à l'annexe II, section A.

Article 9

Système de gestion des risques

1. Un système de gestion des risques est établi, mis en œuvre, documenté et maintenu en relation avec les systèmes d'IA à haut risque, tout au long du cycle de vie du système d'IA. Le système de gestion des risques peut être intégré ou faire partie de procédures de gestion des risques déjà existantes relatives à la législation sectorielle pertinente de l'Union dans la mesure où il satisfait aux exigences du présent article.

2. Le système de gestion des risques consiste en un processus itératif continu exécuté tout au long du cycle de vie d'un système d'IA à haut risque, nécessitant un examen et une mise à jour réguliers du processus de gestion des risques, pour garantir son efficacité continue, et la documentation de toutes les décisions et mesures importantes prises. sous réserve du présent article.
Il comprendra les étapes suivantes :

(un) identification, estimation et évaluation des risques connus et raisonnablement prévisibles que le système d'IA à haut risque peut présenter pour la santé ou la sécurité des personnes physiques, leurs droits fondamentaux, y compris l'égalité d'accès et des chances, la démocratie et l'état de droit ou l'environnement lorsque le système d'IA à haut risque est utilisé conformément à sa destination et dans des conditions d'utilisation abusive raisonnablement prévisible.

~~(b) l'estimation et l'évaluation des risques qui peuvent survenir lorsque le système d'IA à haut risque est utilisé conformément à son objectif prévu et dans des conditions de mauvaise utilisation raisonnablement prévisible ;~~

(c) évaluation des risques significatifs émergents tels que décrits au paragraphe 2, point a), et identifiés sur la base de l'analyse des données recueillies à partir du système de surveillance après commercialisation visé à l'article 61;

(d) l'adoption de mesures de gestion des risques appropriées et ciblées destinées à faire face aux risques identifiés conformément aux lettres a et b du présent paragraphe conformément aux dispositions des paragraphes suivants.

3. Les mesures de gestion des risques visées au paragraphe 2, point c) , tiennent dûment compte des effets et des interactions possibles résultant de l'application combinée des exigences énoncées dans le présent chapitre 2, en vue d'atténuer efficacement les risques tout en garantissant une et la mise en œuvre proportionnée des exigences. Elles tiennent compte de l'état de la technique généralement reconnu, y compris tel qu'il ressort des normes harmonisées ~~ou des spécifications communes pertinentes.~~

4. Les mesures de gestion des risques visées au paragraphe 2, point c), sont telles que le risque résiduel pertinent associé à chaque danger ainsi que le risque résiduel global des systèmes d'IA à haut risque sont raisonnablement jugés acceptables, à condition que le niveau élevé le système d'IA à risque est utilisé conformément à sa destination ou dans des conditions d'utilisation abusive raisonnablement prévisible. Ces risques résiduels et les jugements motivés émis sont communiqués au déployeur.

Lors de l'identification des mesures de gestion des risques les plus appropriées, les éléments suivants doivent être assurés :

(un) l'élimination ou la réduction des risques identifiés dans la mesure où cela est techniquement possible grâce à une conception et un développement adéquats du système d'IA à haut risque, impliquant, le cas échéant, des experts et des parties prenantes

(b) externes ; le cas échéant, la mise en œuvre de mesures d'atténuation et de contrôle adéquates traitant des risques importants qui ne peuvent être éliminés ; fourniture

(c) des informations requises en vertu de l'article 13, notamment en ce qui concerne les risques ~~visés au paragraphe 2, point b), du présent article et, le cas échéant, formation des déployeurs~~.

Lors de l'élimination ou de la réduction des risques liés à l'utilisation du système d'IA à haut risque, les fournisseurs doivent tenir dûment compte d~~es connaissances tec~~hniques, de l'expérience, de l'éducation et de la formation dont le déployeur pe~~ut avoir besoin, y comp~~ris en ce qui concerne le contexte d'utilisation présumé dans le~~q~~uel le système est destiné à être utili~~sé.~~

5. Les systèmes d'IA à haut risque doivent être testés afin d'identifier les mesures de gestion des risques les plus appropriées et les plus ciblées et de soupeser ces mesures par rapport aux avantages potentiels et aux objectifs visés du système. Les tests garantissent que les systèmes d'IA à haut risque fo~~n~~ctionnent de manière cohérente pour l'usage auquel ils sont destinés et qu'ils sont conformes aux exigences énoncées dans le présent chapitre.

6. Les procé~~d~~ures de test doivent être adaptées pour atteindre l'objectif visé du système d'IA et n'ont pas besoin ~~d'aller au-delà de ce qui est nécessaire pour atteindre cet objectif.~~

7. Les tests des systèmes d'IA à haut risque doivent être effectués, le cas échéa~~nt, à tout moment du processus de développement et, en tout état de cause, avant la mise sur le marché ou la mise en~~ service. Les tests doivent être effectués par rapport à des mesures préalablement définies et à des seuils probabilistes adaptés à l'objectif visé ou à l'utilisation abusive raisonnablement prévisible du système d'IA à haut risque.

8. Lors de la mise en œuvre du système de gestion des risques décrit aux paragraphes 1 à 7, les prestataires accordent une attention particulière à la question de savoir si le systè~~me d'IA à haut ris~~que est susceptible d'avoir un impact négatif sur les groupes vulnérables de personnes ou d'enfants.

9. Pour les prestataires et les systèmes d'IA déjà couverts par le droit de l'Union qui les obligent à mettre en place une gestion des risques spécifique, y compris les établissements de crédit régis par la directive 2013/36/UE, les aspects décrits aux paragraphes 1 à 8 font partie ou sont combinés avec la gestion des risques. procédures établies par ces actes du droit de l'Union.

–

Article 10

Données et gouvernance des données

1. Les systèmes d'IA à haut risque qui utilisent des techniques impliquant la formation de modèles avec des données sont développés sur la base d'ensembles de données de formation, de validation et de test qui répondent aux critères de qualité visés aux paragraphes 2 à 5, dans la mesure où cela est techniquement faisable. selon le segment de marché spécifique ou le champ d'application.

Les techniques qui ne nécessitent pas de données d'entrée étiquetées, telles que l'apprentissage non supervisé et l'apprentissage par renforcement, sont développées sur la base d'ensembles de données, par exemple pour les tests et la vérification, qui répondent aux critères de qualité visés aux paragraphes 2 à 5.

2. Les ensembles de données de formation, de validation et de test doivent être soumis ~~à u~~ne gouvernance des données adaptée à l'objectif prévu du système d'IA. Ces pratiques concernent notamment,

a) les choix de conception pertinents ;

(a bis) transparence en ce qui concerne l'objectif initial de la collecte de données; (b)

processus de 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 ~~pertinentes~~, 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 la pertinence des ensembles de données qui sont nécessaire;

f) examen en vue d'éventuels biais susceptibles d'affecter la santé et la sécurité des personnes, d'avoir une incidence négative sur les droits fondamentaux ou de conduire à une discrimination interdite par le droit de l'Union, en particulier lorsque les sorties de données influencent les entrées pour les opérations futures («boucles de rétroaction») et

(f bis) des mesures appropriées pour détecter, prévenir et atténuer d'éventuels biais; g)

l'identification des lacunes ou lacunes pertinentes en matière de données qui empêchent le respect du présent règlement, et la manière dont ces lacunes et lacunes peuvent être traitées.

3. Les ensembles de données de formation et, le cas échéant, les ensembles de données de validation et de test, y compris les étiquettes, doivent être pertinents, suffisamment représentatifs, correctement contrôlés pour détecter les erreurs et être aussi complets que possible compte tenu de l'objectif visé. Ils doivent avoir les propriétés statistiques appropriées, y compris, le cas échéant, en ce qui concerne les personnes

ou des groupes de personnes vis-à-vis desquels le système d'IA à haut risque est destiné à être utilisé. Ces caractéristiques des ensembles de données doivent être respectées au niveau des ensembles de données individuels ou d'une combinaison de ceux-ci.

4. ~~Formation, validation et test d~~Les ensembles de données doivent tenir compte, dans la mesure requise par l'objectif visé ou les utilisations abusives raisonnablement prévisibles du système d'IA, des caractéristiques ou des éléments qui sont particuliers 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 d'assurer la détection et la correction des biais négatifs en rapport avec les systèmes d'IA à haut risque, les fournisseurs de ces systèmes peuvent exceptionnellement traiter des catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, du Règlement (UE) 2016/679, article 10 de la directive (UE) 2016/680 et article 10, paragraphe 1, du règlement (UE) 2018/1725, sous réserve de garanties appropriées pour les libertés et droits fondamentaux des personnes physiques, y compris des limitations techniques sur la réutilisation et l'utilisation des technologies de pointe en matière de sécurité et de protection de la vie privée. En particulier, toutes les conditions suivantes s'appliquent pour que ce traitement ait lieu :

(a) la détection et la correction des biais ne peuvent pas être efficacement réalisées par le traitement de données synthétiques ou anonymisées ;
(b) les données sont pseudonymisées ; (c) le
fournisseur prend les mesures techniques et organisationnelles appropriées pour garantir que les données traitées aux fins du présent paragraphe sont sécurisées, protégées, soumises à des garanties appropriées et que seules les personnes autorisées ont accès à ces données avec des obligations de confidentialité appropriées ; (d) les données traitées aux fins du présent paragraphe
ne doivent pas être transmises,
transférés ou autrement consultés par d'autres parties ;
(e) les données traitées aux fins du présent paragraphe sont protégées au moyen de mesures techniques et organisationnelles appropriées et supprimées une fois que le biais a été corrigé ou que les données personnelles ont atteint la fin de leur période de conservation ;

f) des mesures efficaces et appropriées sont en place pour garantir la disponibilité, la sécurité et la résilience des systèmes et services de traitement contre les incidents techniques ou physiques ;

g) des mesures efficaces et appropriées sont en place pour assurer la sécurité physique des lieux où les données sont stockées et traitées, la gouvernance et la gestion internes de l'informatique et de la sécurité informatique, la certification des processus et des produits ;

Les prestataires ayant recours à cette disposition doivent établir une documentation expliquant pourquoi le traitement de catégories particulières de données à caractère personnel était nécessaire pour détecter et corriger les préjugés.

6. Des pratiques appropriées de gouvernance et de gestion des données s'appliquent au développement de systèmes d'IA à haut risque autres que ceux qui utilisent des techniques impliquant la formation de modèles afin de garantir que ces systèmes d'IA à haut risque sont conformes au paragraphe 2.

6a. Lorsque le fournisseur ne peut pas respecter les obligations prévues au présent article parce qu'il n'a pas accès aux données et que les données sont détenues exclusivement par le

déployeur, celui-ci peut, sur la base d'un contrat, être rendu responsable de toute infraction au présent article.

Article 11

Documentation technique

1. La documentation technique d'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 est conforme aux exigences énoncées dans le présent chapitre et fournit aux autorités de contrôle nationales et aux organismes notifiés toutes les informations nécessaires pour évaluer la conformité du système d'IA. avec ces exigences. Il contient, au minimum, les éléments visés à l'annexe IV ou, dans le cas des PME et des start-up, tout document équivalent répondant aux mêmes objectifs, sous réserve de l'approbation de l'autorité nationale compétente.

2. Lorsqu'un système d'IA à haut risque lié à un produit, auquel s'appliquent les actes juridiques énumérés à l'annexe II, section A, est mis sur le marché ou mis en service, une seule documentation technique est établie contenant toutes les informations énoncées à l'article paragraphe 1 ainsi que les informations requises en vertu de ces actes juridiques.

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

3a. Les prestataires qui sont des établissements de crédit régis par la directive 2013/36/UE conservent la documentation technique dans le cadre de la documentation concernant la gouvernance interne, les dispositifs, les processus et les mécanismes conformément à l'article 74 de ladite directive.

Article 12

Tenue de registres

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

2. Afin d'assurer un niveau de traçabilité du fonctionnement du système d'IA tout au long de sa durée de vie qui soit adapté à l'objectif visé par le système, les capacités de journalisation facilitent le suivi des opérations visées à l'article 29, paragraphe 4, ainsi que la la surveillance après commercialisation visée à l' article 61 . En particulier, ils doivent permettre l'enregistrement d'événements pertinents pour l'identification de situations pouvant :

a) fait en sorte que le système d'IA présente un risque au sens de l'article 65, paragraphe 1; ou (b) entraîner une modification substantielle du système d'IA ;

2a Les systèmes d'IA à haut risque doivent être conçus et développés avec des capacités de journalisation permettant l'enregistrement de la consommation d'énergie, la mesure ou le calcul de l'utilisation des ressources et de l'impact environnemental du système d'IA à haut risque pendant toutes les phases du cycle de vie du système.

3. ~~En particulier, les capacités de journalisation permettent de surveiller le fonctionnement du système d'IA à haut risque en ce qui concerne la survenance de situations susceptibles de faire en sorte que le système d'IA présente un risque au sens de l'article 65, paragraphe 1, ou d'entraîner une modification et faciliter la surveillance après commercialisation visée à l'article 61.~~

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

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

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

(c) les données d'entrée pour lesquelles la recherche a conduit à une

correspondance ; d) l'identification des personnes physiques impliquées dans la vérification des résultats, visée à l'article 14, paragraphe 5.

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 suivantes, applicables au système d'IA concerné:

1. Une description générale du système d'IA comprenant :

(un) sa destination, le nom du fournisseur et la version du système reflétant sa relation avec les versions précédentes et, le cas échéant, plus récentes, dans la succession des révisions ;

(a bis) la nature des données susceptibles ou destinées à être traitées par le système et, dans le cas de données à caractère personnel, les catégories de personnes physiques et de groupes susceptibles ou destinés à être affectés

(b) comment le système d'IA peut interagir ou peut être utilisé pour interagir avec du matériel ou des logiciels, y compris 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 micrologiciels concernés et, le cas échéant, des informations pour le déployeur sur toute exigence liée à la mise à jour de la version ;

d) la description des différentes configurations et variantes du système d'IA qui sont destinées à être mises sur le marché ou mises en service ;

(e) la description du matériel sur lequel le système d'IA est censé fonctionner ; (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 ;

(f bis) la description de l'interface du déployeur; g) les

instructions d'utilisation du déployeur conformément à l'article 13, paragraphes 2 et 3, ainsi qu'à l'article 14, paragraphe 4, point e), et, le cas échéant, les instructions d'installation;

(ga) une description détaillée et facilement intelligible de l'optimisation principale du système but ou buts

(gb) une description détaillée et facilement intelligible de la sortie attendue du système et de la qualité de sortie attendue

(gc) des instructions détaillées et facilement compréhensibles pour interpréter les sortir

(gd) exemples de scénarios pour lesquels le système ne doit pas être utilisé

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

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 préformés fournis par des tiers et la manière dont ceux-ci ont été utilisés, intégrés ou modifiés par le fournisseur;

(b) une description de l'architecture, des spécifications de conception, des algorithmes et des structures de données, y compris une décomposition de ses composants et interfaces, de la manière dont ils sont liés les uns aux autres et de la manière dont ils assurent le traitement global ou la logique du système d'IA ; les principaux choix de conception, y compris la justification et les hypothèses formulées, également en ce qui concerne les personnes ou les groupes de personnes sur lesquels le système est destiné à être utilisé ; les principaux choix de classement ; ce que le système est conçu pour optimiser et la pertinence des différents paramètres ; les décisions relatives à d'éventuels arbitrages concernant les solutions techniques adoptées pour se conformer aux exigences énoncées au titre III, chapitre 2 ;

~~(c) la description de l'architecture du système expliquant comment les composants logiciels se complètent ou s'alimentent les uns les autres et s'intègrent dans le traitement global , les ressources informatiques utilisées pour développer, former, tester et valider le système d'IA ;~~

d) le cas échéant, les exigences en matière de données sous la forme de fiches techniques décrivant les méthodologies et techniques de formation et les ensembles de données de formation utilisés, y compris des informations sur la provenance de ces ensembles de données, leur portée et leurs principales caractéristiques; comment les données ont été obtenues et sélectionnées ; les procédures d'étiquetage (par exemple pour l'apprentissage supervisé), les méthodologies de nettoyage des données (par exemple la détection des valeurs aberrantes) ;

e) évaluation des mesures de surveillance humaine nécessaires conformément à l'article 14, y compris une évaluation des mesures techniques nécessaires pour faciliter l'interprétation des résultats des systèmes d'IA par les déployeurs, conformément à articles 13(3)(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 assurer la conformité continue du système d'IA avec les exigences applicables énoncées au titre III, chapitre 2 ;

g) les procédures de validation et d'essai utilisées, y compris des informations sur les données de validation et d'essai utilisées et leurs principales caractéristiques; les paramètres utilisés pour mesurer l'exactitude, la robustesse, la cyb~~ersécurité et la c~~onformité aux autres exigences pertinentes énoncées au titre III, chapitre 2, ainsi que les impacts potentiellement 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);

g bis) mesures de cybersécurité mises en place.

3. Informations détaillées sur la surveillance, le fonctionnement et le contrôle du système d'IA, notamment en ce qui concerne : ses capacités et ses limites de performance, y compris les degrés de précision pour des personnes ou des groupes de personnes spécifiques sur lesquels le système est destiné à être utilisé et le niveau global de précision attendu par rapport à son objectif ; les résultats imprévus prévisibles et les sources de risques pour la santé et la sécurité, les droits fondamentaux et la discrimination compte tenu de l'objectif visé par le système d'IA ; les mesures de surveillance humaine nécessaires conformément à l'article 14, y compris les mesures techniques mises en place pour faciliter l'interprétation des résultats des systèmes d'IA par les déployeurs ; spécifications sur les données d'entrée, le cas échéant ;

3a. Une description de la pertinence des mesures de performance pour l'IA spécifique système

3b. Informations sur la consommation d'énergie du système d'IA pendant la phase de développement et la consommation d'énergie prévue pendant l'utilisation en tenant compte, le cas échéant, de la législation de l'Union et nationale pertinente ;

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

5. Une description de toute modification pertinente apportée par les fournisseurs au système tout au long de son cycle de vie. 6. Une liste des normes harmonisées appliquées en totalité ou en partie dont les références ont été publiées au Journal officiel de l'Union européenne. si aucune norme harmonisée de ce type n'a été appliquée, une description détaillée des solutions adoptées pour satisfaire aux exigences énoncées au titre III, chapitre 2, y compris une liste des autres normes pertinentes ou spécifications communes appliquées 7. Une copie de la déclaration UE de conformité ;

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

Articles 1 et 2, visas 5a et 5b, considérants 1-6 5a et 10-13	CA

CITATIONS

5a. vu l'avis de la Banque centrale européenne

5b. vu l'avis conjoint du comité européen de la protection des données et du contrôleur européen de la protection des données

(1) Le présent règlement a pour objet de promouvoir l'adoption d'une intelligence artificielle centrée sur l'humain et digne de confiance et d'assurer un niveau élevé de protection de la santé, de la sécurité, des droits fondamentaux, de la démocratie, de l'État de droit et de l'environnement contre les effets nocifs de l'intelligence artificielle. systèmes dans l'Union tout en soutenant l'innovation et en améliorant le fonctionnement du marché intérieur. Le présent règlement établit un cadre juridique uniforme, notamment pour le développement, la mise sur le marché, la mise en service et l'utilisation de l'intelligence artificielle conformément aux valeurs de l'Union, et garantit la libre circulation transfrontière des biens et services basés sur l'IA, empêchant ainsi les États membres d'imposer des restrictions au développement, à la commercialisation et à l'utilisation des systèmes d'IA, sauf autorisation expresse du présent règlement.

Certains systèmes d'IA peuvent également avoir un impact sur la démocratie, l'état de droit et l'environnement. Aux fins du présent règlement, ces préoccupations sont spécifiquement traitées dans les secteurs critiques et les cas d'utilisation énumérés à l'annexe III, point 8, et à l'article 15 bis et à l'annexe IV, point 3 ter, respectivement.

(1 bis) Le présent règlement devrait préserver les valeurs de l'Union en facilitant la répartition des avantages de l'intelligence artificielle dans l'ensemble de la société, en protégeant les individus, les entreprises, la démocratie, l'État de droit et l'environnement contre les risques tout en stimulant l'innovation et l'emploi et en faisant de l'Europe un chef de file dans ce domaine

(2) Les systèmes d'intelligence artificielle (systèmes d'IA) peuvent être facilement déployés dans de multiples secteurs de l'économie et de la société, y compris transfrontaliers, et circuler dans toute l'Union. Certains États membres ont déjà envisagé l'adoption de règles nationales pour garantir que l'intelligence artificielle est fiable et sûre et qu'elle est développée et utilisée dans le respect des obligations en matière de droits fondamentaux. Des règles nationales différentes peuvent entraîner une fragmentation du marché intérieur et réduire la sécurité juridique des opérateurs qui développent ou utilisent des systèmes d'IA. Il convient donc de garantir un niveau de protection cohérent et élevé dans l'ensemble de l'Union afin de parvenir à une IA fiable, tout en prévenant les divergences entravant 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 garantissant la protection uniforme des raisons impérieuses d'intérêt public et des droits des personnes dans l'ensemble du marché intérieur sur la base de l'article 114 du traité sur le fonctionnement de l'Union européenne (TFUE).

(2 bis) Étant donné que l'intelligence artificielle repose souvent sur le traitement de gros volumes de données et que de nombreux systèmes et applications d'intelligence artificielle reposent sur le traitement de données à caractère personnel, il convient de fonder le présent règlement sur l'article 16 du TFUE, qui consacre le droit à la

protection des personnes physiques à l'égard du traitement des données à caractère personnel et prévoit l'adoption de règles relatives à la protection des personnes à l'égard du traitement des données à caractère personnel.

(2 ter) Le droit fondamental à la protection des données à caractère personnel est garanti notamment par les règlements (UE) 2016/679 et (UE) 2018/1725 et la directive 2016/680. La directive 2002/58/CE protège en outre la vie privée et la confidentialité des communications, notamment en prévoyant des conditions pour le stockage et l'accès de toutes les données personnelles et non personnelles dans les équipements terminaux. Ces actes juridiques constituent la base d'un traitement durable et responsable des données, y compris lorsque les ensembles de données comprennent un mélange de données personnelles et non personnelles. Le présent règlement ne vise pas à affecter l'application du droit de l'Union existant régissant le traitement des données à caractère personnel, y compris les missions et les pouvoirs des autorités de contrôle indépendantes compétentes pour contrôler le respect de ces instruments. Le présent règlement n'affecte pas les droits fondamentaux à la vie privée et à la protection des données à caractère personnel tels qu'ils sont prévus par le droit de l'Union sur la protection des données et la vie privée et consacrés dans la charte des droits fondamentaux de l'Union européenne (la « charte »).

(2 quater) Les systèmes d'intelligence artificielle dans l'Union sont soumis à la législation pertinente en matière de sécurité des produits qui fournit un cadre protégeant les consommateurs contre les produits dangereux en général, et cette législation devrait continuer à s'appliquer. Le présent règlement est également 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, notamment le règlement (UE) 2017/2394, le règlement (UE) 2019/1020 et la directive 2001/95/CE relative aux produits sécurité et Directive 2013/11/EU..

(2 quinquies) Conformément à l'article 114, paragraphe 2, du TFUE, le présent règlement complète et ne devrait pas porter atteinte aux droits et intérêts des travailleurs salariés. Le présent règlement ne devrait donc pas affecter le droit communautaire en matière de politique sociale ni le droit et les pratiques nationales du travail, c'est-à-dire toute disposition légale et contractuelle concernant les conditions d'emploi, les conditions de travail, y compris la santé et la sécurité au travail, et les relations entre employeurs et travailleurs, y compris l'information, la consultation et la participation. Le présent règlement ne devrait pas porter atteinte à l'exercice des droits fondamentaux tels qu'ils sont reconnus dans les États membres et au niveau de l'Union, y compris le droit ou la liberté de faire grève ou d'entreprendre d'autres actions couvertes par les systèmes spécifiques de relations industrielles des États membres, conformément au droit national et /ou pratiquer. Elle ne devrait pas non plus affecter les pratiques de concertation, le droit de négocier, de conclure et d'appliquer des conventions collectives ou de mener des actions collectives conformément à la législation et/ou à la pratique nationales. Cela ne devrait en aucun cas empêcher la Commission de proposer une législation spécifique sur les droits et libertés des travailleurs concernés par les systèmes d'IA.

(2 sexies) Le présent règlement ne devrait pas affecter les dispositions visant à améliorer les conditions de travail sur les plateformes de travail énoncées dans la directive 2021/762/CE.

(2 septies) Le présent règlement devrait contribuer à soutenir la recherche et l'innovation et ne devrait pas saper les activités de recherche et de développement et respecter la liberté de la recherche scientifique. Il est donc nécessaire d'exclure de son champ d'application les systèmes d'IA spécifiquement développés aux seules fins de la recherche et du développement scientifiques et de veiller à ce que le règlement n'affecte pas d'une autre manière les activités de recherche et de développement scientifiques sur les systèmes d'IA. En toutes circonstances, toute recherche et développement

l'activité doit être exercée conformément à la Charte des droits fondamentaux,
Le droit de l'Union ainsi que le droit des États membres

(3) L'intelligence artificielle est une famille de technologies en évolution rapide qui peut et contribue déjà à un large éventail d'avantages économiques, environnementaux et sociétaux dans l'ensemble du spectre des industries et des activités sociales si elle est développée conformément aux principes généraux pertinents conformément à la Charte des principes fondamentaux de l'UE. Les droits et les valeurs sur lesquelles l'Union est fondée. En améliorant la prévision, en optimisant les opérations et l'allocation des ressources et en personnalisant les solutions numériques disponibles pour les individus et les organisations, l'utilisation de l'intelligence artificielle peut fournir des avantages concurrentiels clés aux entreprises et soutenir des résultats bénéfiques sur le plan social et environnemental, par exemple dans les soins de santé, l'agriculture, la sécurité alimentaire, l'éducation et la formation, les médias, le sport, la culture, la gestion des infrastructures, l'énergie, le transport et la logistique, la gestion de crise, les services publics, la sécurité, la justice, l'efficacité des ressources et de l'énergie, la surveillance de l'environnement, la conservation et la restauration de la biodiversité et des écosystèmes et l'atténuation du changement climatique et adaptation.

(3 bis) Pour contribuer à atteindre les objectifs de neutralité carbone, les entreprises européennes devraient s'efforcer d'utiliser toutes les avancées technologiques disponibles susceptibles de contribuer à la réalisation de cet objectif. L'intelligence artificielle est une technologie qui a le potentiel d'être utilisée pour traiter la quantité toujours croissante de données créées lors de processus industriels, environnementaux, sanitaires et autres. Afin de faciliter les investissements dans les outils d'analyse et d'optimisation fondés sur l'IA, le présent règlement devrait fournir un environnement prévisible et proportionné pour les solutions industrielles à faible risque.

(4) Dans le même temps, en fonction des circonstances de son application et de son utilisation spécifiques, ainsi que du niveau de développement technologique, l'intelligence artificielle peut générer des risques et porter atteinte aux intérêts publics ou privés et aux droits fondamentaux des personnes physiques qui sont protégés par le droit de l'Union. Un tel préjudice peut être matériel ou immatériel, y compris un préjudice physique, psychologique, sociétal ou économique.

(4 bis) Compte tenu de l'impact majeur que l'intelligence artificielle peut avoir sur la société et de la nécessité d'instaurer la confiance, il est essentiel que l'intelligence artificielle et son cadre réglementaire soient développés conformément aux valeurs de l'Union consacrées à l'article 2 du TUE, aux libertés et droits fondamentaux consacrés dans les Traités, la Charte et le droit international des droits de l'homme. Comme condition préalable, l'intelligence artificielle devrait être une technologie centrée sur l'humain. Elle ne doit pas se substituer à l'autonomie humaine ni assumer la perte de la liberté individuelle et doit avant tout servir les besoins de la société et le bien commun.
Il convient de prévoir des garanties pour garantir le développement et l'utilisation d'une intelligence artificielle éthiquement intégrée qui respecte les valeurs de l'Union et la charte.

(5) Un cadre juridique de l'Union établissant des règles harmonisées en matière d'intelligence artificielle est donc nécessaire pour favoriser le développement, l'utilisation et l'adoption de l'intelligence artificielle dans le marché intérieur tout en répondant à un niveau élevé de protection des intérêts publics, tels que la santé et la sécurité, la protection des droits fondamentaux, la démocratie et l'état de droit et l'environnement, tels que reconnus et protégés par le droit de l'Union. Pour atteindre cet objectif, il convient d'établir des règles régissant la mise sur le marché, la mise en service et l'utilisation de certains systèmes d'IA, garantissant ainsi le bon fonctionnement du marché intérieur et permettant à ces systèmes de bénéficier du principe de libre circulation de biens et de services. Ces règles doivent être claires et solides pour protéger les droits fondamentaux, soutenir de nouvelles solutions innovantes et permettre à un écosystème européen d'acteurs publics et privés de créer des systèmes d'IA conformes aux normes de l'UE.

valeurs. En établissant ces règles ainsi que des mesures de soutien à l'innovation avec un accent particulier sur les PME et les start-up, le présent règlement soutient l'objectif de promouvoir l'"IA made in Europe, de l'Union d'être un leader mondial dans le développement de une intelligence artificielle sûre, digne de confiance et éthique, comme l'a déclaré le Conseil européen4 et elle garantit la protection des principes éthiques, comme l'a spécifiquement demandé le Parlement européen5 .

(5 bis) En outre, afin de favoriser le développement de systèmes d'intelligence artificielle conformes aux valeurs de l'Union, celle-ci doit s'attaquer aux principales lacunes et obstacles qui bloquent le potentiel de la transformation numérique, notamment la pénurie de travailleurs qualifiés dans le domaine numérique, les problèmes de cybersécurité, le manque d'investissement et d'accès à l'investissement, et les écarts existants et potentiels entre les grandes entreprises, les PME et les start-up. Il convient de veiller tout particulièrement à ce que les avantages de l'IA et de l'innovation dans les nouvelles technologies se fassent sentir dans toutes les régions de l'Union et à ce que des investissements et des ressources suffisants soient fournis, en particulier aux régions qui pourraient être à la traîne pour certains indicateurs numériques.

(10) Afin de garantir des conditions de concurrence équitables et une protection efficace des droits et libertés des personnes dans l'ensemble de l'Union et au niveau international, les règles établies par le présent règlement devraient s'appliquer aux fournisseurs de systèmes d'IA de manière non discriminatoire, indépendamment qu'ils soient établis dans l'Union ou dans un pays tiers, et aux déployeurs de systèmes d'IA établis dans l'Union. Pour que l'Union européenne soit fidèle à ses valeurs fondamentales, les systèmes d'IA destinés à être utilisés pour des pratiques jugées inacceptables par le présent règlement devraient également être jugés inacceptables en dehors de l'UE en raison de leur effet particulièrement préjudiciable aux droits fondamentaux consacrés par la la Charte des droits fondamentaux de l'Union européenne. Il convient donc d'interdire l'exportation de ces systèmes d'IA vers des pays tiers par des fournisseurs résidant dans l'Union.

(11) Compte tenu de leur nature numérique, certains systèmes d'IA devraient relever du champ d'application du présent règlement même lorsqu'ils ne sont ni mis sur le marché, ni mis en service, ni utilisés dans l'Union. C'est le cas par exemple d'un opérateur établi dans l'Union qui sous-traite certains services à un opérateur établi hors de l'Union en rapport avec une activité à exercer par un système d'IA qui serait qualifiée de à haut risque et dont les effets impactent les personnes physiques situées dans l'Union. Dans ces circonstances, le système d'IA utilisé par l'opérateur en dehors de l'Union pourrait traiter des données collectées et transférées légalement depuis l'Union, et fournir à l'opérateur contractant dans l'Union le résultat de ce système d'IA résultant de ce traitement, sans que ce système d'IA mis sur le marché, mis en service ou utilisés dans l'Union. Afin d'empêcher le contournement du présent règlement et d'assurer une protection efficace des personnes physiques situées dans l'Union, le présent règlement devrait également s'appliquer aux fournisseurs et aux utilisateurs déployant des systèmes d'IA qui sont établis dans un pays tiers, dans la mesure où ~~la~~ production produite par ces est destiné à être utilisé dans l'Union. Néanmoins, pour tenir compte des arrangements existants et des besoins particuliers de coopération avec les partenaires étrangers avec lesquels des informations et des preuves sont échangées, le présent règlement ne devrait pas

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

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

s'appliquent aux autorités publiques d'un pays tiers et aux organisations internationales lorsqu'elles agissent dans le cadre d'accords internationaux conclus au niveau national ou européen pour la coopération répressive et judiciaire avec l'Union ou avec ses États membres.
De tels accords ont été conclus bilatéralement entre des États membres et des pays tiers ou entre l'Union européenne, Europol et d'autres agences de l'UE et des pays tiers et des organisations internationales. Cette exception devrait néanmoins être limitée aux pays de confiance et aux organisations internationales qui partagent les valeurs de l'Union.

(12) Le présent règlement devrait également s'appliquer aux institutions, offices, organes et agences de l'Union lorsqu'ils agissent en tant que fournisseur ou déployeur d'un système d'IA. Les systèmes d'IA exclusivement développés ou utilisés à des fins militaires devraient être exclus du champ d'application du présent règlement lorsque cette utilisation relève de la compétence exclusive de la politique étrangère et de sécurité commune régie par le titre V du traité sur l'Union européenne (TUE). Le présent règlement devrait être sans préjudice des dispositions relatives à la responsabilité des prestataires de services intermédiaires énoncées dans la directive 2000/31/CE du Parlement européen et du Conseil [telle que modifiée par la loi sur les services numériques].

(12 bis) Les logiciels et les données qui sont ouvertement partagés et auxquels les utilisateurs peuvent accéder librement, les utiliser, les modifier et les redistribuer ou des versions modifiées de ceux-ci peuvent contribuer à la recherche et à l'innovation sur le marché. Les recherches de la Commission européenne montrent également que les logiciels libres et open source peuvent contribuer entre 65 et 95 milliards d'euros au PIB de l'Union européenne et qu'ils peuvent offrir d'importantes opportunités de croissance pour l'économie européenne. Les utilisateurs sont autorisés à exécuter, copier, distribuer, étudier, modifier et améliorer les logiciels et les données, y compris les modèles, au moyen de licences libres et open source. Afin de favoriser le développement et le déploiement de l'IA, en particulier par les PME, les start-up, la recherche universitaire mais aussi par les particuliers, le présent règlement ne devrait pas s'appliquer à ces composants d'IA libres et open source, sauf dans la mesure où ils sont mis sur le marché ou mis en service par un fournisseur dans le cadre d'un système d'IA à haut risque ou d'un système d'IA qui relève du titre II ou IV du présent règlement.

(12 ter) Ni le développement collaboratif de composants d'IA libres et open source ni leur mise à disposition sur des référentiels ouverts ne devraient constituer une mise sur le marché ou une mise en service. Une activité commerciale, au sens de la mise à disposition sur le marché, pourrait cependant se caractériser par la facturation d'un prix, à l'exception des transactions entre micro-entreprises, pour un composant d'IA libre et open source mais aussi par la facturation d'un prix pour le support technique services, en fournissant une plate-forme logicielle à travers laquelle le fournisseur monétise d'autres services, ou en utilisant des données personnelles à des fins autres que exclusivement pour améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel.

(12 quater) Les développeurs de composants d'IA gratuits et open source ne devraient pas être mandatés, en vertu du présent règlement, pour se conformer aux exigences ciblant la chaîne de valeur de l'IA et, en particulier, pas envers le fournisseur qui a utilisé ce composant d'IA gratuit et open source. Les développeurs de composants d'IA gratuits et open source devraient toutefois être encouragés à mettre en œuvre des pratiques de documentation largement adoptées, telles que des modèles et des cartes de données, afin d'accélérer le partage d'informations tout au long de la chaîne de valeur de l'IA, permettant la promotion de systèmes d'IA fiables dans l'UE. .

(13) Afin de garantir un niveau cohérent et élevé de protection des intérêts publics en ce qui concerne la santé, la sécurité et les droits fondamentaux ainsi que la démocratie, l'État de droit et l'environnement, il convient d'établir des normes normatives communes pour tous les systèmes d'IA à haut risque .
Ces normes devraient être conformes à la Charte des droits fondamentaux

droits de l'Union européenne (la charte), le pacte vert européen (le pacte vert), la déclaration commune sur les droits numériques de l'Union (la déclaration) et les lignes directrices en matière d'éthique pour une intelligence artificielle (IA) digne de confiance du groupe d'experts de haut niveau sur l'intelligence artificielle (IA HLEG), et devrait être non discriminatoire et conforme aux engagements commerciaux internationaux de l'Union.

TITRE I

DISPOSITIONS GÉNÉRALES

Article 1

Objet

Le présent règlement a pour objet de promouvoir l'adoption d'une intelligence artificielle centrée sur l'humain et digne de confiance et d'assurer un niveau élevé de protection de la santé, de la sécurité, des droits fondamentaux, de la démocratie et de l'État de droit, ainsi que de l'environnement contre les effets néfastes des systèmes d'intelligence artificielle dans l'Union tout en soutenant l'innovation.

Ce règlement établit :

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

b) les interdictions de certaines pratiques d'intelligence artificielle ;

c) exigences spécifiques pour les systèmes d'IA à haut risque et obligations pour les opérateurs de de tels systèmes ;

d) des règles de transparence harmonisées pour certains systèmes d'IA ~~destinés à interagir avec des personnes physiques, les systèmes de reconnaissance des émotions et les systèmes de catégorisation biométrique, et les systèmes d'IA utilisés pour générer ou manipuler du contenu image, a~~udio ou vidéo

e) règles relatives au contrôle du marché, à la surveillance du marché, à la gouvernance et à l'application

(e bis) des mesures de soutien à l'innovation, avec un accent particulier sur les PME et les start-up, y compris la mise en place de bacs à sable réglementaires et des mesures ciblées pour réduire la charge réglementaire pesant sur les PME et les start-up;

ter) les règles d'établissement et de fonctionnement de l'Office de l'intelligence artificielle de l'Union européenne.

Article 2

Portée

1. Le présent règlement s'applique :

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

(b) les déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou qui sont situé dans l'Union

c) les fournisseurs et les déployeurs de systèmes d'IA qui ont leur lieu d'établissement ou sont situés dans un pays tiers, où soit la législation de l'État membre s'applique en vertu du droit international public, soit la production produite par le système est destinée à être utilisée dans l'Union ;

c bis) les fournisseurs mettant sur le marché ou mettant en service les systèmes d'IA visés à l'article 5 en dehors de l'Union lorsque le fournisseur ou le distributeur de ces systèmes est situé dans l'Union;

c ter) les importateurs et distributeurs de systèmes d'IA ainsi que les mandataires des fournisseurs de systèmes d'IA, lorsque ces importateurs, distributeurs ou mandataires ont leur établissement ou sont situés dans l'Union;

cc) les personnes concernées au sens de l'article 3, paragraphe 8 bis, qui se trouvent dans l'Union et dont la santé, la sécurité ou les droits fondamentaux ont été compromis par l'utilisation d'un système d'IA qui a été mis sur le marché ou mis en service dans l'Union ;

2. Pour les systèmes d'IA à haut risque qui sont des composants de sécurité de produits ou de systèmes, ou qui sont eux-mêmes des produits ou des systèmes et qui relèvent du champ d'application de la législation d'harmonisation énumérée à l'annexe II - section B, seul l'article 84 du présent règlement s'applique :

~~(a) Règlement (CE) 300/2008; (b) Règlement (UE) n° 167/2013; (c) Règlement (UE) n° 168/2013; (d) Directive 2014/90/UE; (e) Directive (UE) 2016/797; (f) Règlement (UE) 2018/858; (g) Règlement (UE) 2018/1139; (h) Règlement (UE) 2019/2144.~~

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

4. Le présent règlement ne s'applique pas aux autorités publiques d'un pays tiers ni aux organisations internationales relevant du champ d'application du présent règlement en vertu du paragraphe 1, lorsque ces autorités ou organisations utilisent des systèmes d'IA dans le cadre de la coopération internationale ou d'accords de coopération en matière répressive et judiciaire. avec l'Union ou avec un ou plusieurs États membres et font l'objet d'une décision de la Commission adoptée conformément à l'article 36 de la directive (UE) 2016/680 ou à l'article 45 du règlement 2016/679 (décision d'adéquation) ou font partie d'une accord international conclu entre l'Union et ce pays tiers ou cette organisation internationale en vertu de l'article 218 du TFUE prévoyant des garanties adéquates en ce qui concerne la protection de la vie privée et des libertés et droits fondamentaux des personnes.

5. Le présent règlement n'affecte pas l'application des dispositions relatives à la responsabilité des prestataires de services intermédiaires énoncées au chapitre II, section IV, de la directive

2000/31/CE du Parlement européen et du Conseil6 [à remplacer par les dispositions correspondantes de la loi sur les services numériques].

5a. Le droit de l'Union relatif à la protection des données à caractère personnel, à la vie privée et à la confidentialité des communications s'applique aux traitements de données à caractère personnel dans le cadre des droits et obligations énoncés dans le présent règlement. Le présent règlement n'affecte pas les règlements (UE) 2016/679, (UE) 2018/1725, la directive 2002/58/CE et (UE) 2016/680, sans préjudice des dispositions prévues à l'article 54 du présent règlement.

5b. Le présent règlement est 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.

5c. Le présent règlement n'empêche pas les États membres ou l'Union de maintenir ou d'introduire des dispositions législatives, réglementaires ou administratives plus favorables aux travailleurs en termes de protection de leurs droits en ce qui concerne l'utilisation des systèmes d'IA par les employeurs, ou d'encourager ou de permettre l'application de conventions collectives plus favorables aux travailleurs.

5d. Le présent règlement ne s'applique pas aux activités de recherche, d'essai et de développement concernant un système d'IA avant que ce système ne soit mis sur le marché ou mis en service, à condition que ces activités soient menées dans le respect des droits fondamentaux et du droit de l'Union applicable. Les essais en conditions réelles ne sont pas couverts par cette exemption. La Commission est habilitée à peut adopter des actes délégués conformément à l'article 73 pour préciser cette exemption afin d'en prévenir les abus existants et potentiels. L'Office AI fournit des orientations sur la gouvernance de la recherche et du développement conformément à l'article 56, visant également à coordonner son application par les autorités nationales de surveillance.

5d. Le présent règlement ne s'applique pas aux composants d'IA fournis dans le cadre de licences libres et open source, sauf dans la mesure où ils sont mis sur le marché ou mis en service par un fournisseur dans le cadre d'un système d'IA à haut risque ou d'un système d'IA relevant du titre II ou IV. Cette dérogation ne s'applique pas aux modèles de fondation tels que définis à l'art 3.

---

6 Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 sur certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique») (JO L 178 du 17.7 .2000, p.1).

Articles 70 à 85 et considérants associés	COMME 7

(83) Afin d'assurer une coopération confiante et constructive des autorités compétentes au niveau de l'Union et au niveau national, toutes les parties impliquées dans l'application du présent règlement devraient viser la transparence et l'ouverture tout en respectant la confidentialité des informations et des données obtenues dans l'accomplissement de leurs tâches en mettant en place mesures techniques et organisationnelles pour protéger la sécurité et la confidentialité des informations obtenues dans le cadre de leurs activités, y compris pour les droits de propriété intellectuelle et les intérêts de sécurité publique et nationale. Dans les cas où les activités de la Commission, des autorités nationales compétentes et des organismes notifiés en vertu du présent règlement entraînent une violation des droits de propriété intellectuelle, les États membres devraient prévoir des mesures et des recours adéquats pour garantir le respect des droits de propriété intellectuelle en application de la directive 2004 /48/CE.

(84) Le respect du présent règlement devrait être opposable au moyen de l'imposition d'amendes par l'autorité de contrôle nationale lorsqu'elle engage une procédure dans le cadre de la procédure prévue par le présent règlement. Les États membres devraient prendre toutes les mesures nécessaires pour assurer la mise en œuvre des dispositions du présent règlement, notamment en prévoyant des sanctions effectives, proportionnées et dissuasives en cas d'infraction.
Afin de renforcer et d'harmoniser les sanctions administratives en cas d'infraction au présent règlement, celui-ci fixe les plafonds pour la fixation des amendes administratives pour certaines infractions spécifiques. Lors de l'évaluation du montant des amendes, les autorités nationales compétentes devraient, dans chaque cas individuel, prendre compte de toutes les circonstances pertinentes de la situation spécifique, en tenant dûment compte notamment de la nature, de la gravité et de la durée de l'infraction et de ses conséquences ainsi que de la taille du prestataire, en particulier si le prestataire est une PME ou une start-up. 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 champ d'application du présent règlement. Les sanctions et les frais de justice prévus par le présent règlement ne devraient pas faire l'objet de clauses contractuelles ou de tout autre arrangement.

(84 bis) Étant donné que les droits et libertés des personnes physiques et morales et des groupes de personnes physiques peuvent être gravement compromis par les systèmes d'IA, il est essentiel que les personnes physiques et morales ou les groupes de personnes physiques aient un accès significatif aux mécanismes de signalement et de recours et soient droit d'accéder à des recours proportionnés et efficaces. Ils devraient pouvoir signaler les infractions au présent règlement à leur autorité de contrôle nationale et avoir le droit de porter plainte contre les fournisseurs ou les déployeurs de systèmes d'IA. Le cas échéant, les déployeurs devraient fournir des mécanismes de plainte internes à l'usage des personnes physiques et morales ou des groupes de personnes physiques. Sans préjudice de tout autre recours administratif ou non judiciaire, les personnes physiques et morales et les groupes de personnes physiques devraient également avoir droit à un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité nationale de contrôle les concernant ou, lorsque la l'autorité de contrôle ne traite pas une plainte, n'informe pas le plaignant de l'état d'avancement ou du résultat préliminaire de la plainte déposée ou ne respecte pas son obligation de prendre une décision définitive concernant la plainte.

(84 ter) Les personnes concernées devraient toujours être informées qu'elles sont soumises à l'utilisation d'un système d'IA à haut risque, lorsque les déployeurs utilisent un système d'IA à haut risque pour aider à la prise de décision ou prendre des décisions concernant des personnes physiques. Ces informations peuvent servir de base aux personnes concernées pour exercer leur droit à une explication en vertu du présent règlement. Lorsque les déployeurs fournissent une explication aux personnes concernées en vertu du présent règlement, ils devraient tenir compte du niveau d'expertise et de connaissances du consommateur moyen ou de l'individu

(84 quater) La législation de l'Union relative à la protection des lanceurs d'alerte [directive (UE) 2019/1937] s'applique pleinement aux universitaires, concepteurs, développeurs, contributeurs de projets, auditeurs, chefs de produit, ingénieurs et opérateurs économiques qui obtiennent des informations sur des violations du droit de l'Union par un fournisseur du système d'IA ou de son système d'IA.

(85) Afin de garantir que le cadre réglementaire puisse être adapté si nécessaire, il convient de déléguer à la Commission le pouvoir d'adopter des actes conformément à l'article 290 du TFUE pour modifier les techniques et approches visées ~~à l'annexe I afin de définir les systèmes d'IA, la législation d'harmonisation de l'Union énu~~mérée à l'annexe II, les systèmes d'IA à haut risque énumérés à l'annexe III, les dispositions relatives à la documentation technique énumérées à l'annexe IV, le contenu de la déclaration UE de conformité à l'annexe V, les dispositions relatives aux procédures d'évaluation de la conformité à Les annexes VI et VII et les dispositions établissant les systèmes d'IA à haut risque auxquels devrait s'appliquer la procédure d'évaluation de la conformité fondée sur l'évaluation du système de gestion de la qualité et l'évaluation de la documentation technique. Il est particulièrement important que la Commission procède aux consultations appropriées au cours de ses travaux préparatoires, y compris au niveau des experts, et que ces consultations soient menées conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer". Ces consultations devraient impliquer la participation d'une sélection équilibrée de parties prenantes, y compris des organisations de consommateurs, la société civile, des associations représentant les personnes concernées, des représentants d'entreprises de différents secteurs et tailles, ainsi que des chercheurs et des scientifiques. 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 traitant de la préparation des actes délégués.

(85 bis) Compte tenu de l'évolution technologique rapide et de l'expertise technique requise pour procéder à l'évaluation des systèmes d'IA à haut risque, la Commission devrait réexaminer régulièrement l'article 5, l'article 52 et l'annexe III, au moins une fois par an, tout en consultant le Bureau de l'IA et les parties prenantes concernées

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

(87) Étant donné que l'objectif du présent règlement ne peut pas être réalisé de manière suffisante par les États membres et peut, en raison des dimensions ou des effets de l'action, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité telle qu'énoncée à l'article 5 du TUE. Conformément au principe de

proportionnalité telle qu'énoncée audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(87 bis) Étant donné que les informations fiables sur l'utilisation des ressources et de l'énergie, la production de déchets et les autres incidences sur l'environnement des systèmes d'IA et des technologies TIC connexes, y compris les logiciels, le matériel et, en particulier, les centres de données, sont limitées, la Commission devrait introduire une méthodologie adéquate pour mesurer l'incidence environnementale et l'efficacité du présent règlement à la lumière des objectifs environnementaux et climatiques de l'Union.

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

(89) Le Contrôleur européen de la protection des données et le comité européen de la protection des données ont été consultés conformément à l'article 42, paragraphe 2, du règlement (UE) 2018/1725 et ont rendu un avis le 18.6.2021.

TITRE X - Confidentialité et sanctions

Article 70
Confidentialité

1. La Commission, les autorités nationales compétentes et les organismes notifiés, l'Office AI et toute autre personne physique ou morale impliquée dans l'application du présent règlement respectent la confidentialité des informations et des données obtenues dans l'exercice de leurs missions et activités de manière à protéger , en particulier:

un. les droits de propriété intellectuelle et les informations commerciales confidentielles ou les secrets commerciaux d'une personne physique ou morale, conformément aux dispositions de la directive 2004/48/CE et de la directive 2016/943/CE, y compris le code source, à l'exception des cas visés à l'article 5 du La directive 2016/943 relative à la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre leur acquisition, leur utilisation et leur divulgation illicites s'applique.

b. la mise en œuvre effective du présent règlement, notamment pour la objet des inspections, enquêtes ou audits;

ba. intérêts publics et de sécurité nationale

c. l'intégrité des procédures pénales ou administratives.

1a. Les autorités impliquées dans l'application du présent règlement en vertu du paragraphe 1 réduisent au minimum la quantité de données dont la divulgation est demandée aux données strictement nécessaires au regard du risque perçu et de l'évaluation de ce risque et suppriment les données dès qu'elles ne sont plus nécessaires. plus nécessaires aux fins pour lesquelles elles ont été demandées et mettent en place des mesures de cybersécurité, techniques et organisationnelles adéquates et efficaces pour protéger la sécurité et la confidentialité des informations et des données obtenues dans l'exercice de leurs tâches et activités

2. Sans préjudice des paragraphes 1 et 1 bis, les informations échangées sur une base confidentielle entre les autorités nationales compétentes et entre les autorités nationales compétentes et la Commission ne sont pas divulguées sans la consultation préalable de l'autorité nationale compétente d'origine et du déployeur lorsque des systèmes d'IA à haut risque visées aux points 1, 6 et 7 de l'annexe III sont utilisées par les autorités chargées de l'application des lois, de l'immigration ou de l'asile, lorsqu'une telle divulgation compromettrait les intérêts de la sécurité publique o~~u nationale~~ .

Lorsque les autorités répressives, de l'immigration ou de l'asile sont des fournisseurs de systèmes d'IA à haut risque visés aux points 1, 6 et 7 de l'annexe III, la documentation technique visée à l'annexe IV reste dans les locaux de ces autorités. Ces autorités veillent à ce que les autorités de surveillance du marché visées à l'article 63, paragraphes 5 et 6, selon le cas, puissent, sur demande, accéder immédiatement à la documentation ou en obtenir une copie. Seul le personnel de l'autorité de surveillance du marché titulaire du niveau approprié d'habilitation de sécurité est autorisé à accéder à cette documentation ou à toute copie de celle-ci.

2. Les paragraphes 1, 1 bis et 2 n'affectent pas les droits et obligations de la Commission, des États membres et des organismes notifiés en ce qui concerne l'échange d'informations et la diffusion d'avertissements, ni les obligations des parties concernées de fournir des informations en vertu du droit pénal. des États membres.

3. La Commission et les États membres peuvent échanger, lorsque cela est strictement nécessaire et conformément aux dispositions pertinentes des accords internationaux et commerciaux, des informations confidentielles avec les autorités de régulation des pays tiers avec lesquels ils ont conclu des accords de confidentialité bilatéraux ou multilatéraux garantissant un niveau de confidentialité adéquat.

Article 71
Pénalités

1. Dans le respect des modalités et conditions prévues par le présent règlement, les États membres établissent les règles relatives aux sanctions, y ~~compris les amendes administrati~~ves, applicables aux infractions au présent règlement commises par tout opérateur, et prennent toutes les mesures nécessaires pour qu'elles soient correctement et efficacement mises en œuvre et alignées sur les lignes directrices émises par la Commission et l' Office AI conformément à l' article 82 ter . Les sanctions prévues doivent être effectives, proportionnées et dissuasives. Ils tienn~~ent compte~~ en particuli~~er~~ des intérêts des PME et des jeunes pousses et de leur viabilité économique.

2. Les États membres notifient à la Commission et à l'Office, au plus tard le [12 mois suivant la date d'entrée en vigueur du présent règlement], ces règles et ces mesures et leur notifient sans délai toute modification ultérieure les concernant.

3. Le non-respect de l'interdiction des pratiques d'intelligence artificielle visée à l'article 5 est passible d'amendes administratives pouvant aller jusqu'à 40 000 000 EUR ou, si le contrevenant est une entreprise, jusqu'à 7 % de son chiffre d'affaires annuel mondial total pour l'exercice précédent, si celui-ci est plus élevé ;

3a. Le non-respect par le système d'IA des exigences prévues aux articles 10 et 13 est passible d'amendes administratives pouvant aller jusqu'à 20 000 000 EUR ou, si le contrevenant est une entreprise, jusqu'à 4 % de son chiffre d'affaires annuel mondial total pour de l'exercice précédent, celui qui est le plus élevé

4. Le non-respect par le système d'IA ou le modèle de fondation de toute exigence ou obligation prévue par le présent règlement, autres que celles prévues aux articles 5, 10 et 13, est passible d'amendes administratives pouvant aller jusqu'à 10 000 000 EUR ou, si le contrevenant est une entreprise, jusqu'à 2% de son chiffre d'affaires mondial annuel total de l'exercice précédent, le plus élevé des deux.

5. La fourniture d'informations incorrectes, incomplètes ou trompeuses aux organismes notifiés et aux autorités nationales compétentes en réponse à une demande est passible d'amendes administratives pouvant aller jusqu'à 5 θ00 000 EUR ou, si le contrevenant est une entreprise, jusqu'à 1 % du son chiffre d'affaires mondial annuel total pour l'exercice précédent, si celui-ci est le plus élevé

6. Des amendes peuvent être infligées en plus ou à la place des mesures non pécuniaires telles que les ordonnances ou les avertissements. Lors de la décision sur le montant de l'amende administrative dans chaque cas individuel, toutes les circonstances pertinentes de la situation spécifique sont prises en compte et il est dûment tenu compte des éléments suivants :

un. la nature, la gravité et la durée de l'infraction et de ses conséquences, compte tenu de la finalité du système d'IA, ainsi que, le cas échéant, du nombre de personnes concernées et de l'ampleur du préjudice subi par celles-ci ;

b. si des amendes administratives ont déjà été infligées par d'autres autorités de contrôle d'un ou plusieurs États membres au même opérateur pour la même infraction.

c. la taille et le chiffre d'affaires annuel de l'opérateur commettant l'infraction

c bis) toute mesure prise par l'exploitant pour atténuer le préjudice ou les dommages subis par les personnes concernées

c ter) le caractère intentionnel ou négligent de l'infraction

cc) le degré de coopération avec les autorités nationales compétentes, afin de remédier à l'infraction et d'atténuer les éventuels effets préjudiciables de l'infraction

(cd) le degré de responsabilité de l'exploitant compte tenu des mesures techniques et organisationnelles mises en œuvre par celui-ci;

(ce) la manière dont l'infraction a été portée à la connaissance des autorités nationales compétentes, en particulier si, et si oui dans quelle mesure, l'exploitant a notifié l'infraction;

(cf) le respect des codes de conduite approuvés ou des mécanismes de certification approuvés ;

(cg) toute infraction antérieure pertinente de la part de l'opérateur

(ch) tout autre facteur aggravant ou atténuant applicable aux circonstances de l'affaire

7. Chaque État membre établit des règles indiquant si et dans ~~quelle mesure les amendes admini~~stratives à infliger aux autorités et organismes publics établis dans cet État membre

8. En fonction du système juridique des États membres, les règles relatives aux amendes administratives peuvent être appliquées de telle sorte que les amendes soient infligées par les juridictions nationales compétentes d'autres instances applicables dans ces États membres. L'application de ces règles dans ces États membres a un effet équivalent.

8a. Les sanctions visées au présent article ainsi que les frais de justice et les demandes d'indemnisation associés ne peuvent faire l'objet de clauses contractuelles ou d'autres formes d'accords de partage des charges entre les fournisseurs et les distributeurs, les importateurs, les déployeurs ou tout autre tiers ; −

8b. Les autorités nationales de surveillance informent annuellement l'Office AI des amendes qu'elles ont infligées au cours de l'année, conformément au présent article ;

8c. L'exercice par les autorités compétentes des pouvoirs qui leur sont conférés par le présent article est soumis à des garanties procédurales appropriées conformément au droit de l'Union et des États membres, y compris un recours juridictionnel et une procédure régulière.

Article 72

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

1. Le Contrôleur européen de la protection des données peut infliger des amendes administratives aux institutions, agences et organes de l'Union relevant du champ d'application du présent règlement. Lors de la décision d'imposer ou non une amende administrative et du montant de l'amende administrative dans chaque cas individuel, toutes les circonstances pertinentes de la situation spécifique sont prises en compte et il est dûment tenu compte des éléments suivants :

a) la nature, la gravité et la durée de l'infraction et de ses conséquences ; compte tenu de l'objectif du système d'IA concerné ainsi que du nombre de personnes concernées et du niveau de préjudice subi par elles, et de toute infraction antérieure pertinente ;

a bis) toute action entreprise par l'institution, l'agence ou l'organe de l'Union pour atténuer le préjudice subi par les personnes concernées ;

(a ter) le degré de responsabilité de l'institution, de l'agence ou de l'organe de l'Union, compte tenu des mesures techniques et organisationnelles qu'ils mettent en œuvre;

b) le degré de coopération avec le Contrôleur européen de la protection des données afin de remédier à l'infraction et d'atténuer les éventuels effets négatifs de l'infraction, y compris le respect de toute mesure précédemment ordonnée par le Contrôleur européen de la protection des données à l'encontre de l'institution ou de l'agence de l'Union ou organisme concerné par la même matière

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

(c bis) la manière dont l'infraction a été portée à la connaissance du contrôleur de la protection des données, en particulier si, et si oui dans quelle mesure, l'institution ou l'organe de l'Union a notifié l'infraction

c ter) le budget annuel de l'organisme

2. Le non-respect de l'interdiction des pratiques d'intelligence artificielle visée à l'article 5 est passible d'amendes administratives pouvant aller jusqu'à 1 500 000 EUR. -

2a. La non-conformité du système d'IA aux exigences énoncées à l'article 10 être passible d'amendes administratives pouvant aller jusqu'à 1 000 000 EUR

3. Le non-respect par le système d'IA de toute exigence ou obligation prévue par le présent règlement, autres que celles prévues aux articles 5 et 10, est passible d'amendes administratives 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, à l'agence ou à l'organe de l'Union qui fait l'objet de la procédure menée par le Contrôleur européen de la protection des données la possibilité d'être entendu sur l'affaire concernant l'infraction éventuelle . Le Contrôleur européen de la protection des données fonde ses décisions uniquement sur des éléments et des circonstances sur lesquels les parties concernées ont pu se prononcer.
Les plaignants, le cas échéant, seront étroitement associés à la procédure.

5. Les droits de la défense des parties concernées doivent être pleinement respectés dans la procédure. Ils ont le droit d'accéder au fichier du Contrôleur européen de la protection des données, sous réserve de l'intérêt légitime des personnes ou des entreprises à la protection de leurs données à caractère personnel ou secrets d'affaires.

6. Les fonds collectés par l'imposition d'amendes dans le présent article contribuent au budget général de l'Union. Les amendes n'affectent pas le fonctionnement efficace de l'institution, de l'organe ou de l'agence de l'Union sanctionné.

6a. Le Contrôleur européen de la protection des données notifie chaque année à l'IA Bureau des amendes qu'il a infligées en vertu du présent article

TITRE XI - Délégation de pouvoir et comitologie

Article 73
Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués est conféré à la Commission sous réserve des conditions prévues au présent article.

2. Le pouvoir d'adopter des actes délégués visé à l'article 4, à l'article 7, paragraphe 1, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, et à l'article 48, paragraphe 5, est conféré à la Commission pour une période de cinq ans à compter de [la date d'entrée en vigueur du règlement]. La Commission établit un rapport relatif à la délégation de pouvoir au plus tard 9 mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prorogée pour des périodes d'une durée identique, à moins que le Parlement européen ou le Conseil ne s'y oppose au plus tard trois mois avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 4, à l'article 7, paragraphe 1, à l'article 11, paragraphe 3, à l'article 43, paragraphes 5 et 6, et à l'article 48, paragraphe 5, peut être révoquée à tout moment par le Parlement européen ou par le Conseil. Une décision de révocation met fin à la délégation de pouvoir précisée dans cette décision. Elle prend effet le jour suivant celui de sa publication au Journal officiel de l'Union européenne ou à une date ultérieure qui y est précisée. Elle n'affecte pas la validité des actes délégués déjà en vigueur.

3a. Avant d'adopter un acte délégué, la Commission consulte les institutions concernées, l'Office, le forum consultatif et les autres parties prenantes concernées conformément aux principes énoncés dans l'accord interinstitutionnel du 13 avril 2016 "Mieux légiférer". Dès que la Commission décide de rédiger un acte délégué, elle en informe le Parlement européen. Cette notification n'oblige pas la Commission à adopter ledit acte.

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

5. Tout acte délégué adopté en vertu de l'article 4, de l'article 7, paragraphe 1, de l'article 11, paragraphe 3, de l'article 43, paragraphes 5 et 6, et de l'article 48, paragraphe 5, n'entre en vigueur que si aucune objection n'a été exprimée par soit le Parlement européen ou le Conseil dans un délai de trois mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont tous deux informé la Commission qu'ils ne objet. Ce délai est prolongé de trois mois à l'initiative du Parlement européen ou du Conseil.

Article 74
Procédure de comité

1. La Commission est assistée par un comité. Ce comité est un comité au sens du règlement (UE) no 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 doit s'appliquer.

TITRE XII

PROVISIONS FINALES

Article 75

Modification du règlement (CE) n° 300/2008

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

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

_____

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

Article 76

Modification du règlement (UE) n° 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 en vertu du premier alinéa concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil*, les exigences énoncées au titre III, chapitre 2 dudit règlement est pris en compte.

_____

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

Article 77

Modification du règlement (UE) n° 168/2013

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

de l'adoption d'actes délégués en vertu du premier alinéa concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/ XX sur [l'intelligence artificielle] du Parlement européen et du Conseil*, les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte.

_____

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

Article 78

Modification de la directive 2014/90/UE

À l'article 8 de la directive 2014/90/UE, le paragraphe suivant est ajouté : « 4.

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

_____

* Règlement (UE) YYY/XX [relatif à l'intelligence artificielle] (JO …) ».

Article 79

Modification de la directive (UE) 2016/797

À l'article 5 de la directive (UE) 2016/797, le paragraphe suivant est ajouté : « 12.

Lors de l'adoption d'actes délégués conformément au paragraphe 1 et d'actes d'exécution conformément au paragraphe 11 concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [relatif à l'intelligence artificielle] du Parlement européen et du Conseil*, le les exigences énoncées au titre III, chapitre 2, dudit règlement sont prises en compte.

_____

* Règlement (UE) YYY/XX [relatif à l'intelligence artificielle] (JO …) ».

Article 80

Modification du règlement (UE) 2018/858

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

« 4. Lors de l'adoption d'actes délégués conformément au paragraphe 3 concernant les systèmes d'intelligence artificielle qui sont des composants de sécurité au sens du règlement (UE) YYY/XX [sur l'intelligence artificielle] du Parlement européen et du Conseil *, les exigences énoncées au titre III, Le chapitre 2 dudit règlement est pris en compte.

_____

* Règlement (UE) YYY/XX [relatif à l'intelligence artificielle] (JO …) ».

Article 81

Modification du règlement (UE) 2018/1139

Le règlement (UE) 2018/1139 est modifié comme suit :

(1) À l'article 17, l'alinéa suivant est ajouté :

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

Article 81 bis

Modification du règlement (UE) 2019/1020

Le règlement (UE) 2019/1020 est modifié comme suit :

À l'article 14, paragraphe 4, l'alinéa suivant est ajouté:

« (l) Le pouvoir de mettre en œuvre à distance, le cas échéant, les pouvoirs prévus au présent article.

_____

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

(2) À l'article 19, l'alinéa suivant est ajouté :

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

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

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

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

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

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

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

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

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

Article 82

Modification du règlement (UE) 2019/2144

À l'article 11 du règlement (UE) 2019/2144, le paragraphe suivant est ajouté:

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

_____

* Règlement (UE) YYY/XX [relatif à l'intelligence artificielle] (JO …) ».

Article 82 bis

Une meilleure réglementation

En tenant compte des exigences du présent règlement conformément aux modifications des articles 75, 76, 77, 78, 79, 80, 81 et 82, la Commission procède à une analyse et consulte les parties prenantes concernées afin de déterminer les lacunes potentielles ainsi que les chevauchements. entre la législation sectorielle existante et les dispositions du présent règlement.

Article 82b

Orientations de la Commission sur la mise en œuvre du présent règlement

1. La Commission élabore, en consultation avec l'office AI, des lignes directrices sur la mise en œuvre pratique du présent règlement, et notamment sur: l'application des exigences

(je) visées aux articles 8 à 15 et aux articles 28 à 28 ter; (ii) les pratiques interdites visées à l'article 5 ; (iii) la mise en œuvre pratique des dispositions relatives à la modification substantielle ; les circonstances pratiques dans lesquelles le résultat d'un système d'intelligence artificielle visé à

(iv) l'annexe III présenterait un risque significatif d'atteinte à la santé, à la sécurité ou aux droits fondamentaux des personnes physiques visées à l'article 6, paragraphe 2, y compris des exemples en relation avec un risque élevé les systèmes d'IA visés à l'annexe III ; la mise en œuvre pratique des obligations de transparence prévues à l'article 52 ; vi) l'élaboration de codes de

(dans) conduite visés à l'article 69, vii) la relation entre le présent règlement et d'autres actes législatifs pertinents de l'Union, notamment en ce qui concerne la cohérence de leur application. (viii) la mise en œuvre pratique de l'article 12, 28 ter sur l'impact environnemental des modèles de fondation et de l'annexe IV 3, point b), en particulier les méthodes de mesure et de diagraphie permettant de calculer et de déclarer l'impact environnemental des systèmes pour se conformer aux obligations du présent règlement , y compris l'empreinte carbone et l'efficacité énergétique, en tenant compte des méthodes de pointe et des économies d'échelle

Lors de l'émission de ces orientations, la Commission accorde une attention particulière aux besoins des PME, y compris des start-up, des autorités publiques locales et des secteurs les plus susceptibles d'être affectés par le présent règlement.

2. À la demande des États membres ou de l'Office AI, ou de sa propre initiative, la Commission met à jour les lignes directrices déjà adoptées lorsqu'elle le juge nécessaire.

Article 83

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

1. Les opérateurs des systèmes d'IA qui sont des composants des systèmes d'information à grande échelle établis par les actes juridiques énumérés à l'annexe IX qui ont été mis sur le marché ou mis en service avant le ... [la date d'entrée en vigueur du présent règlement] prend les mesures nécessaires pour se conformer aux exigences énoncées dans le présent règlement au plus tard le [4 ans après la date d'entrée en vigueur du présent règlement]

   Les exigences énoncées dans le présent règlement sont prises en compte lors de l'évaluation de chaque système d'information à grande échelle établi par les actes juridiques énumérés à l'annexe IX à entreprendre conformément à ces actes respectifs et chaque fois que ces actes juridiques sont remplacés ou modifiés. .

2. Le présent règlement s'applique aux exploitants de systèmes d'IA à haut risque, autres que ceux visés au paragraphe 1, qui ont été mis sur le marché ou mis en service avant le [date d'application du présent règlement visée à l'article 85, paragraphe 2]], uniquement si, à compter de cette date, ces systèmes font l'objet de modifications substantielles telles que définies à l'article 3, paragraphe 23. Dans le cas de systèmes d'IA à haut risque destinés à être utilisés par des autorités publiques, les fournisseurs et les déployeurs de ces systèmes prennent les mesures nécessaires pour se conformer aux exigences du présent règlement dans un délai de 2 ans à compter de son entrée en vigueur.

Article 84

Évaluation et révision

1. Après consultation de l'Office AI, la Commission évalue la nécessité de modifier la liste de l'annexe III, y compris l'extension des intitulés de domaine existants ou l'ajout de nouveaux intitulés de domaine dans cette annexe; la liste des pratiques d'IA interdites à l'article 5, et la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires à l'article 52 (une fois par an après l'entrée en vigueur du présent règlement et sur recommandation de l'Office AI). La Commission soumet les résultats de cette évaluation au Parlement européen et au Conseil.

2. Au plus tard le [deux ans après la date d'application du présent règlement visée à l'article 85, paragraphe 2] et tous les deux ans par la suite, la Commission, conjointement avec l'office AI, soumet un rapport sur l'évaluation et le réexamen du présent règlement au Parlement européen et au Conseil. Les rapports sont rendus publics.

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

   a) l'état des ressources financières, techniques et humaines dont disposent les autorités nationales compétentes pour s'acquitter efficacement des tâches qui leur sont confiées en vertu du présent règlement;

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

   (b bis) le niveau de développement des normes harmonisées et des spécifications pour l'intelligence artificielle

   bb) les niveaux d'investissement dans la recherche, le développement et l'application de systèmes d'IA dans l'ensemble de l'Union;

(bc) la compétitivité du secteur européen agrégé de l'IA par rapport à l'IA secteurs dans les pays tiers

(bd) l'impact du règlement en ce qui concerne l'utilisation des ressources et de l'énergie, ainsi que la production de déchets et d'autres impacts environnementaux

(be) la mise en œuvre du plan coordonné sur l'IA, en tenant compte des différents niveaux de progrès entre les États membres et en identifiant les obstacles existants à l'innovation dans le domaine de l'IA.

(bf) la mise à jour des exigences spécifiques concernant la durabilité des systèmes d'IA et des modèles de base, sur la base de l'exigence de déclaration et de documentation de l'annexe IV et de l'article 28 ter

(bg) le régime juridique régissant les modèles de fondation (bh)

la liste des clauses contractuelles abusives de l'article 28 bis en tenant compte, si nécessaire, des nouvelles pratiques commerciales

3a. [2 ans après la date d'entrée en application du présent règlement visée à l'article 85, paragraphe 2], la Commission évalue le fonctionnement du bureau AI, si le bureau a été doté de pouvoirs et de compétences suffisants pour s'acquitter de ses tâches et s'il serait pertinent et nécessaire pour la bonne mise en œuvre et l'application du présent règlement afin d'améliorer l'Office et ses compétences d'exécution et d'augmenter ses ressources. La Commission soumet ce rapport d'évaluation au Parlement européen et au Conseil.

4. Dans un délai de [un an après la date d'application du présent règlement visée à l'article 85, paragraphe 2], puis tous les deux ans, la Commission évalue l'impact et l'efficacité des codes de conduite pour favoriser l'application des exigences énoncées au titre III, chapitre 2 et éventuellement d'autres exigences supplémentaires pour les systèmes d'IA autres que les systèmes d'IA à haut risque.

5. Aux fins des paragraphes 1 à 4 , l' Office AI , les États membres et les autorités nationales compétentes fournissent à la Commission des informations sur sa demande sans retard injustifié Lors de la réalisation des évaluations et des

6. examens visés aux paragraphes 1 à 4 , la Commission tient compte tient compte des positions et des conclusions de l'Office AI, du Parlement européen, du Conseil et d'autres organes ou sources pertinents et consulte les parties prenantes concernées. Le résultat de cette consultation est joint au rapport.

7. La Commission présente, si nécessaire, des propositions appropriées visant à modifier le présent règlement, en tenant compte notamment de l'évolution de la technologie et de l'incidence des systèmes d'IA sur la santé et la sécurité, les droits fondamentaux, l'environnement, l'égalité et l'accessibilité pour les personnes handicapées, la démocratie et la l'État de droit et à la lumière de l'état d'avancement de la société de l'information.

7h du matin Pour guider les évaluations et les examens visés aux paragraphes 1 à 4 du présent article, l'Office s'engage à développer une méthodologie objective et participative pour l'évaluation du niveau de risque sur la base des critères énoncés dans les articles pertinents et l'inclusion de nouveaux systèmes dans : la liste de l'annexe III, y compris l'extension des vedettes de domaine existantes ou l'ajout de nouvelles vedettes de domaine dans cette annexe; la liste des interdits

pratiques prévues à l'article 5; et la liste des systèmes d'IA nécessitant des mesures de transparence supplémentaires conformément à l'article 52.

7b. Toute modification du présent règlement conformément au paragraphe 7 du présent article, ou des futurs actes délégués ou actes d'exécution pertinents, qui concernent la législation sectorielle énumérée à l'annexe II, section B, tient compte des spécificités réglementaires de chaque secteur, ainsi que de la gouvernance, de l'évaluation de la conformité et des les mécanismes d'application et les autorités qui y sont établies.

7c. Au plus tard cinq ans à compter de la date d'application du présent règlement, la Commission procède à une évaluation de l'application du présent règlement et en fait rapport au Parlement européen, au Conseil et au Comité économique et social européen, en tenant compte les premières années d'application du règlement. Sur la base des conclusions, ce rapport est, le cas échéant, accompagné d'une proposition de modification du présent règlement en ce qui concerne la structure d'exécution et la nécessité pour une agence de l'UE de remédier à toute lacune identifiée.

Article 85

Entrée en vigueur et application

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

2. Le présent règlement s'applique à partir du [24 mois après l'entrée en vigueur du règlement].

3. Par dérogation au paragraphe 2 :

a) le titre III, le chapitre 4 et le titre VI s'appliquent à partir du [trois mois suivant l'entrée en vigueur du présent règlement];

b) L'article 71 s'applique à partir de [douze mois après l'entrée en vigueur du présent Régulation].

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

Titre VI, chapitre 1 et considérant 76	CA 8

(76) Afin d'éviter la fragmentation, d'assurer le fonctionnement optimal du marché unique, d'assurer une mise en œuvre efficace et harmonisée du présent règlement, d'atteindre un niveau élevé de fiabilité et de protection de la santé, de la sécurité, des droits fondamentaux, de l'environnement, la démocratie et l'État de droit dans l'ensemble de l'Union en ce qui concerne les systèmes d'intelligence artificielle, à soutenir activement les autorités nationales de surveillance, les institutions, organes et organismes de l'Union sur les questions relatives au présent règlement, et à accroître l'adoption de l'intelligence artificielle dans l'ensemble de l'Union, un Office de l'intelligence artificielle de l'Union européenne devrait être créé. L'Office AI devrait être doté de la personnalité juridique, agir en toute indépendance, être chargé d'un certain nombre de tâches de conseil et de coordination, y compris l'émission d'avis, de recommandations, de conseils ou d'orientations sur des questions liées à la mise en œuvre du présent règlement, et être doté d'un financement et d'une doté de personnel. Les États membres devraient assurer la direction stratégique et le contrôle de l'Office AI par l'intermédiaire du conseil d'administration de l'Office AI, aux côtés de la Commission, du CEPD, de la FRA et de l'ENISA. Un directeur exécutif devrait être chargé de gérer les activités du secrétariat du bureau AI et de représenter le bureau AI. Les parties prenantes doivent officiellement participer aux travaux du Bureau AI par le biais d'un forum consultatif qui doit garantir une représentation variée et équilibrée des parties prenantes et doit conseiller le Bureau AI sur les questions relatives. Au cas où la création de l'Office AI s'avérerait insuffisante pour garantir une application pleinement cohérente du présent règlement au niveau de l'Union ainsi que des mesures d'exécution transfrontières efficaces, la création d'une agence AI devrait être envisagée.

TITRE VI

GOUVERNANCE

CHAPITRE 1

BUREAU EUROPÉEN D'INTELLIGENCE ARTIFICIELLE

SECTION 1 : Dispositions générales relatives à l'Office européen de l'intelligence artificielle

Article 56

Création de l'Office européen de l'intelligence artificielle

1. L'«Office européen de l'intelligence artificielle» (ci-après l'«Office IA») est institué. Le Bureau AI est un organe indépendant de l'Union. Elle est dotée de la personnalité juridique.

2. L'Office AI dispose d'un secrétariat et dispose de ressources financières et d'un personnel suffisants pour s'acquitter de ses tâches conformément au présent règlement.

3. Le siège de l'Office AI est à Bruxelles.

Article 56 bis
Structure

La structure administrative et de gestion de l'Office AI comprend: a) un conseil d'administration, comprenant un président

(b) un secrétariat géré par un directeur exécutif;

(c) un forum consultatif.

Article 56b
Tâches du bureau AI

Le Bureau de l'AI exécute les tâches suivantes :

un) soutenir, conseiller et coopérer avec les États membres, les autorités nationales de surveillance, la Commission et les autres institutions, organes, offices et agences de l'Union en ce qui concerne la mise en œuvre du présent règlement ;

b) surveiller et assurer l'application efficace et cohérente du présent règlement, sans préjudice des missions des autorités nationales de surveillance;

c) contribuer à la coordination entre les autorités nationales de surveillance chargées de l'application du présent règlement, –

d) servir de médiateur dans les discussions sur les désaccords graves pouvant survenir entre les autorités compétentes concernant l'application du règlement

C'est) coordonner les enquêtes conjointes, conformément à l'article 66 bis;

F) contribuer à une coopération efficace avec les autorités compétentes des pays tiers et avec les organisations internationales.

g) recueillir et partager l'expertise et les meilleures pratiques des États membres et aider les États membres autorités nationales de surveillance des États et de la Commission pour développer l'expertise organisationnelle et technique nécessaire à la mise en œuvre de la présente réglementation, y compris en facilitant la création et le maintien d'un Pool d'experts de l'Union

h) examiner, de sa propre initiative ou à la demande de son directoire ou du Commission, les questions relatives à la mise en œuvre du présent règlement et d'émettre des avis, des recommandations ou des contributions écrites notamment en ce qui concerne :

(je) spécifications techniques ou normes existantes;

(ii) les lignes directrices de la Commission

(iii) les codes de conduite et leur application, en étroite coopération avec l'industrie et les autres parties prenantes concernées ; la révision éventuelle

(iv) du règlement, la préparation des actes délégués et les éventuels alignements du présent règlement sur les actes juridiques énumérés à l'annexe II;

(dans) tendances, telles que la compétitivité mondiale européenne en matière d'intelligence artificielle, l'adoption de l'intelligence artificielle dans l'Union, le développement des compétences numériques et les menaces systémiques émergentes liées à l'intelligence artificielle

vi) des orientations sur la manière dont le présent règlement s'applique à la typologie en constante évolution des chaînes de valeur de l'IA, en particulier sur les implications qui en résultent en termes de responsabilité de toutes les entités concernées

i) émettre :

(je) un rapport annuel comprenant une évaluation de la mise en œuvre du présent règlement, un examen des déclarations d'incident grave visées à l'article l'article 62 et le fonctionnement de la base de données visée à l'article 60 et

ii) des recommandations à la Commission sur la catégorisation des pratiques interdites, les systèmes d'IA à haut risque visés à l'annexe III, les codes de conduite visés à l'article 69 et l'application des principes généraux énoncés à l'article 4 bis

j) aider les autorités à établir et à développer des bacs à sable réglementaires et à faciliter la coopération entre les bacs à sable réglementaires ;

k) organiser des réunions avec les agences de l'Union et les organes de gouvernance dont les tâches sont liées à l'intelligence artificielle et à la mise en œuvre de la présente Régulation;

l) organiser des consultations trimestrielles avec le forum consultatif et, le cas échéant, des consultations publiques avec d'autres parties prenantes, et rendre publics les résultats de ces consultations sur son site Internet ;

m) promouvoir la sensibilisation du public et sa compréhension des avantages, des risques, des garanties et des droits et obligations liés à l'utilisation des systèmes d'IA ;

n) faciliter l'élaboration de critères communs et une compréhension partagée par les opérateurs du marché et les autorités compétentes des concepts pertinents prévus dans le présent règlement ;

O) assurer le suivi des modèles de fondation et organiser un dialogue régulier avec les développeurs de modèles de fondation en ce qui concerne leur conformité ainsi que les systèmes d'IA qui utilisent ces modèles d'IA

p) fournir des conseils d'interprétation sur la manière dont la loi sur l'IA s'applique à la typologie en constante évolution des chaînes de valeur de l'IA, et quelles sont les implications qui en résultent en termes de

la responsabilité de toutes les entités concernées se fera selon les différents scénarios basés sur l'état de la technique généralement reconnu, y compris tel que reflété dans les normes harmonisées pertinentes ;

q) assurer une surveillance et un suivi particuliers et institutionnaliser un dialogue régulier avec les fournisseurs de modèles de fondations sur la conformité des modèles de fondations ainsi que des systèmes d'IA qui utilisent ces modèles d'IA avec l'article 28 ter du présent règlement, et sur les meilleures pratiques du secteur en matière d'auto-gouvernance. Toute réunion de ce type est ouverte aux autorités nationales de surveillance, aux organismes notifiés et aux autorités de surveillance du marché pour y participer et y contribuer ;

r) publier et mettre à jour périodiquement des directives sur les seuils qui qualifient la formation d'un modèle de fondation comme une grande course de formation, enregistrer et surveiller les instances connues de grandes courses de formation et publier un rapport annuel sur l'état d'avancement du développement, de la prolifération et de l'utilisation de la fondation modèles parallèlement aux options politiques pour faire face aux risques et opportunités spécifiques aux modèles de fondation.

s) promouvoir la connaissance de l'IA conformément à l'article 4b.

Article 56c

Responsabilité, indépendance et transparence

1. Le Bureau AI doit :

un. être responsable devant le Parlement européen et le Conseil en conformément au présent règlement ;

b. agir en toute indépendance dans l'accomplissement de ses tâches ou l'exercice de ses pouvoirs ; et

c. assurer un haut niveau de transparence concernant ses activités et développer de bonnes pratiques administratives à cet égard.

Le règlement (CE) n° 1049/2001 s'applique aux documents détenus par l'Office AI.

SECTION 2 : Conseil d'administration

Article 57b

Composition du directoire

1. Le conseil d'administration est composé des membres suivants: a) un représentant de l'autorité de surveillance nationale de chaque État membre; (b) un représentant de la Commission (c) un représentant du Contrôleur européen de la protection des données (CEPD);

d) un représentant de l'Agence de l'Union européenne pour la cybersécurité (ENISA); e) un représentant de l'Agence des droits fondamentaux (FRA).

Chaque représentant d'une autorité nationale de contrôle dispose d'une voix. Les représentants de la Commission, du CEPD, de l'ENISA et de la FRA n'ont pas de droit de vote. Chaque membre aura un suppléant. La nomination des membres et des membres suppléants du conseil d'administration tient compte de la nécessité de la parité hommes-femmes. Les membres du directoire et leurs suppléants sont rendus publics.

2. Les membres et membres suppléants du conseil d'administration ne doivent pas occuper de positions ou d'intérêts commerciaux conflictuels en ce qui concerne tout sujet lié à ~~l'a~~pplication du présent règlement.

3. Les règles relatives aux réunions et aux votes du conseil d'administration ainsi qu'à la nomination et à la révocation du directeur exécutif sont fixées dans le règlement intérieur visé à l'article 57 quater, point a).

Article 57b

Fonctions du conseil d'administration

1. Le conseil d'administration a les tâches suivantes :

(un) prendre des décisions stratégiques sur les activités du Bureau AI et adopter son règlement intérieur à la majorité des deux tiers de ses membres ; mettre en œuvre son règlement intérieur ; adopter le document

(avant JC) unique de programmation de l'Office AI ainsi que son rapport public annuel et les transmettre au Parlement européen, au Conseil, à la Commission et à la Cour des comptes ; adopter le budget du Bureau AI; nommer le directeur général et, le

(d) cas échéant, proroger ou écourter le

(e) mandat du directeur général ou le révoquer ; décider de la mise en place des structures internes du Bureau AI et, le cas échéant, de la modification de ces structures internes nécessaires à

(F) l'accomplissement des tâches du Bureau AI ;

Article 57c

Président du conseil d'administration

1. Le conseil d'administration élit un président et deux vice-présidents parmi ses membres votants, à la majorité simple.

2. Le mandat du président et des vice-présidents est de quatre ans. Les mandats du président et des vice-présidents, renouvelables une fois. —

SECTION 2 : Secrétariat

Article 57

Secrétariat

1. Les activités du secrétariat sont gérées par un directeur exécutif, qui est responsable de ses activités devant le conseil d'administration. Sans préjudice des compétences respectives du conseil d'administration et des institutions de l'Union, le directeur exécutif ne sollicite ni n'accepte d'instructions d'aucun gouvernement ni d'aucun autre organisme

2. Le directeur exécutif assiste aux auditions sur toute question liée aux activités de l'Office AI et rend compte de l'exercice de ses fonctions lorsqu'il y est invité par le Parlement européen ou le Conseil.

3. Le directeur exécutif représente l'Office AI, y compris dans les enceintes internationales de coopération en matière d'intelligence artificielle ;

4. Le secrétariat fournit au conseil d'administration et au forum consultatif le soutien analytique, administratif et logistique nécessaire à l'accomplissement des tâches de l'IA
Bureau, notamment

en : a) mettant en œuvre les décisions, programmes et activités adoptés par le conseil d'administration;

(b) préparer chaque année le projet de document unique de programmation, le projet de budget, le rapport annuel d'activité de l'Office AI, les projets d'avis et de positions de l'Office AI, et les soumettre au conseil d'administration;

c) Coordonner avec les instances internationales de coopération sur les intelligence;

SECTION 4 : Forum consultatif

Article 58

Forum consultatif

1. Le forum consultatif fournit à l'Office AI les contributions des parties prenantes sur les questions liées au présent règlement, en particulier en ce qui concerne les tâches énoncées à l'article 56 septies, point b).

2. Les membres du forum consultatif représentent une sélection équilibrée de parties prenantes, y compris l'industrie, les start-ups, les PME, la société civile, les partenaires sociaux et les universités. La composition du forum consultatif doit être équilibrée en ce qui concerne les intérêts commerciaux et non commerciaux et, dans la catégorie des intérêts commerciaux, en ce qui concerne les PME et les autres entreprises.

3. Le conseil d'administration nomme les membres du forum consultatif conformément à la procédure de sélection établie dans le règlement intérieur de l'Office AI et en tenant compte de l'exigence de transparence et conformément aux critères énoncés au paragraphe 2 ;

4. Le mandat des membres du forum consultatif est de deux ans et peut être prolongé de quatre ans au maximum.

5. Le Comité européen de normalisation (CEN), le Comité européen de normalisation électrotechnique (CENELEC) et l'Institut européen des normes de télécommunications (ETSI) sont membres permanents du forum consultatif. Le Centre commun de recherche est membre permanent, sans droit de vote.

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

7. Le forum consultatif se réunit au moins quatre fois par an. Le forum consultatif peut inviter des experts et d'autres parties prenantes à ses réunions. Le directeur général peut assister d'office aux réunions du forum consultatif.

8. Dans l'accomplissement de son rôle tel qu'énoncé au paragraphe 1, le forum consultatif peut préparer des avis, des recommandations et des contributions écrites.

9. Le forum consultatif peut établir des sous-groupes permanents ou temporaires, selon le cas, aux fins d'examiner des questions spécifiques liées aux objectifs du présent règlement.

10. Le forum consultatif prépare un rapport annuel de ses activités. Ce rapport doit être rendue publique.

SECTION 5 : Autorités européennes en matière de benchmarking

Article 58 bis

Analyse comparative

Les autorités européennes en matière d'analyse comparative visées à l'article 15, paragraphe 1 bis, et l'Office IA élaborent conjointement, en étroite coopération avec des partenaires internationaux, des orientations et des capacités d'un bon rapport coût-efficacité pour mesurer et comparer les aspects des systèmes et des composants d'IA, et notamment modèles pertinents pour le respect et l'application du présent règlement sur la base de l'état de la technique généralement reconnu, y compris tel qu'il ressort des normes harmonisées pertinentes.

Titre VI, Chapitre 2, Titre VII, Titre VIII et considérants 77-80a et 82-82b	CA 9

(77) Chaque État membre devrait désigner une autorité nationale de surveillance chargée de surveiller l'application et la mise en œuvre du présent règlement. Il devrait également représenter son État membre au conseil d'administration de l'Office AI. Afin d'accroître l'efficacité de l'organisation du côté des États membres et d'établir un point de contact officiel vis-à-vis du public et d'autres homologues aux niveaux des États membres et de l'Union.
Chaque autorité nationale de surveillance devrait agir en toute indépendance dans l'accomplissement de ses missions et l'exercice de ses pouvoirs conformément au présent règlement.

(77 bis) Les autorités de contrôle nationales devraient contrôler l'application des dispositions du présent règlement et contribuer à son application cohérente dans toute l'Union. À cette fin, les autorités nationales de surveillance devraient coopérer entre elles, ainsi qu'avec les autorités nationales compétentes concernées, la Commission et l'Office AI.

(77 ter) Le membre ou le personnel de chaque autorité de contrôle nationale devrait, conformément au droit de l'Union ou du droit des États membres, être soumis à une obligation de secret professionnel, tant pendant qu'après leur mandat, à l'égard de toute information confidentielle parvenue à leur connaissance dans le cadre de l'exécution de leurs missions ou de l'exercice de leurs pouvoirs. Pendant leur mandat, cette obligation de secret professionnel devrait notamment s'appliquer aux secrets d'affaires et au signalement par des personnes physiques d'infractions au présent règlement

(78) Afin de garantir que les fournisseurs de systèmes d'IA à haut risque peuvent tenir compte de 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 peuvent prendre toute mesure corrective éventuelle en temps opportun De cette manière, tous les fournisseurs devraient avoir mis en place un système de surveillance post-commercialisation. Ce système est également essentiel pour garantir que les risques éventuels émergeant des systèmes d'IA qui continuent à «apprendre» ou à évoluer après avoir été mis sur le marché ou mis en service peuvent être traités plus efficacement et en temps opportun. Dans ce contexte, les fournisseurs devraient également être tenus de mettre en place un système pour signaler aux autorités compétentes tout incident grave ou toute violation du droit national et de l'Union, y compris ceux protégeant les droits fondamentaux et les droits des consommateurs résultant de l'utilisation de leurs systèmes d'IA et prendre les mesures correctives appropriées. Les déployeurs devraient également signaler aux autorités compétentes tout incident grave ou violation du droit national et de l'Union résultant de l'utilisation de leur système d'IA lorsqu'ils ont connaissance de tels incidents ou violations graves.

(79) Afin d'assurer une mise en œuvre appropriée et efficace des exigences et obligations énoncées par le présent règlement, qui est la législation d'harmonisation de l'Union, le système de surveillance du marché et de conformité des produits établi par le règlement (UE) 2019/1020 devrait s'appliquer dans son intégralité. Aux fins du présent règlement, les autorités de surveillance nationales devraient agir en tant qu'autorités de surveillance du marché pour les systèmes d'IA couverts par le présent règlement, à l'exception des systèmes d'IA couverts par l'annexe II du présent règlement. Pour les systèmes d'IA couverts par des actes juridiques énumérés à l'annexe II, les autorités compétentes en vertu de ces actes juridiques devraient rester l'autorité chef de file. Les autorités nationales de surveillance et les autorités compétentes dans la législation énumérée à l'annexe II devraient collaborer chaque fois que nécessaire. Le cas échéant, les autorités compétentes

Les autorités compétentes de la législation énumérée à l'annexe II devraient envoyer du personnel compétent à l'autorité de contrôle nationale afin de l'assister dans l'accomplissement de ses tâches. Aux fins du présent règlement, les autorités nationales de surveillance devraient avoir les mêmes pouvoirs et obligations que les autorités de surveillance du marché en vertu du règlement (UE) 2019/1020. Lorsque cela est nécessaire pour leur mandat, les autorités ou organismes publics nationaux qui surveillent l'application du droit de l'Union protégeant les droits fondamentaux, y compris les organismes de promotion de l'égalité, devraient également avoir accès à toute documentation créée en vertu du présent règlement. Après avoir épuisé tous les autres moyens raisonnables d'évaluer/vérifier la conformité et sur demande motivée, l'autorité de contrôle nationale devrait se voir accorder l'accès aux ensembles de données de formation, de validation et d'essai, au modèle formé et de formation du système d'IA à haut risque, y compris ses paramètres de modèle pertinents et leur environnement d'exécution/d'exécution. Dans le cas de systèmes logiciels plus simples relevant du présent règlement qui ne sont pas basés sur des modèles entraînés, et lorsque tous les autres moyens de vérifier la conformité ont été épuisés, l'autorité de contrôle nationale peut exceptionnellement avoir accès au code source, sur demande motivée. Lorsque l'autorité de contrôle nationale s'est vu accorder l'accès aux ensembles de données de formation, de validation et d'essai conformément au présent règlement, cet accès devrait être obtenu au moyen de moyens et d'outils techniques appropriés, y compris un accès sur place et, dans des circonstances exceptionnelles, un accès à distance. L'autorité de contrôle nationale devrait traiter toute information, y compris le code source, les logiciels et les données, le cas échéant, obtenue comme une information confidentielle et respecter le droit de l'Union applicable en matière de protection de la propriété intellectuelle et des secrets d'affaires. L'autorité de contrôle nationale devrait supprimer toute information obtenue à l'issue de l'enquête.

(80) La législation de l'Union sur les services financiers comprend des règles et des exigences en matière de gouvernance interne et de gestion des risques qui sont applicables aux établissements financiers réglementés dans le cadre de la fourniture de ces services, y compris lorsqu'ils utilisent des systèmes d'intelligence artificielle. Afin d'assurer une application et une mise en œuvre cohérentes des obligations prévues par le présent règlement et des règles et exigences pertinentes de la législation de l'Union sur les services financiers, les autorités compétentes chargées de la surveillance et de l'application de la législation sur les services financiers, y compris, le cas échéant, la Banque centrale européenne, devraient être désignées comme autorités compétentes aux fins de surveiller la mise en œuvre du présent règlement, y compris pour les activités de surveillance du marché, en ce qui concerne les systèmes d'intelligence artificielle fournis ou utilisés par des établissements financiers réglementés et surveillés. Afin de renforcer encore la cohérence entre le présent règlement et les règles applicables aux établissements de crédit réglementés en vertu de la directive 2013/36/UE du Parlement européen et du Conseil[7], il convient également d'intégrer la procédure d'évaluation de la conformité et certaines des obligations procédurales des prestataires dans concernant la gestion des risques, la surveillance post-commercialisation et la documentation dans les obligations et procédures existantes en vertu de la directive 2013/36/UE. Afin d'éviter les chevauchements, des dérogations limitées devraient également être envisagées en ce qui concerne le système de gestion de la qualité des prestataires et l'obligation de surveillance imposée aux déployeurs de systèmes d'IA à haut risque dans la mesure où ceux-ci s'appliquent aux établissements de crédit régis par la directive 2013/36/ UE.

[7] 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).

(80 bis) Compte tenu des objectifs du présent règlement, à savoir assurer un niveau équivalent de protection de la santé, de la sécurité et des droits fondamentaux des personnes physiques, assurer la protection de l'État de droit et de la démocratie, et compte tenu du fait que l'atténuation de la les risques du système d'IA à l'encontre de ces droits peuvent ne pas être suffisamment pris en compte au niveau national ou peuvent faire l'objet d'interprétations divergentes qui pourraient finalement conduire à un niveau inégal de protection des personnes physiques et créer une fragmentation du marché, les autorités nationales de surveillance devraient être habilitées à mener des actions conjointes enquêtes ou se prévaloir de la procédure de sauvegarde syndicale prévue par le présent règlement pour une application efficace. Des enquêtes conjointes devraient être ouvertes lorsque l'autorité de contrôle nationale a des raisons suffisantes de croire qu'une infraction au présent règlement constitue une infraction de grande ampleur ou une infraction de grande ampleur de dimension européenne, ou lorsque le système d'IA ou le modèle de fondation présente un risque qui affecte ou est susceptible d'affecter au moins 45 millions de personnes dans plus d'un État membre.

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

(84 bis) Étant donné que les droits et libertés des personnes physiques et morales et des groupes de personnes physiques peuvent être gravement compromis par les systèmes d'IA, il est essentiel que les personnes physiques et morales ou les groupes de personnes physiques aient un accès significatif aux mécanismes de signalement et de recours et soient droit d'accéder à des recours proportionnés et efficaces. Ils devraient pouvoir signaler les infractions au présent règlement à leur autorité de contrôle nationale et avoir le droit de porter plainte contre les fournisseurs ou les déployeurs de systèmes d'IA. Le cas échéant, les déployeurs devraient fournir des mécanismes de plainte internes à l'usage des personnes physiques et morales ou des groupes de personnes physiques. Sans préjudice de tout autre recours administratif ou non judiciaire, les personnes physiques et morales et les groupes de personnes physiques devraient également avoir droit à un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité nationale de contrôle les concernant ou, lorsque la l'autorité de contrôle ne traite pas une plainte, n'informe pas le plaignant de l'état d'avancement ou du résultat préliminaire de la plainte déposée ou ne respecte pas son obligation de prendre une décision définitive concernant la plainte.

(84 ter) Les personnes concernées devraient toujours être informées qu'elles sont soumises à l'utilisation d'un système d'IA à haut risque, lorsque les déployeurs utilisent un système d'IA à haut risque pour aider à la prise de décision ou prendre des décisions concernant des personnes physiques. Ces informations peuvent servir de base aux personnes concernées pour exercer leur droit à une explication en vertu du présent règlement. Lorsque les déployeurs fournissent une explication aux personnes concernées en vertu du présent règlement, ils devraient tenir compte du niveau d'expertise et de connaissances du consommateur moyen ou de l'individu

(84 quater) La législation de l'Union relative à la protection des lanceurs d'alerte [directive (UE) 2019/1937] s'applique pleinement aux universitaires, concepteurs, développeurs, contributeurs de projets, auditeurs, chefs de produit, ingénieurs et opérateurs économiques qui obtiennent des informations sur des violations du droit de l'Union par un fournisseur du système d'IA ou de son système d'IA.

CHAPITRE 2

AUTORITÉS NATIONALES COMPÉTENTES

Article 59

Désignation des autorités nationales de surveillance

1. Chaque État membre désigne une autorité de contrôle nationale, qui est organisée de manière à garantir l'objectivité et l'impartialité de ses activités et missions au plus tard le [3 mois après l'entrée en vigueur du présent règlement].

2. L'autorité de contrôle nationale veille à l'application et à la mise en œuvre du présent règlement. En ce qui concerne les systèmes d'IA à haut risque, liés aux produits auxquels s'appliquent les actes juridiques énumérés à l'annexe II, les autorités compétentes désignées en vertu de ces actes juridiques continuent de diriger les procédures administratives. Toutefois, dans la mesure où une affaire concerne des aspects exclusivement couverts par le présent règlement, ces autorités compétentes sont liées par les mesures relatives à ces aspects émises par l'autorité de contrôle nationale désignée en vertu du présent règlement. L'autorité nationale de surveillance agit en qualité d'autorité de surveillance du marché.

3. Les États membres mettent à la disposition du public et communiquent à l'Office AI et à la Commission l'autorité nationale de contrôle et les informations sur la manière de la contacter, au plus tard le ... [trois mois après l'entrée en vigueur du présent règlement]. L'autorité nationale de contrôle fait office de point de contact unique pour le présent règlement et devrait pouvoir être contactée par des moyens de communication électroniques.

4. Les États membres veillent à ce que l'autorité nationale de surveillance soit dotée des ressources techniques, financières et humaines et de l'infrastructure nécessaires pour s'acquitter efficacement de ses missions au titre du présent règlement. En particulier, l'autorité de contrôle nationale dispose en permanence d'un nombre suffisant d'agents dont les compétences et l'expertise incluent une connaissance approfondie des technologies de l'intelligence artificielle, des données et de l'informatique, de la protection des données à caractère personnel, de la cybersécurité, du droit de la concurrence, des droits fondamentaux, de la santé et les risques de sécurité et la connaissance des normes existantes et des exigences légales. Les États membres évaluent et, si nécessaire, mettent à jour les exigences en matière de compétences et de ressources visées au présent paragraphe sur une base annuelle.

4a. Chaque autorité de contrôle nationale exerce ses pouvoirs et s'acquitte de ses fonctions de manière indépendante, impartiale et impartiale. Les membres de chaque autorité nationale de surveillance, dans l'accomplissement de leurs missions et l'exercice des pouvoirs qui leur sont conférés par le présent règlement, ne sollicitent ni n'acceptent d'instructions d'aucun organisme

4b. Les autorités de contrôle nationales satisfont aux exigences minimales en matière de cybersécurité fixées pour les entités de l'administration publique identifiées comme opérateurs de services essentiels conformément à la directive XXXX/XX concernant des mesures visant à assurer un niveau commun élevé de cybersécurité dans l'Union (NIS 2), abrogeant la directive (UE) 2016 /1148.

4c. Dans l'accomplissement de ses missions, l' autorité nationale de contrôle agit en le respect des obligations de confidentialité prévues à l'article 70.

5. Les États membres font annuellement rapport à la Commission sur l'état des ressources financières et humaines de l'autorité nationale de surveillance, avec une évaluation de leur adéquation. La Commission transmet ces informations au Bureau AI pour discussion et recommandations éventuelles.

6. ~~L'Office AI facilite l'échange d'expériences entre les autorités nationales de surveillance compétentes.~~

7. Les autorités de surveillance nationales peuvent fournir des orientations et des conseils sur la mise en œuvre du présent règlement, y compris aux PME et aux start-up , en tenant compte des orientations et conseils de l'Office AI ou de la Commission . Chaque fois que les autorités de contrôle nationales ont l'intention de fournir des orientations et des conseils concernant un système d'IA dans des domaines couverts par une autre législation de l'Union, les orientations sont rédigées en consultation avec les autorités nationales compétentes en vertu de cette législation de l'Union, le cas échéant. ~~Les États membres peuvent également établir un point de contact central pour la communication~~ avec les opérateurs

8. Lorsque les institutions, agences et organes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données agit en tant qu'autorité compétente pour leur contrôle et leur coordination .

Article 59a

Mécanisme de coopération entre les autorités nationales de surveillance dans les cas impliquant deux ou plus d'États membres

1. Chaque autorité nationale de surveillance exerce les missions et pouvoirs qui lui sont conférés conformément au présent règlement sur le territoire de son propre État membre.

2. Dans le cas d'une affaire impliquant deux ou plusieurs autorités de contrôle nationales, l'autorité de contrôle nationale de l'État membre où l'infraction a eu lieu est considérée comme l'autorité de contrôle chef de file.

3. Dans les cas visés au paragraphe 2, les autorités de contrôle compétentes coopèrent et échangent toutes les informations pertinentes en temps utile. Les autorités nationales de surveillance coopèrent afin de parvenir à un consensus.

TITRE VII

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

Article 60

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

1. La Commission, en collaboration avec les États membres, crée et gère une base de données publique de l'UE contenant les informations visées aux paragraphes 2 et 2 bis concernant les systèmes d'IA à haut risque visés à l'article 6, paragraphe 2, qui sont enregistrés conformément à l'article 51 .

2. Les données énumérées à l'annexe VIII, section A, sont saisies dans la base de données de l'UE par les fournisseurs. La Commission leur apporte un soutien technique et administratif.

2a. Les données énumérées à l'annexe VIII, section B, sont introduites dans la base de données de l'UE par les déployeurs qui sont ou qui agissent pour le compte d'autorités publiques ou d'institutions, organes, offices ou agences de l'Union et par les déployeurs qui sont des entreprises visées à l'article 51 (1a) et (1b).

3. Les informations contenues dans la base de données de l'UE sont librement accessibles au public, conviviales et accessibles, facilement navigables et lisibles par machine et contiennent des données numériques structurées basées sur un protocole normalisé.

4. La base de données de l'UE ne contient des données à caractère personnel que dans la mesure nécessaire à la collecte et au traitement des informations conformément au présent règlement. Ces informations comprennent les noms et les coordonnées des personnes physiques qui sont responsables de l'enregistrement du système et qui sont légalement habilitées à représenter le fournisseur ou le déployeur qui est une autorité publique ou une institution, un organe, un office ou une agence de l'Union ou un déployeur agissant sur pour leur compte ou un déployeur qui est une entreprise visée à l'article 51, paragraphe 1 bis, points b) et 1 ter).

5. La Commission est le responsable du traitement de la base de données de l'UE. Il doit également assurer aux fournisseurs et aux déployeurs un soutien technique et administratif adéquat.

5a. La base de données est conforme aux exigences d'accessibilité de l'annexe I du Directive 2019/882

TITRE VIII

SUIVI POST-MISE SUR LE MARCHÉ, PARTAGE DE L'INFORMATION, MARCHÉ SURVEILLANCE

CHAPITRE 1

SUIVI POST-MISE SUR LE MARCHÉ

Article 61

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

1. Les fournisseurs établissent et documentent un système de surveillance post-commercialisation d'une manière proportionnée à la nature des technologies d'intelligence artificielle et aux risques du système d'IA à haut risque.

2. Le système de surveillance post-commercialisation collecte, documente et analyse activement et systématiquement les données pertinentes fournies par les déployeurs ou collectées par d'autres sources sur les performances des systèmes d'IA à haut risque tout au long de leur durée de vie, et permet au fournisseur d'évaluer la conformité continue des systèmes d'IA. aux exigences énoncées au titre III, chapitre 2. Le cas échéant, la surveillance après commercialisation comprend une analyse de l'interaction avec l'environnement d'autres systèmes d'IA,

y compris d'autres appareils et logiciels en tenant compte des règles applicables dans des domaines tels que la protection des données, les droits de propriété intellectuelle et le droit de la concurrence.

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 établissant des dispositions détaillées établissant un modèle de plan de surveillance après commercialisation et la liste des éléments à inclure dans le plan au plus tard le [12 mois après l'entrée en vigueur].

4. Pour les systèmes d'IA à haut risque couverts par les actes juridiques visés à l'annexe II, lorsqu'un système et un plan de surveillance après commercialisation sont déjà établis en vertu de cette législation, les éléments décrits aux paragraphes 1, 2 et 3 sont intégrés dans ce système et planifier le cas échéant.

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

CHAPITRE 2

PARTAGE DES INFORMATIONS SUR LES INCIDENTS ET LES DYSFONCTIONNEMENTS

Article 62

Signalement des incidents graves et ~~des dysfonctionnements~~

1. Les fournisseurs et, lorsque les déployeurs ont identifié un incident grave, les déployeurs de systèmes d'IA à haut risque mis sur le marché de l'Union signalent tout incident grave ou tout dysfonction~~nement de ces systèmes qu~~i constitue une violation des obligations prévues par le droit de l'Union visant à protéger les droits fondamentaux de l'État l'autorité de contrôle de l'État membre où cet incident ou cette infraction s'est produit.

Cette notification est faite sans retard in~~j~~ustifié après que le fournisseur, ou le cas échéant le déployeur, a établi un lien de causalité entre le système d'IA et l'incident ou le dysfonctionnement ou la probabilité raisonnable ~~d'un tel lien, et, en to~~ut état de cause, au plus tard le 15 jours 72 heures (après que les prestataires ou, le cas é~~chéant, le~~ déployeur ont pris connaissance d~~e l'i~~ncident grave ou du dysfonctionnement.

1a. Après avoir établi un lien de causalité entre le système d'IA et l'incident grave ou la probabilité raisonnable d'un tel lien, les fournisseurs prennent les mesures correctives appropriées conformément à l'article 21.

2. Dès réception d'une notification relative à une violation des obligations prévues par le droit de l'Union visant à protéger les droits fondamentaux, l'autorité nationale de contrôle informe les autorités ou organismes publics nationaux visés à l'article 64, paragraphe 3. La Commission élabore des orientations spécifiques pour faciliter le respect des obligations énoncées au paragraphe 1. Ces orientations sont publiées au plus tard le [l'entrée en vigueur du présent règlement] et sont évaluées régulièrement.

2a. L'autorité de contrôle nationale prend les mesures appropriées dans un délai de sept jours à compter de la date à laquelle elle a reçu la notification visée au paragraphe 1. Lorsque l'infraction a lieu ou est susceptible d'avoir lieu dans d'autres États membres, l'autorité nationale

l'autorité de contrôle en informe l'Office AI et les autorités de contrôle nationales compétentes de ces États membres.

3. 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 soumis à des instruments législatifs de l'Union prévoyant des obligations de déclaration équivalentes à celles prévues dans le présent règlement, la notification des incidents graves constituant une infraction des droits fondamentaux en vertu du droit de l'Union sont transférés à l'autorité de contrôle nationale

3a. Les autorités nationales de surveillance notifient chaque année à l'Office AI les incidents graves qui leur sont signalés conformément au présent article.

CHAPITRE 3

MISE EN VIGUEUR

Article 63

Surveillance du marché et contrôle des systèmes d'IA sur le marché de l'Union Le

1. règlement (UE) 2019/1020 s'applique aux systèmes d'IA et aux modèles de base couverts par le présent règlement. Toutefois, aux fins de l'application effective du présent règlement :

a) toute référence à un opérateur économique au titre du règlement (UE) 2019/1020 s'entend comme incluant tous les opérateurs identifiés au titre III, chapitre 3, du présent Régulation;

b) toute référence à un produit au titre du règlement (UE) 2019/1020 s'entend comme incluant tous les systèmes d'IA relevant du champ d'application du présent règlement.

b bis) les autorités nationales de surveillance agissent en tant qu'autorités de surveillance du marché en vertu du présent règlement et ont les mêmes pouvoirs et obligations que les autorités de surveillance du marché en vertu du règlement (UE) 2019/1020.

2. L'autorité nationale de surveillance rend compte chaque année à la Commission et à l'Office AI des résultats des activités de surveillance du marché pertinentes. L'autorité nationale de surveillance communique sans délai à la Commission et aux autorités nationales de concurrence compétentes toute information identifiée au cours des activités de surveillance du marché qui pourrait présenter un intérêt potentiel pour l'application du droit de l'Union relatif aux règles de concurrence.

3. Pour les systèmes d'IA à haut risque, liés aux produits auxquels s'appliquent les actes juridiques énumérés à l'annexe II, section A, l'autorité de surveillance du marché aux fins du présent règlement est l'autorité responsable des activités de surveillance du marché désignée en vertu de ces actes juridiques.

3a. Aux fins d'assurer l'application effective du présent règlement, les autorités nationales de surveillance peuvent:

(un) Effectuer des inspections inopinées sur place et à distance des systèmes d'IA ;

(b) Acquérir des échantillons liés aux systèmes d'IA à haut risque, y compris par le biais d'inspections à distance, pour rétroconcevoir les systèmes d'IA et acquérir des preuves pour identifier la non-conformité.

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

5. Pour les systèmes d'IA qui sont utilisés à des fins répressives, points 6 et 7 de l'annexe III, les États membres désignent comme autorités de surveillance du marché aux fins du présent règlement soit les autorités de contrôle compétentes en matière de protection des données en vertu de la directive (UE) 2016/680, soit Règlement 2016/679 ou les autorités nationales compétentes supervisant les activités des autorités répressives, de l'immigration ou de l'asile mettant en service ou utilisant ces systèmes.

6. Lorsque les institutions, agences et organes de l'Union relèvent du champ d'application du présent règlement, le Contrôleur européen de la protection des données agit en tant qu'autorité de surveillance du marché.

7. Les autorités nationales de surveillance désignées en vertu du présent règlement assurent la coordination avec les autres autorités ou organismes nationaux compétents qui surveillent l'application de la législation d'harmonisation de l'Union énumérée à l'annexe II ou d'autres actes législatifs de l'Union qui pourraient être pertinents pour les systèmes d'IA à haut risque visés à l'annexe III.

Article 64
Accès aux données et à la documentation

1. Dans le cadre de leurs activités, et sur demande motivée, l'autorité de contrôle nationale se voit accorder un accès complet aux ensembles de données de formation, de validation et de test utilisés par le fournisseur ou, le cas échéant, le déployeur, qui sont pertinents et strictement nécessaires aux fins de sa demande par le biais d'interfaces de programmation d'application (« API ») ou d'autres moyens et outils techniques appropriés permettant un accès à distance.

2. S'il est nécessaire d'évaluer la conformité du système d'IA à haut risque avec les exigences énoncées au titre III, chapitre 2, après que tous les autres moyens raisonnables de vérifier la conformité, y compris le paragraphe 1, ont été épuisés et se sont révélés insuffisants, et sur avis motivé demande, l'autorité de surveillance nationale se voit accorder l'accès à la formation et aux modèles formés du système d'IA, y compris ses paramètres de modèle pertinents. Toutes les informations obtenues conformément à l'article 70 sont traitées comme des informations confidentielles et sont soumises au droit de l'Union en vigueur sur la protection de la propriété intellectuelle et des secrets d'affaires et sont supprimées à l'issue de l'enquête pour laquelle les informations ont été demandées.

2a. Les paragraphes 1 et 2 sont sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020.

3. Les autorités ou organismes publics nationaux qui surveillent ou font respecter les obligations découlant du droit de l'Union protégeant les droits fondamentaux en ce qui concerne l'utilisation de systèmes d'IA à haut risque visés à l'annexe III ont le pouvoir de demander et d'accéder à toute documentation créée ou conservée en vertu du présent règlement lorsque l'accès à cette documentation est nécessaire à l'exercice des compétences relevant de leur

mandat dans les limites de leur compétence. L'autorité ou l'organisme public compétent informe l'autorité de contrôle nationale de l'État membre concerné d'une telle demande.

4. Au plus tard trois mois après l'entrée en vigueur du présent règlement, chaque État membre identifie les autorités ou organismes publics visés au paragraphe 3 et met une liste à la disposition du public sur le site internet de l'autorité nationale de surveillance. Les autorités nationales de surveillance notifient la liste à la Commission, à l'Office AI et à toutes les autres autorités nationales de surveillance et tiennent la liste à jour. La Commission publie sur un site internet dédié la liste de toutes les autorités compétentes désignées par les États membres conformément au présent article.

5. Lorsque la documentation visée au paragraphe 3 est insuffisante pour établir s'il y a eu manquement aux obligations découlant du droit de l'Union visant à protéger les droits fondamentaux, l'autorité ou l'organisme public visé au paragraphe 3 peut adresser une demande motivée à l'autorité nationale de contrôle afin d'organiser tester le système d'IA à haut risque par des moyens techniques. L'autorité nationale de contrôle organise le test avec la participation étroite de l'autorité ou de l'organisme public demandeur dans un délai raisonnable suivant la demande.

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

Article 65

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

1. Par systèmes d'IA présentant un risque, on entend un système d'IA susceptible de nuire à la santé et à la sécurité, aux droits fondamentaux des personnes en général, y compris sur le lieu de travail, à la protection des consommateurs, à l'environnement, à la sécurité publique, à la démocratie ou à l'État de droit et d'autres intérêts publics, qui sont protégés par la législation d'harmonisation de l'Union applicable, dans une mesure qui va au-delà de ce qui est considéré comme raisonnable et acceptable au regard de sa destination ou dans les conditions normales ou raisonnablement prévisibles d'utilisation du système, y compris la durée d'utilisation et, le cas échéant, ses exigences de mise en service, d'installation et d'entretien.

2. Lorsque l'autorité de surveillance nationale d'un État membre a des raisons suffisantes de considérer qu'un système d'IA présente un risque tel que visé au paragraphe 1, elle procède à une évaluation du système d'IA concerné en ce qui concerne sa conformité avec toutes les exigences et obligations prévues dans le présent règlement. Lorsque des risques pour la protection des droits fondamentaux sont présents, l'autorité de contrôle nationale informe également immédiatement et coopère pleinement avec les autorités ou organismes publics nationaux concernés visés à l'article 64, paragraphe 3. Lorsqu'il existe des raisons suffisantes de considérer qu'un système d'IA exploite les vulnérabilités de groupes vulnérables ou viole leurs droits intentionnellement ou non, l'autorité nationale de surveillance est tenue d'enquêter sur les objectifs de conception, les entrées de données, la sélection de modèles, la mise en œuvre et les résultats des le système d'IA. Les opérateurs concernés coopèrent en tant que de besoin avec l'autorité de contrôle nationale et les autres autorités ou organismes publics nationaux visés à l'article 64, paragraphe 3.

Lorsque, au cours de cette évaluation, l'autorité de contrôle nationale ou, le cas échéant, l'autorité publique nationale visée à l'article 64, paragraphe 3, constate que l'AI

système ne respecte pas les exigences et les obligations énoncées dans le présent règlement, il exige sans délai de l'opérateur concerné qu'il prenne toutes les mesures correctives appropriées pour mettre le système d'IA en conformité, pour retirer le système d'IA du marché ou pour le rappeler dans un délai raisonnable, proportionné à la nature du risque, qu'il peut prescrire et, en tout état de cause, au plus tard 15 jours ouvrables ou conformément à la législation d'harmonisation de l'Union applicable, le cas échéant

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

3. Lorsque l'autorité de contrôle nationale estime que la non-conformité n'est pas limitée à son territoire national, elle informe sans délai la Commission, l'Office AI et l'autorité de contrôle nationale des autres États membres des résultats de l'évaluation et des actions qu'il a demandé à l'opérateur de prendre.

4. L'opérateur veille à ce que toutes les mesures correctives appropriées soient prises pour tous les systèmes d'IA concernés qu'il a mis à disposition sur le marché dans toute l'Union.

5. Lorsque l'opérateur d'un système d'IA ne prend pas de mesures correctives adéquates dans le délai visé au paragraphe 2, l'autorité de contrôle nationale 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 , de retirer le système d'IA de ce marché ou de le rappeler. Cette autorité informe immédiatement et sans délai la Commission, l'Office AI et l'autorité de contrôle nationale des autres États membres de ces mesures.

———————

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

(a) un échec du système d'IA à haut risque à satisfaire aux exigences énoncées dans le présent Régulation;

b) les lacunes des normes harmonisées ou des spécifications communes visées aux articles 40 et 41 conférant une présomption de conformité. (b bis) non-respect

de l'interdiction des pratiques d'intelligence artificielle visée à l'article 5;

bb) non-respect des dispositions énoncées à l'article 52

7. Les autorités nationales de contrôle des États membres autres que l'autorité nationale de contrôle de l'État membre qui engage la procédure informent sans délai la Commission, l'Office AI et les autres États membres de toute mesure adoptée et de toute information complémentaire dont elles disposent concernant de la non-conformité du système d'IA concerné et, en cas de désaccord avec la mesure nationale notifiée, de leurs objections.

8. Lorsque, dans les trois mois suivant la réception des informations visées au paragraphe 5, aucune objection n'a été soulevée par une autorité nationale de contrôle d'un État membre ou par la Commission à l'égard d'une mesure provisoire prise par une autorité nationale de contrôle d'un autre État membre , cette mesure est réputée justifiée. Ceci est sans préjudice des droits procéduraux de l'opérateur concerné conformément à l'article 18 du règlement (UE) 2019/1020. Le délai visé à la première phrase du présent alinéa est ramené à 30 jours en cas de non-respect de l'interdiction des pratiques d'intelligence artificielle visée à l'article 5.

9. Les autorités nationales de surveillance de tous les États membres veillent à ce que des mesures restrictives appropriées soient prises à l'égard du système d'IA concerné, telles que le retrait du système d'IA de leur marché, sans délai.

9a. Les autorités nationales de surveillance rendent compte chaque année à l'Office AI de l'utilisation de pratiques interdites survenues au cours de l'année et des mesures prises pour éliminer ou atténuer les risques conformément au présent article.

Article 66

Procédure de sauvegarde de l'Union

1. Lorsque, dans les trois mois suivant la réception de la notification visée à l'article 65, paragraphe 5, ou dans les 30 jours en cas de non-respect de l'interdiction des pratiques d'intelligence artificielle visée à l'article 5, des objections sont soulevées par l'autorité nationale de surveillance d'un État membre contre une mesure prise par une autre autorité de contrôle nationale, ou dans les cas visés à l'article 59 bis, paragraphe 4, ou lorsque la Commission considère que la mesure est contraire au droit de l'Union, la Commission engage sans délai une consultation avec l'autorité de surveillance nationale de l'État membre et de l'opérateur ou des opérateurs concernés et évalue la mesure nationale. Sur la base des résultats de cette évaluation, la Commission décide si la mesure nationale est justifiée ou non dans un délai de trois mois, ou de 60 jours en cas de non-respect de l'interdiction des pratiques d'intelligence artificielle visée à l'article 5, à compter de la notification visée à l'article 65, paragraphe 5, et notifie cette décision à l'autorité de contrôle nationale de l'État membre concerné. La Commission informe également toutes les autres autorités nationales de surveillance de cette décision.

2. Si la mesure nationale est jugée justifiée, toutes les autorités nationales de surveillance désignées en vertu du présent règlement prennent les mesures nécessaires pour garantir que le système d'IA non conforme est retiré sans délai de leur marché et en informent la Commission et l'Office de l'IA. Si la mesure nationale est considérée comme injustifiée, l'autorité de contrôle nationale de l'État membre concerné retire la mesure.

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

.

Article 66 bis

Enquêtes conjointes

1. Lorsqu'une autorité de contrôle nationale a des raisons de soupçonner que l'infraction par un fournisseur ou un déployeur d'un système d'IA à haut risque ou d'un modèle de base au présent règlement constitue une infraction généralisée de dimension européenne, ou affecte ou est susceptible d'affecter au moins 45 millions de personnes, dans plus d'un État membre, cette autorité de contrôle nationale en informe l'Office AI et peut demander aux autorités de contrôle nationales des États membres où l'infraction a eu lieu d'ouvrir une enquête conjointe. Le bureau AI assure la coordination centrale de l'enquête conjointe. Les pouvoirs d'enquête restent du ressort des autorités nationales de contrôle.

Article 67

Systèmes d'IA conformes qui présentent un risque

1. Lorsque, après avoir effectué une évaluation au titre de l'article 65, en pleine coopération avec l'autorité publique nationale compétente visée à l'article 64, paragraphe 3, l'autorité de contrôle nationale d'un État membre constate que, bien qu'un système d'IA soit conforme au présent règlement, il présente un risque grave pour la santé ou la sécurité des personnes, pour le respect des obligations découlant du droit de l'Union ou du droit national visant à protéger les droits fondamentaux, ou l'environnement ou la démocratie et l'État de droit ou pour d'autres aspects de la protection de l'intérêt public , il exige à l'opérateur concerné de prendre toutes les mesures appropriées pour que le système d'IA concerné, lors de sa mise sur le marché ou de sa mise en service, ne présente plus ce risque, de retirer le système d'IA du marché ou de le rappeler dans un délai raisonnable, proportionnée à la nature du risque, comme elle peut le prescrire.

2. Le fournisseur ou les autres opérateurs concernés veillent à ce que des mesures correctives soient prises à l'égard de tous les systèmes d'IA concernés qu'ils ont mis à disposition sur le marché dans toute l'Union dans le délai prescrit par l'autorité de surveillance nationale de l'État membre visé au paragraphe 1 .

2a. Lorsque le fournisseur ou d'autres opérateurs concernés ne prennent pas les mesures correctives visées au paragraphe 2 et que le système d'IA continue de présenter un risque tel que visé au paragraphe 1, l'autorité de contrôle nationale peut demander à l'opérateur concerné de retirer le système d'IA du marché ou de le rappeler dans un délai raisonnable, proportionné à la nature du risque.

3. L'autorité nationale de contrôle informe immédiatement la Commission, l'Office AI et les autres autorités nationales de contrôle. Ces informations comprennent tous les détails disponibles, notamment les données nécessaires à l'identification du système d'IA concerné, l'origine et la chaîne d'approvisionnement du système d'IA, la nature du risque encouru ainsi que la nature et la durée des mesures nationales prises.

4. La Commission, en consultation avec l'Office AI, entre sans délai en consultation avec les autorités nationales de surveillance concernées et l'opérateur concerné et évalue les mesures nationales prises. Sur la base des résultats de cette évaluation, l'Office AI décide si la mesure est justifiée ou non et, le cas échéant, propose des mesures appropriées.

5. La Commission, en consultation avec l'Office AI, communique immédiatement sa décision aux autorités nationales de surveillance des États membres concernés.

et aux opérateurs concernés. Elle informe également de sa décision toutes les autres autorités nationales de surveillance.

5a. La Commission adopte des lignes directrices pour aider les autorités nationales compétentes à identifier et à rectifier, si nécessaire, des problèmes similaires survenant dans d'autres systèmes d'IA.

Article 68

Non-conformité formelle

1. Lorsque l'autorité de contrôle nationale d'un État membre fait l'une des constatations suivantes, elle demande au prestataire concerné de mettre fin à la non-conformité concernée :

a) le marquage CE a été apposé en violation de l'article 49; (b) le marquage CE n'a pas été apposé; c) la déclaration UE de conformité n'a pas été établie; d) la déclaration UE de conformité n'a pas été établie correctement; e) le numéro d'identification de l'organisme notifié qui participe à la procédure d'évaluation de la conformité, le cas échéant, n'a pas été apposé;

(ea) la documentation technique n'est pas disponible ;

eb) l'enregistrement dans la base de données de l'UE n'a pas été effectué.

(ec) le cas échéant, le mandataire n'a pas été désigné.

2. Lorsque la non-conformité visée au paragraphe 1 persiste, l'autorité de contrôle nationale de l'État membre concerné prend toutes les mesures appropriées et proportionnées pour restreindre ou interdire la mise à disposition sur le marché du système d'IA à haut risque ou pour assurer son rappel ou retirés du marché sans délai. L'autorité de contrôle nationale de l'État membre concerné informe immédiatement l'Office AI du non-respect et des mesures prises.

Chapitre 3a Recours

Article 68 bis

Droit d'introduire une réclamation auprès d'une autorité de contrôle nationale

1. Sans préjudice de tout autre recours administratif ou judiciaire, toute personne physique ou groupe de personnes physiques a le droit d'introduire une réclamation auprès d'une autorité nationale de contrôle, notamment dans l'État membre de sa résidence habituelle, de son lieu de travail ou de son lieu de l'infraction alléguée s'ils estiment que le système d'IA le concernant enfreint le présent règlement.

2. L'autorité de contrôle nationale auprès de laquelle la plainte a été déposée informe le plaignant de l'état d'avancement et de l'issue de la plainte, y compris de la possibilité d'un recours juridictionnel conformément à l'article 78.

Article 68b

Droit à un recours juridictionnel effectif contre une autorité de contrôle Sans

1. préjudice de tout autre recours administratif ou non judiciaire, toute personne physique ou morale a droit à un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité nationale de contrôle la concernant.

2. Sans préjudice de tout autre recours administratif ou non judiciaire, toute personne physique ou morale a droit à un recours juridictionnel effectif lorsque l'autorité nationale de contrôle compétente en vertu de l'article 59 ne traite pas une réclamation ou ne communique pas les données informé dans un délai de trois mois de l'état d'avancement ou de l'issue de la réclamation introduite en vertu de l'article 68 bis.

3. Les actions contre une autorité nationale de contrôle sont portées devant les juridictions de l'État membre dans lequel l'autorité nationale de contrôle est établie.

4. Lorsqu'un recours est formé contre une décision d'une autorité nationale de contrôle qui a été précédée d'un avis ou d'une décision de la Commission dans le cadre de la procédure de sauvegarde de l'Union, l'autorité de contrôle transmet cet avis ou cette décision au tribunal.

Article 68c

Un droit à l'explication de la prise de décision individuelle

1. Toute personne concernée faisant l'objet d'une décision prise par le déployeur sur la base des résultats d'un système d'IA à haut risque qui produit des effets juridiques ou l'affecte de manière significative de manière similaire d'une manière qu'elle considère comme préjudiciable à sa santé , la sécurité, les droits fondamentaux, le bien-être socio-économique ou tout autre droit découlant des obligations prévues par le présent règlement, a le droit de demander au déployeur des explications claires et significatives conformément à l'article 13, paragraphe 1, sur la rôle du système d'IA dans la procédure de prise de décision, les principaux paramètres de la décision prise et les données d'entrée associées.

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 au paragraphe 1 découlent du droit de l'Union ou du droit national sont prévues dans la mesure où ces exceptions ou restrictions respectent l'essence des libertés et droits fondamentaux et est une mesure nécessaire et proportionnée dans une société démocratique.

3. Le présent article s'applique sans préjudice des articles 13, 14, 15 et 22 du Règlement 2016/679

Article 68d

Actions représentatives

Le texte suivant est ajouté à l'annexe I de la directive (UE) 2020/1828 relative aux actions représentatives pour la protection des intérêts collectifs des consommateurs : « Règlement

xxxx/xxxx du Parlement européen et du Conseil établissant des règles harmonisées sur l'intelligence artificielle (loi sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union ».

Article 68

sexies Signalement des infractions et protection des informateurs La directive (UE) 2019/1937 du Parlement européen et du Conseil s'applique au signalement des infractions au présent règlement et à la protection des personnes signalant ces infractions.

Titre III, chapitre 1, annexes II et III et considérants 27 à 41 bis	CA 10

(27) 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 respectent certaines exigences obligatoires. Ces exigences devraient garantir que les systèmes d'IA à haut risque disponibles dans l'Union ou dont la production est utilisée d'une autre manière dans l'Union ne présentent pas de risques inacceptables pour des intérêts publics importants de l'Union tels qu'ils sont reconnus et protégés par le droit de l'Union, y compris les droits fondamentaux, la démocratie, l'État ou la la loi ou l'environnement. Afin d'assurer l'alignement sur la législation sectorielle et d'éviter les doubles emplois, les exigences applicables aux systèmes d'IA à haut risque devraient tenir compte de la législation sectorielle établissant les exigences applicables aux systèmes d'IA à haut risque inclus dans le champ d'application du présent règlement, comme le règlement (UE) 2017/ 745 sur les dispositifs médicaux et le règlement (UE) 2017/746 sur les dispositifs de diagnostic in vitro ou la directive 2006/42/CE sur les machines. Les systèmes d'IA identifiés comme à haut risque devraient être limités à ceux qui ont un impact préjudiciable significatif sur la santé, la sécurité et les droits fondamentaux des personnes dans l'Union, et cette limitation minimise toute restriction potentielle au commerce international, le cas échéant. Compte tenu du rythme rapide du développement technologique, ainsi que des changements potentiels dans l'utilisation des systèmes d'IA, la liste des domaines à haut risque et des cas d'utilisation figurant à l'annexe III devrait néanmoins faire l'objet d'un réexamen permanent au moyen d'une évaluation régulière.

(28) Les systèmes d'IA pourraient avoir une incidence négative sur la santé et la sécurité des personnes, en particulier lorsque ces systèmes fonctionnent comme des composants de sécurité des 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 par ailleurs conformes se retrouvent sur le marché, il est important que les risques pour la sécurité pouvant être générés par un produit dans son ensemble en raison de ses composants numériques, y compris les systèmes d'IA, sont dûment prévenus et atténués. Par exemple, des robots de plus en plus autonomes, que ce soit dans le cadre de la fabrication ou de l'assistance et des soins personnels, devraient pouvoir fonctionner 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 d'aide à la décision humaine doivent être fiables et précis.

(28 bis) L'ampleur de l'impact négatif causé par le système d'IA sur les droits fondamentaux protégés par la charte revêt une importance particulière lors de la classification d'un système d'IA comme étant à haut risque. Ces droits comprennent le droit à la dignité humaine, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'expression et d'information, la liberté de réunion et d'association et la non-discrimination, le droit à l'éducation, la protection des consommateurs, les droits des travailleurs, les droits des personnes handicapées, égalité entre les femmes et les hommes, droits de propriété intellectuelle, droit à un recours effectif et à un procès équitable, droit de la défense et présomption d'innocence, droit à une bonne administration. En plus de ces droits, il est important de souligner que les enfants ont des droits spécifiques tels qu'énoncés à l'article 24 de la Charte de l'UE et dans la Convention des Nations Unies relative aux droits de l'enfant (développés plus en détail dans l'Observation générale n° 25 de la CNUDE en ce qui concerne l'environnement numérique), qui nécessitent tous deux de prendre en compte les vulnérabilités des enfants et de leur fournir la protection et les soins nécessaires à leur bien-être. Le droit fondamental à un niveau élevé de protection de l'environnement

inscrits dans la charte et mis en œuvre dans les politiques de l'Union devraient également être pris en compte lors de l'évaluation de la gravité des dommages qu'un système d'IA peut causer, y compris en ce qui concerne la santé et la sécurité des personnes ou l'environnement.

(29) En ce qui concerne les systèmes d'IA à haut risque qui sont des composants de sécurité de produits, ou qui sont eux-mêmes des produits ou des systèmes relevant du champ d'application du règlement (CE) n° 300/2008 du Parlement européen et du Conseil8 , le règlement (UE) n° 167/2013 du Parlement européen et du Conseil9 , règlement (UE) n° 168/2013 du Parlement européen et du Conseil10, directive 2014/90/UE du Parlement européen et du Conseil11, directive (UE) 2016 /797 du Parlement européen et du Conseil12, règlement (UE) 2018/858 du Parlement européen et du Conseil13, règlement (UE) 2018/1139 du Parlement européen et du Conseil14 et règlement (UE) 2019/ 2144 du Parlement européen et du Conseil15, il convient de modifier ces actes pour garantir que la Commission tienne compte, sur la base des spécificités techniques et réglementaires de chaque secteur, et sans interférer avec la gouvernance existante, l'évaluation de la conformité, mécanismes de surveillance et d'exécution et les autorités qui y sont établies, les exigences obligatoires applicables aux systèmes d'IA à haut risque énoncées dans le présent règlement lors de l'adoption de tout futur acte délégué ou acte d'exécution pertinent sur la base de ces actes.

(30) En ce qui concerne les systèmes d'IA qui sont des composants de sécurité de produits, ou qui sont eux-mêmes des produits, relevant du champ d'application de certaines législations d'harmonisation de l'Union énumérées au l'annexe II du présent règlement, il convient de les classer comme à haut risque au titre du présent

---

8 Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 établissant des 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).

9 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).

dix 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).

11 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).

12 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).

13 Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques destinés à ces véhicules, modifiant le règlement (CE) n° 715/2007 et (CE) no 595/2009 et abrogeant la directive 2007/46/CE (JO L 151 du 14.6.2018, p. 1).

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

15 Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions pour 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 des règlements de la Commission (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65/2012, (UE) n° 130/2012, (UE) n° 347 /2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 (JO L 325 du 16/12/2019, p. 1).

règlement si le produit en question est soumis à la procédure d'évaluation de la conformité afin de garantir le respect des exigences essentielles de sécurité auprès d'un organisme tiers d'évaluation de la conformité conformément à la législation d'harmonisation de l'Union applicable. Ces produits sont notamment des machines, des jouets, des ascenseurs, des équipements et des systèmes de protection destinés à être utilisés dans des atmosphères potentiellement explosives, des équipements radio, des équipements sous pression, des équipements de bateaux de plaisance, des installations de téléphériques, des appareils brûlant des combustibles gazeux, des dispositifs médicaux et des dispositifs médicaux de diagnostic in vitro. dispositifs.

(31) La classification d'un système d'IA comme étant à haut risque conformément au présent règlement ~~ne devrait pas~~ nécessairement signifier que le produit dont le composant de sécurité est le système d'IA, ou le système d'IA lui-même en tant que produit, est considéré comme «à haut risque» en vertu du critères établis dans la législation d'harmonisation de l'Union pertinente qui s'applique au produit. C'est notamment le cas du règlement (UE) 2017/745 du Parlement européen et du Conseil16 et du règlement (UE) 2017/746 du Parlement européen et du Conseil17, où une évaluation de la conformité par une tierce partie est prévue pour les produits à risque et à haut risque.

(32) En ce qui concerne les systèmes d'IA autonomes, c'est-à-dire les systèmes d'IA à haut risque autres que ceux qui sont des composants de sécurité des produits, ou qui sont eux-mêmes des produits et qui sont répertoriés dans l'un des domaines et cas d'utilisation de l'annexe III, il est approprié de les classer comme à haut risque si, compte tenu de leur destination, ils présentent un risque significatif d'atteinte à la santé et à la sécurité ou aux droits fondamentaux des personnes et, lorsque le système d'IA est utilisé comme élément de sécurité d'un infrastructure critique, à l'environnement . Un tel risque significatif de préjudice devrait être identifié en évaluant, d'une part, l'effet de ce risque par rapport à son niveau de gravité, d'intensité, de probabilité d'occurrence et de durée combinés et, d'autre part, si le risque peut affecter un individu, un pluralité de personnes ou un groupe particulier de personnes. Une telle combinaison pourrait par exemple entraîner une forte gravité mais une faible probabilité d'affecter une personne physique, ou une forte probabilité d'affecter un groupe de personnes avec une faible intensité sur une longue période de temps, selon le contexte. L'identification de ces systèmes repose sur la même méthodologie et les mêmes critères que ceux envisagés également pour toute future modification de la liste des systèmes d'IA à haut risque.

(32 bis) Les fournisseurs dont les systèmes d'IA relèvent de l'un des domaines et cas d'utilisation énumérés à l'annexe III et qui considèrent que leur système ne présente pas de risque significatif d'atteinte à la santé, à la sécurité, aux droits fondamentaux ou à l'environnement devraient informer les autorités nationales de surveillance par l'envoi d'une notification motivée. Cela pourrait prendre la forme d'un résumé d'une page des informations pertinentes sur le système d'IA en question, y compris son objectif et pourquoi il ne présenterait pas de risque significatif de préjudice pour la santé, la sécurité, les droits fondamentaux ou l'environnement. La Commission devrait spécifier des critères permettant aux entreprises d'évaluer si leur système présenterait de tels risques, ainsi que développer un modèle standardisé et facile à utiliser pour la notification. Les fournisseurs devraient soumettre la notification le plus tôt possible et en tout état de cause avant la mise sur le marché ou la mise en service du système d'IA, idéalement au stade du développement, et ils devraient être libres de le mettre sur le marché à tout moment. temps

---

16 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 Directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1).

17 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).

après la notification. Toutefois, si l'autorité estime que le système d'IA en question a été mal classé, elle doit s'opposer à la notification dans un délai de trois mois.
L'objection doit être motivée et expliquer dûment pourquoi le système d'IA a été mal classé. Le fournisseur doit conserver le droit de faire appel en fournissant des arguments supplémentaires. Si après les trois mois il n'y a pas eu d'objection à la notification, les autorités nationales de surveillance pourraient encore intervenir si le système d'IA présente un risque au niveau national, comme pour tout autre système d'IA sur le marché. Les autorités nationales de surveillance doivent soumettre des rapports annuels à l'Office AI détaillant les notifications reçues et les décisions prises.

(33) Les imprécisions techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Ceci est particulièrement pertinent en ce qui concerne l'âge, l'origine ethnique, le sexe ou les handicaps. Par conséquent, les systèmes d'identification biométrique à distance « en temps réel » et « post » doivent être classés comme présentant un risque élevé. Compte tenu des risques qu'ils présentent, les deux types de systèmes d'identification biométrique à distance devraient être soumis à des exigences spécifiques en matière de capacités d'enregistrement et de surveillance humaine.

(33) Étant donné que les données biométriques constituent une catégorie particulière de données à caractère personnel sensibles conformément au règlement 2016/679, il convient de classer comme à haut risque plusieurs cas d'utilisation critiques de systèmes biométriques et basés sur la biométrie. Systèmes d'IA destinés à être utilisés pour l'identification biométrique de personnes physiques et systèmes d'IA destinés à être utilisés pour faire des déductions sur les caractéristiques personnelles de personnes physiques sur la base de données biométriques ou fondées sur la biométrie, y compris les systèmes de reconnaissance des émotions, à l'exception de ceux qui sont interdits en vertu du présent règlement doivent donc être classés comme à haut risque. Cela ne devrait pas inclure les systèmes d'IA destinés à être utilisés pour la vérification biométrique, qui comprend l'authentification, dont le seul but est de confirmer qu'une personne physique spécifique est la personne qu'elle prétend être et de confirmer l'identité d'une personne physique pour le seul le but d'avoir accès à un service, un appareil ou des locaux (vérification individuelle). Les systèmes biométriques et basés sur la biométrie qui sont prévus par le droit de l'UE pour permettre des mesures de cybersécurité et de protection des données à caractère personnel ne devraient pas être considérés comme présentant un risque significatif d'atteinte à la santé, à la sécurité et aux droits fondamentaux.

(34) En ce qui concerne la gestion et l'exploitation des infrastructures critiques, il convient de classer comme à haut risque les systèmes d'IA destinés à être utilisés comme composants de sécurité dans la gestion et l'exploitation de l'approvisionnement en eau, en gaz, en électricité de chauffage et en énergie numérique critique. infrastructure, car leur défaillance ou leur dysfonctionnement peut porter atteinte à la sécurité et à l'intégrité de ces infrastructures critiques ou mettre en danger la vie et la santé des personnes à grande échelle et entraîner des perturbations sensibles dans le déroulement normal des activités sociales et économiques. Les composants de sécurité des infrastructures critiques, y compris les infrastructures numériques critiques, sont des systèmes utilisés pour protéger directement l'intégrité physique des infrastructures physiques ou la santé et la sécurité des personnes et des biens. La défaillance ou le dysfonctionnement de ces composants pourrait entraîner directement des risques pour l'intégrité physique des infrastructures critiques et donc 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 doivent pas être considérés comme des composants de sécurité. Des exemples de tels composants de sécurité peuvent inclure des systèmes de surveillance de la pression de l'eau ou des systèmes de contrôle d'alarme incendie dans les centres de cloud computing.

(35) Le déploiement de systèmes d'IA dans l'éducation est important pour aider à moderniser des systèmes éducatifs entiers, à améliorer la qualité de l'éducation, tant hors ligne qu'en ligne, et à accélérer l'éducation numérique, la rendant ainsi également accessible à un public plus large . Systèmes d'IA utilisés dans l'éducation ou la formation professionnelle, notamment pour déterminer l'accès ou influencer matériellement les décisions d'admission ou d'affectation de personnes dans des établissements d'enseignement et de formation professionnelle ou pour évaluer des personnes lors de tests dans le cadre ou comme condition préalable à leur éducation ou pour évaluer le niveau approprié d'éducation d'un individu et influençant matériellement le niveau d'éducation et de formation auquel les individus recevront ou pourront accéder ou pour surveiller et détecter les comportements interdits des élèves pendant les tests devraient être classés comme des systèmes d'IA à haut risque, car ils peuvent déterminer l'éducation et le cours professionnel de la vie d'une personne et affectent donc sa capacité à assurer sa subsistance. Lorsqu'ils sont mal conçus et utilisés, ces systèmes peuvent être particulièrement intrusifs et peuvent violer le droit à l'éducation et à la formation ainsi que le droit de ne pas faire l'objet de discrimination et perpétuer des schémas historiques de discrimination, par exemple à l'encontre des femmes, de certains groupes d'âge, des personnes handicapées , ou des personnes de certaines origines raciales ou ethniques ou d'orientation sexuelle.

(36) les systèmes d'intelligence artificielle utilisés dans l'emploi, la gestion des travailleurs et l'accès au travail indépendant, notamment pour le recrutement et la sélection de personnes, pour prendre des décisions ou influencer matériellement les décisions d'initiation, de promotion et de licenciement et pour l'attribution personnalisée des tâches en fonction du comportement individuel, les caractéristiques personnelles ou les données biométriques, le suivi ou l'évaluation des personnes dans des relations contractuelles liées au travail, devraient également être classés comme à haut risque, étant donné que ces systèmes peuvent avoir une incidence sensible sur les perspectives de carrière futures, les moyens de subsistance de ces personnes et les droits des travailleurs. Les relations contractuelles liées au travail pertinentes devraient impliquer de manière significative les employés et les personnes fournissant des services via des plateformes, comme indiqué dans le programme de travail 2021 de la Commission. peuvent perpétuer des schémas historiques de discrimination, par exemple à l'encontre des femmes, de certains groupes d'âge, des personnes handicapées ou des personnes de certaines origines raciales ou ethniques ou de certaines orientations sexuelles. Les systèmes d'IA utilisés pour surveiller les performances et le comportement de ces personnes peuvent également porter atteinte à l'essence de leur impact fondamental sur leurs droits à la protection des données et à la vie privée. Le présent règlement s'applique sans préjudice des compétences de l'Union et des États membres pour prévoir des règles plus spécifiques pour l'utilisation des systèmes d'IA dans le contexte de l'emploi.

(37) Un autre domaine dans lequel l'utilisation des systèmes d'IA mérite une attention particulière est l'accès et la jouissance de certains services privés et publics essentiels, y compris les services de santé, et les services essentiels, y compris, mais sans s'y limiter, le logement, l'électricité, le chauffage/la climatisation et internet, et les avantages nécessaires pour que les gens participent pleinement à la société ou pour améliorer leur niveau de vie. En particulier, les systèmes d'IA utilisés pour évaluer la cote de crédit ou la solvabilité des personnes physiques devraient être classés comme des systèmes d'IA à haut risque, car ils déterminent l'accès de ces personnes aux ressources financières ou aux services essentiels tels que le logement, l'électricité et les services de télécommunication. Les systèmes d'IA utilisés à cette fin peuvent conduire à la discrimination de personnes ou de groupes et perpétuer des modèles historiques de discrimination, par exemple basés sur les origines raciales ou ethniques, le sexe, les handicaps, l'âge, l'orientation sexuelle, ou créer de nouvelles formes d'impacts discriminatoires. Toutefois, les systèmes d'intelligence artificielle prévus par le droit de l'Union aux fins de détecter la fraude dans l'offre de services financiers ne devraient pas être considérés comme

à haut risque au titre du présent règlement. Les personnes physiques qui demandent ou reçoivent des prestations et services d'assistance publique des autorités publiques, y compris des services de santé et des services essentiels, y compris, mais sans s'y limiter, le logement, l'électricité, le chauffage/la climatisation et Internet, dépendent généralement de ces prestations et services et se trouvent dans une position vulnérable en relation avec les autorités compétentes. Si les systèmes d'IA sont utilisés pour déterminer si ces avantages et services doivent être refusés, réduits, révoqués ou récupérés par les autorités, ils peuvent avoir un impact significatif sur les moyens de subsistance des personnes et peuvent porter atteinte à leurs droits fondamentaux, tels que le droit à la protection sociale, à la non - la discrimination, la dignité humaine ou un recours effectif. De même, les systèmes d'intelligence artificielle destinés à être utilisés pour prendre des décisions ou influencer matériellement les décisions concernant l'éligibilité des personnes physiques à l'assurance maladie et vie peuvent également avoir un impact significatif sur les moyens de subsistance des personnes et peuvent porter atteinte à leurs droits fondamentaux, par exemple en limitant l'accès aux soins de santé ou en en perpétuant la discrimination fondée sur les caractéristiques personnelles. Ces systèmes devraient donc être classés comme à haut risque. Néanmoins, le présent règlement ne devrait pas entraver le développement et l'utilisation d'approches innovantes dans l'administration publique, qui bénéficierait d'une utilisation plus large de systèmes d'IA conformes et sûrs, à condition que ces systèmes n'entraînent pas de risque élevé pour les personnes morales et physiques . Enfin, les systèmes d'IA utilisés pour évaluer et classer les appels d'urgence de personnes physiques ou pour répartir ou établir la priorité dans la répartition des services de première intervention d'urgence devraient également être classés comme à haut risque car ils prennent des décisions dans des situations très critiques pour la vie et la santé des personnes et leurs biens.

(37 bis) Compte tenu du rôle et de la responsabilité des autorités policières et judiciaires, et de l'impact des décisions qu'elles prennent aux fins de la prévention, de l'investigation, de la détection ou de la poursuite d'infractions pénales ou de l'exécution de sanctions pénales, certains cas d'utilisation spécifiques de l'IA les applications dans les services répressifs doivent être classées comme présentant un risque élevé, en particulier dans les cas où il existe un risque d'affecter de manière significative la vie ou les droits fondamentaux des individus.

(38) Les actions des autorités répressives impliquant certaines utilisations des systèmes d'IA se caractérisent par un degré important de déséquilibre des pouvoirs et peuvent conduire à la surveillance, à l'arrestation ou à la privation de liberté d'une personne physique ainsi qu'à d'autres atteintes aux droits fondamentaux garantis par la charte . En particulier, si le système d'IA n'est pas formé avec des données de haute qualité, ne répond pas aux exigences adéquates en termes de performances, de précision ou de robustesse, ou n'est pas correctement conçu et testé avant d'être mis sur le marché ou autrement mis en service, il peut isoler des personnes de manière discriminatoire ou autrement incorrecte ou injuste. En outre, l'exercice d'importants droits procéduraux fondamentaux, tels que le droit à un recours effectif et à un procès équitable ainsi que le droit de la défense et la présomption d'innocence, pourrait être entravé, en particulier lorsque ces systèmes d'IA ne sont pas suffisamment transparent, explicable et documenté. Il convient donc de classer comme à haut risque un certain nombre de systèmes d'IA destinés à être utilisés dans le contexte de l'application de la loi, où l'exactitude, la fiabilité et la transparence sont particulièrement importantes pour éviter les effets néfastes, conserver la confiance du public et garantir la responsabilité et des recours efficaces. Compte tenu de la nature des activités en question et des risques y afférents, ces systèmes d'IA à haut risque devraient notamment inclure des systèmes d'IA destinés à être utilisés par ou pour le compte des autorités répressives ou par des agences, offices ou organes de l'Union en soutien de la loi

autorités chargées de l'application de la loi, en tant que polygraphes et outils similaires, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, pour l'évaluation de la fiabilité des preuves dans les procédures pénales, pour le profilage dans le cadre de la détection, de l'enquête ou de la poursuite d'infractions pénales, ainsi que comme pour l'analyse de la criminalité concernant les personnes physiques. Les systèmes d'IA spécifiquement destinés à être utilisés dans le cadre de procédures administratives par les autorités fiscales et douanières ne devraient pas être classés comme des systèmes d'IA à haut risque utilisés par les autorités répressives à des fins de prévention, de détection, d'enquête et de poursuite d'infractions pénales. L'utilisation des outils d'IA par les forces de l'ordre et les autorités judiciaires ne doit pas devenir un facteur d'inégalité, de fracture sociale ou d'exclusion. L'impact de l'utilisation des outils d'IA sur les droits de la défense des suspects ne doit pas être ignoré, notamment la difficulté d'obtenir des informations significatives sur leur fonctionnement et la difficulté conséquente de contester leurs résultats devant les tribunaux, notamment par les personnes mises en examen.

(39) Les systèmes d'intelligence artificielle utilisés dans la gestion des migrations, de l'asile et du contrôle des frontières affectent des personnes qui se trouvent souvent dans une situation particulièrement vulnérable et qui dépendent du résultat des actions des autorités publiques compétentes. La précision, le caractère non discriminatoire et la transparence des systèmes d'IA utilisés dans ces contextes sont donc particulièrement importants pour garantir le respect des droits fondamentaux des personnes concernées, notamment leurs droits à la libre circulation, à la non-discrimination, à la protection de la vie privée et données personnelles, protection internationale et bonne administration. Il convient donc de classer comme systèmes d'intelligence artificielle à haut risque destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou par des agences, offices ou organes de l'Union chargés de tâches dans les domaines de la gestion des migrations, de l'asile et du contrôle des frontières en tant que polygraphes et similaires des outils, dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables, pour évaluer certains risques posés par des personnes physiques entrant sur le territoire d'un État membre ou demandant un visa ou l'asile; pour vérifier l'authenticité des documents pertinents des personnes physiques ; pour assister les autorités publiques compétentes dans l'examen et l'évaluation de la véracité des éléments de preuve relatifs aux demandes d'asile, de visa et de permis de séjour et aux plaintes associées en ce qui concerne l'objectif d'établir l'éligibilité des personnes physiques demandant un statut ; pour le contrôle, la surveillance ou le traitement de données à caractère personnel dans le cadre d'activités de gestion des frontières, à des fins de détection, de reconnaissance ou d'identification de personnes physiques ; pour la prévision ou la prédiction des tendances liées aux mouvements migratoires et aux passages frontaliers. Les systèmes d'IA dans le domaine de la gestion des migrations, de l'asile et des contrôles aux frontières couverts par le présent règlement devraient respecter les exigences procédurales pertinentes fixées par la directive 2013/32/UE du Parlement européen et du Conseil49, le règlement (CE) n° 810/ 2009 du Parlement européen et du Conseil50 et autres actes législatifs pertinents. L'utilisation de systèmes d'intelligence artificielle dans la gestion des migrations, de l'asile et du contrôle des frontières ne devrait en aucun cas être utilisée par les États membres ou les institutions, agences ou organes de l'Union comme un moyen de contourner leurs obligations internationales en vertu de la convention du 28 juillet 1951 relative au statut des réfugiés tels que modifiés par le protocole du 31 janvier 1967, ils ne doivent pas non plus être utilisés pour enfreindre de quelque manière que ce soit le principe de non-refoulement ou empêcher des voies légales sûres et efficaces d'entrer sur le territoire de l'Union, y compris le droit à la protection internationale.

(40) Certains systèmes d'IA destinés à l'administration de la justice et aux processus démocratiques devraient être classés comme à haut risque, compte tenu de leur impact potentiellement significatif sur la démocratie, l'État de droit, les libertés individuelles ainsi que le droit à un recours effectif

et à un procès équitable. En particulier, pour faire face aux risques de biais, d'erreurs et d'opacité potentiels, il convient de qualifier de systèmes d'IA à haut risque destinés à être utilisés par une autorité judiciaire ou un organe administratif ou en leur nom pour aider les autorités judiciaires ou les organes administratifs à rechercher et en interprétant les faits et la loi et en appliquant la loi à un ensemble concret de faits ou utilisée de manière similaire dans le règlement extrajudiciaire des différends. L'utilisation d'outils d'intelligence artificielle peut soutenir, mais ne doit pas remplacer le pouvoir décisionnel des juges ou l'indépendance judiciaire, car la prise de décision finale doit rester une activité et une décision axées sur l'homme. Cette qualification ne devrait toutefois pas s'étendre aux systèmes d'IA destinés à des activités administratives purement auxiliaires qui n'affectent pas l'administration effective de la justice dans des affaires individuelles, telles que l'anonymisation ou la pseudonymisation des décisions judiciaires, des documents ou des données, la communication entre le personnel, les tâches administratives ou allocation des ressources.

(40 bis) 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 disproportionnés sur les processus démocratiques, 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 des personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums devraient être classés comme des systèmes d'IA à haut risque. à l'exception des systèmes d'IA dont les résultats ne sont pas directement exposés aux personnes physiques, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques d'un point de vue administratif et logistique.

(40 ter) Compte tenu du nombre de personnes physiques utilisant les services fournis par les plateformes de médias sociaux désignées comme de très grandes plateformes en ligne, ces plateformes en ligne peuvent être utilisées d'une manière qui influence fortement la sécurité en ligne, la formation de l'opinion et du discours publics, les élections et la démocratie. les processus et les préoccupations sociétales. Il convient donc que les systèmes d'IA utilisés par ces plateformes en ligne dans leurs systèmes de recommandation soient soumis au présent règlement afin de garantir que les systèmes d'IA respectent les exigences fixées par le présent règlement, y compris les exigences techniques en matière de gouvernance des données, de documentation technique et de traçabilité, transparence, contrôle humain, précision et robustesse. Le respect du présent règlement devrait permettre à ces très grandes plateformes en ligne de se conformer à leurs obligations plus larges d'évaluation et d'atténuation des risques prévues aux articles 34 et 35 du règlement UE 2022/2065. Les obligations énoncées dans le présent règlement sont sans préjudice du règlement (UE) 2022/2065 et devraient compléter les obligations requises en vertu du règlement (UE) 2022/2065 lorsque la plateforme de médias sociaux a été désignée comme une très grande plateforme en ligne. Compte tenu de l'impact à l'échelle européenne des plateformes de médias sociaux désignées comme de très grandes plateformes en ligne, les autorités désignées au titre du règlement (UE) 2022/2065 devraient agir en tant qu'autorités d'exécution aux fins de l'application de cette disposition.

(41) Le fait qu'un système d'IA est classé comme système d'IA à haut risque en vertu du présent règlement ne devrait pas être interprété comme indiquant que l'utilisation du système est nécessairement licite ou illicite en vertu d'autres actes du droit de l'Union ou en vertu du droit national compatible avec le droit de l'Union. droit, par exemple sur la protection des données à caractère personnel, Toute utilisation de ce type devrait continuer à se faire uniquement en conformité avec les exigences applicables résultant de la Charte et des actes applicables du droit dérivé de l'Union et du droit national.

(41 bis) Un certain nombre de règles juridiquement contraignantes aux niveaux européen, national et international s'appliquent déjà ou sont pertinentes pour les systèmes d'IA aujourd'hui, y compris, mais sans s'y limiter, l'UE

droit primaire (les traités de l'Union européenne et sa Charte des droits fondamentaux), droit secondaire de l'UE (tel que le règlement général sur la protection des données, la directive sur la responsabilité du fait des produits, le règlement sur la libre circulation des données à caractère non personnel, les directives anti-discrimination , droit de la consommation et directives sur la sécurité et la santé au travail), les traités des droits de l'homme des Nations unies et les conventions du Conseil de l'Europe (telles que la convention européenne des droits de l'homme) et de nombreuses lois des États membres de l'UE. Outre les règles applicables horizontalement, il existe diverses règles spécifiques à un domaine qui s'appliquent à des applications particulières de l'IA (comme par exemple le règlement sur les dispositifs médicaux dans le secteur de la santé).

TITRE III

SYSTÈMES D'IA À HAUT RISQUE

CHAPITRE 1

CLASSIFICATION DES SYSTÈMES D'IA À HAUT RISQUE

Article 6

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

1. Indépendamment du fait qu'un système d'IA est mis sur le marché ou mis en service indépendamment des produits visés aux points a) et b), ce système d'IA est considéré à haut risque lorsque les deux conditions suivantes sont remplies:

a) le système d'IA est destiné à être utilisé en tant que composant de sécurité d'un produit ou Le système d'IA est lui-même un produit, couvert par la législation d'harmonisation de l'Union énumérée à l'annexe II,

b) le produit dont le composant de sécurité conformément au point a) est le système d'IA, ou le système d'IA lui-même en tant que produit, doit faire l'objet d'une évaluation de la conformité par une tierce partie liée aux risques pour la santé et la sécurité, en vue de la mise sur le marché ou la mise en service de ce produit conformément à la législation d'harmonisation de l'Union énumérée à l'annexe II.

2. Outre les systèmes d'IA à haut risque visés au paragraphe 1, les systèmes d'IA relevant d'un ou de plusieurs des domaines et cas d'utilisation critiques visés à l'annexe III sont considérés comme à haut risque s'ils présentent un risque significatif de préjudice pour le la santé, la sécurité ou les droits fondamentaux des personnes physiques. Lorsqu'un système d'IA relève de l'annexe III, point 2, il est considéré comme présentant un risque élevé s'il présente un risque significatif d'atteinte à l'environnement.

La Commission, six mois avant l'entrée en vigueur du présent règlement, après consultation de l'Office IA et des parties prenantes concernées, fournit des lignes directrices précisant clairement les circonstances dans lesquelles les résultats des systèmes d'IA visés à l'annexe III présenteraient un risque important de préjudice à la santé, à la sécurité ou aux droits fondamentaux des personnes physiques ou dans les cas où cela ne le serait pas.

2a. Lorsque les fournisseurs relevant d'un ou plusieurs des domaines critiques et des cas d'utilisation visés à l'annexe III estiment que leur système d'IA ne présente pas de risque significatif au sens du paragraphe 2, ils soumettent une notification motivée à l'Autorité nationale

l'Autorité de surveillance qu'ils ne sont pas soumis aux exigences du titre III, chapitre 2, du présent règlement. Lorsque le système AI est destiné à être utilisé dans deux ou plusieurs États membres, la notification susmentionnée est adressée à l'Office AI. Sans préjudice de l'article 65, l'Autorité nationale de surveillance examine et répond, directement ou via l'Office AI, dans un délai de 3 mois si elle estime que le système AI est mal classé.

2b. Les fournisseurs qui classent à tort leur système d'IA comme non soumis aux exigences du titre III, chapitre 2, du présent règlement et le mettent sur le marché avant la date limite d'objection par les autorités nationales de surveillance sont responsables et passibles d'amendes conformément à l'article 71.

2c. Les autorités nationales de surveillance soumettent un rapport annuel à l'Office AI détaillant le nombre de notifications reçues, les domaines à haut risque concernés et les décisions prises concernant les notifications reçues.

Article 7
Amendements à l'annexe III

1. La Commission est habilitée à adopter des actes délégués conformément à l'article 73 afin de modifier l'annexe III en ajoutant ou en modifiant des domaines ou des cas d'utilisation de systèmes d'IA à haut risque lorsqu'ils présentent un risque significatif d'atteinte à la santé et à la sécurité, ou une incidence négative sur droits fondamentaux, à l'environnement ou à la démocratie et à l'état de droit, et que le risque est, en ce qui concerne sa gravité et sa probabilité d'occurrence, équivalent ou supérieur au risque de préjudice ou d'impact négatif posé par le risque élevé Systèmes d'IA déjà mentionnés à l'annexe III.

1a. La Commission est également habilitée à adopter des actes délégués conformément à l'article 73 pour supprimer les cas d'utilisation de systèmes d'IA à haut risque de la liste figurant à l'annexe III si les conditions visées au paragraphe 1 ne s'appliquent plus

2. Lors de l'évaluation d'un système d'IA aux fins des paragraphes 1 et 1 bis, la Commission tient compte des critères suivants: a) la finalité du

système d'IA;

(aa) les capacités et fonctionnalités générales du système d'IA indépendamment de son objectif prévu;

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

utilisé ; (b bis) la nature et la quantité des données traitées et utilisées par le système

d'IA ; (bb) la mesure dans laquelle le système d'IA agit de manière

autonome; c) la mesure dans laquelle l'utilisation d'un système d'IA a déjà porté atteinte à la santé et à la sécurité, a eu une incidence négative sur les droits fondamentaux, l'environnement, la démocratie et l'État de droit ou a suscité des inquiétudes importantes en ce qui concerne la probabilité d'un tel préjudice ou effet préjudiciable, démontrée par exemple par des rapports ou des allégations documentées soumis aux autorités de contrôle nationales, à la Commission, à l'Office AI, au CEPD ou au Agence des droits fondamentaux de l'Union européenne ;

d) l'étendue potentielle de ce dommage ou de cet impact négatif, notamment en termes d'intensité et de capacité à affecter une pluralité de personnes ou à affecter de manière disproportionnée un groupe particulier de personnes

e) la mesure dans laquelle les personnes potentiellement lésées ou lésées dépendent de la production produite impliquant un système d'IA, et cette production est purement accessoire par rapport à l'action ou à la décision pertinente à prendre, notamment parce que, pour des raisons pratiques ou juridiques il n'est pas raisonnablement possible de se retirer de cette sortie ;

(e bis) l'utilisation abusive et malveillante potentielle du système d'IA et de la technologie qui le sous-tend;

(f) la mesure dans laquelle il existe un déséquilibre de pouvoir, ou dans quelle mesure les personnes potentiellement lésées ou affectées négativement se trouvent dans une position vulnérable par rapport à l'utilisateur d'un système d'IA, notamment en raison de leur statut, de leur autorité, de leurs connaissances, de la situation économique ou sociale les circonstances ou l'âge ;

g) la mesure dans laquelle le résultat produit impliquant un système d'IA est facilement réversible ou remédiable, les résultats ayant une incidence négative sur la santé, la sécurité, les droits fondamentaux des personnes, l'environnement ou la démocratie et l'État de droit ne devant pas être considéré comme facilement réversible ;

g bis) l'étendue de la disponibilité et de l'utilisation de solutions et de mécanismes techniques efficaces pour le contrôle, la fiabilité et la corrigibilité du système d'IA;

(gb) l'ampleur et la probabilité des avantages du déploiement du système d'IA pour les individus, les groupes ou la société dans son ensemble, y compris les améliorations possibles de la sécurité des produits ;

(gc) l'étendue de la surveillance humaine et la possibilité pour un être humain d'intervenir afin d'annuler une décision ou des recommandations pouvant entraîner un préjudice potentiel ;

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

(je) des mesures efficaces de réparation en rapport avec les dommages causés par un système d'IA, à l'exclusion des réclamations pour dommages directs ou indirects ;

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

2a. Lors de l'évaluation d'un système d'IA aux fins des paragraphes 1 ou 1 bis, la Commission consulte l'Office IA et, le cas échéant, les représentants des groupes sur lesquels un système d'IA a une incidence, l'industrie, des experts indépendants, les partenaires sociaux et les organisations de la société civile. La Commission organise également des consultations publiques à cet égard et rend publics les résultats de ces consultations et de l'évaluation finale.

2b. L'Office AI, les autorités nationales de surveillance ou le Parlement européen peuvent demander à la Commission de réévaluer la catégorisation des risques conformément aux paragraphes 1 et 1 bis. Le système d'IA doit ensuite être examiné pour être réévalué et peut être reclassé. La Commission motive sa décision et la rend publique.

Article 15

Précision, robustesse et cybersécurité

1a. Pour traiter les aspects techniques de la manière de mesurer les niveaux appropriés d'exactitude et de robustesse énoncés au paragraphe 1 du présent article, l'Office AI réunit les autorités nationales et internationales de métrologie et d'étalonnage et fournit des orientations non contraignantes sur la question, comme indiqué à l'article 56, paragraphe 2, point a).

ANNEXE II

LISTE DES LÉGISLATIONS D'HARMONISATION DE L'UNION

Section A – Liste des législations d'harmonisation de l'Union fondées sur la nouvelle législation Cadre

Directive 2006/42/CE du Parlement européen et du Conseil du 17 mai 2006 relative aux machines et modifiant la directive 95/16/CE (JO L 157 du 9.6.2006, p. 24) [abrogée par le règlement Machines] ; directive 2009/48/CE du Parlement européen et du

2. 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 au rapprochement des législations des États membres relatives aux ascenseurs et aux 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 au rapprochement des législations des États membres relatives aux appareils et 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 au rapprochement des législations des États membres concernant la mise à disposition sur le marché d'équipements hertziens et abrogeant la directive 1999/5/CE (JO L 153, 22.5.2014, p.62);

7. Directive 2014/68/UE du Parlement européen et du Conseil du 15 mai 2014 relative au rapprochement des législations des États membres relatives à la mise à disposition sur le marché d'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);

dix. règlement (UE) 2016/426 du Parlement européen et du Conseil du 9 mars 2016 relatif aux appareils brûlant des combustibles gazeux et abrogeant la directive 2009/142/CE (JO L 81 du 31.3.2016, p. 99);

11. Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant directives 90/385/CEE et 93/42/CEE du Conseil (JO L 117 du 5.5.2017, p. 1);

12. Règlement (UE) 2017/746 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la directive 98/79/CE et la décision 2010/227/UE de la Commission (JO L 117 du 5.5.2017, p. 176).

Section B. Liste des autres actes législatifs d'harmonisation de l'Union

Règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 établissant des 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).

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);

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); 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);

Directive (UE) 2016/797 du Parlement européen et du Conseil du 11 mai 2016 relative à l'interopérabilité du système ferroviaire au sein de l'Union européenne (JO L 138 du 26.5.2016, p. 44).

Règlement (UE) 2018/858 du Parlement européen et du Conseil du 30 mai 2018 relatif à la réception et à la surveillance du marché des véhicules à moteur et de leurs remorques, ainsi que des systèmes, composants et entités techniques destinés à ces véhicules, modifiant le règlement (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); 3. Règlement (UE) 2019/2144 du Parlement européen et du Conseil du 27 novembre 2019 relatif aux prescriptions pour 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 la sécurité 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 règlements de la Commission (CE) n° 631/2009, (UE) n° 406/2010, (UE) n° 672/2010, (UE) n° 1003/2010, (UE) n° 1005/2010, (UE) n° 1008/2010, (UE) n° 1009/2010, (UE) n° 19/2011, (UE) n° 109/2011, (UE) n° 458/2011, (UE) n° 65 /2012, (UE) n° 130/2012, (UE) n° 347/2012, (UE) n° 351/2012, (UE) n° 1230/2012 et (UE) 2015/166 (JO L 325 du 16.12.2019, p.1);

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 le règlement (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil et règlement (CEE) n° 3922/91 du Conseil (JO L 212 du 22.8.2018, p. 1), dans la mesure où la conception, la production et la mise sur le marché d'aéronefs visés à l'article 2, paragraphe 1, points a) et b), de celui-ci, lorsqu'il s'agit

les aéronefs sans pilote et leurs moteurs, hélices, pièces et équipements pour les contrôler à distance, sont concernés.

ANNEXE III

SYSTÈMES D'IA À HAUT RISQUE VISÉS À L'ARTICLE 6, PARAGRAPHE 2

Les systèmes d'IA spécifiquement mentionnés aux points 1 à 8a correspondent à des cas d'utilisation critiques et sont chacun considérés comme des systèmes d'IA à haut risque conformément à l'article 6, paragraphe 2, pour autant qu'ils remplissent les critères énoncés dans cet article:

1. Systèmes biométriques et basés sur la biométrie

a) les systèmes d'IA destinés à être utilisés pour l'identification biométrique des personnes physiques, à l'exception de ceux mentionnés à l'article 5 ;

a bis) les systèmes d'intelligence artificielle destinés à être utilisés pour faire des déductions sur les caractéristiques personnelles de personnes physiques sur la base de données biométriques ou fondées sur la biométrie, y compris les systèmes de reconnaissance des émotions, à l'exception de ceux mentionnés à l'article 5;

Le point 1 n'inclut pas les systèmes d'intelligence artificielle destinés à être utilisés pour la vérification biométrique dont le seul but est de confirmer qu'une personne physique spécifique est la personne qu'elle prétend être.

2. Gestion et exploitation des infrastructures critiques :

a) les systèmes d'intelligence artificielle destinés à être utilisés comme composants de sécurité dans la gestion et l'exploitation du trafic routier, ferroviaire et aérien, à moins qu'ils ne soient réglementés par une législation d'harmonisation ou sectorielle.

aa) Systèmes d'intelligence artificielle destinés à être utilisés comme composants de sécurité dans la gestion et l'exploitation de l'approvisionnement en eau, en gaz, en chauffage, en électricité et en infrastructures numériques critiques

3. Éducation et formation professionnelle :

a) les systèmes d'IA destinés à être utilisés aux fins de déterminer l'accès ou d'influencer sensiblement les décisions d'admission ou d'affectation des personnes physiques aux établissements d'enseignement et de formation professionnelle ;

b) les systèmes d'IA destinés à être utilisés aux fins d'évaluer les étudiants dans les établissements d'enseignement et de formation professionnelle et d'évaluer les participants aux tests généralement requis pour l'admission dans ces établissements; ba) les systèmes destinés

à être utilisés dans le but d'évaluer le niveau d'éducation approprié pour un individu et influençant sensiblement le niveau d'éducation et de formation professionnelle que cet individu recevra ou pourra

accéder.

bb) les systèmes d'IA destinés à être utilisés pour surveiller et détecter les comportements interdits des étudiants lors des tests dans le cadre de/au sein des établissements d'enseignement et de formation professionnelle ;

4. Emploi, gestion des travailleurs et accès au travail indépendant :

(a) les systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, notamment pour placer des annonces d'emploi ciblées, filtrer ou filtrer les candidatures, évaluer les candidats lors d'entretiens ou de tests ;

(b) les systèmes d'IA destinés à être utilisés pour prendre ou influencer matériellement les décisions affectant l'initiation, la promotion et la résiliation des relations contractuelles liées au travail, l'attribution des tâches en fonction du comportement individuel ou des traits ou caractéristiques personnels, ou pour surveiller et évaluer les performances et le comportement des personnes dans de telles relations.

5. Accès et jouissance des services privés essentiels et des services et avantages publics :

(a) Les systèmes d'intelligence artificielle destinés à être utilisés par ou au nom des autorités publiques pour évaluer l'éligibilité des personnes physiques aux prestations et services d'assistance publique, y compris les services de santé et les services essentiels, y compris, mais sans s'y limiter, le logement, l'électricité, le chauffage/refroidissement et Internet, ainsi que pour accorder, réduire, révoquer, augmenter ou réclamer ces avantages et services ;

(b) les systèmes d'intelligence artificielle destinés à être utilisés pour évaluer la solvabilité de personnes physiques ou établir leur pointage de crédit, à l'exception des Systèmes d'IA utilisés à des fins de détection de fraude financière, à l'exception des ~~systèmes d'IA mis en service par de petits prestataires pour leur propre usage ;~~

(b bis) les systèmes d'intelligence artificielle destinés à être utilisés pour prendre des décisions ou influencer sensiblement les décisions concernant l'éligibilité des personnes physiques à l'assurance maladie et vie;

c) les systèmes d'intelligence artificielle destinés à évaluer et à classer les appels d'urgence émis par des personnes physiques ou à être utilisés pour envoyer ou établir la priorité dans l'envoi des services de première intervention d'urgence, y compris par la police et les forces de l'ordre, les pompiers et l'aide médicale, ainsi que des systèmes de triage des patients en soins d'urgence.

6. Forces de l'ordre:

~~a) les systèmes d'intelligence artificielle destinés à être utilisés par les autorités répressives pour effectuer des évaluations individuelles des risques des personnes physiques afin d'évaluer le risque d'infraction ou de récidive d'une personne physique ou le risque pour les victimes potentielles d'infractions pénales;~~

b) les systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte des autorités répressives, ou par des agences, bureaux ou organes de l'Union en soutien aux autorités répressives en tant que polygraphes et outils similaires ; dans la mesure où leur utilisation est autorisée par le droit de l'Union et le droit national applicables

~~c) les systèmes d'intelligence artificielle destinés à être utilisés par les autorités répressives pour détecter les deep fakes, comme indiqué à l'article 52, paragraphe~~ 3 ;

~~d) l~~es systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte des autorités répressives, ou par des agences, bureaux ou organes de l'Union en soutien aux autorités répressives pour évaluer la fiabilité des preuves dans le cadre d'enquêtes ou de poursuites relatives à des infractions pénales;

~~c) les systèmes d'intelligence artificielle destinés à être utilisés par les autorités répressives pour prédire la survenance ou la récurrence d'une infraction pénale réelle ou potentielle fondée sur le profilage de personnes physiques, tel que visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 ou évaluer les traits de personnalité et les caractéristiques ou le comportement criminel passé de personnes physiques ou de groupes ;~~

~~f) l~~es systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte des autorités répressives ou par des agences, offices ou organes de l'Union en soutien aux autorités répressives pour le profilage des personnes physiques, tel que visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre de la détection, de la recherche ou de la poursuite d'infractions pénales ou, dans le cas d'agences, d'offices ou d'organes de l'Union, tels que visés à l'article 3, paragraphe 5, du règlement (UE) 2018/1725 ;

~~g) s~~ystèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte des autorités répressives ou par des agences, bureaux ou organes de l'Union en soutien aux autorités répressives pour l'analyse de la criminalité concernant des personnes physiques, permettant aux autorités répressives d'effectuer des recherches dans des données volumineuses complexes, liées et non liées ensembles disponibles dans différentes sources de données ou dans différents formats de données afin d'identifier des modèles inconnus ou de découvrir des relations cachées dans les données.

7. Gestion de la migration, de l'asile et du contrôle des frontières :

a) les systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou d'agences, d'offices ou d'organismes de l'Union en tant que polygraphes et outils similaires, dans la mesure où leur utilisation est autorisée par le droit de l'Union ou le droit national applicable

b) les systèmes d'IA destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou d'agences, d'offices ou d'organes de l'Union pour évaluer un risque, y compris un risque pour la sécurité, un risque d'immigration irrégulière ou un risque pour la santé, posé par une personne physique personne qui a l'intention d'entrer ou est entrée sur le territoire d'un État membre;

c) les systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou d'agences, d'offices ou d'organes de l'Union pour vérifier l'authenticité des documents de voyage et des pièces justificatives des personnes physiques et détecter les documents non authentiques en vérifiant leur sécurité caractéristiques;

d) les systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou d'agences, d'offices ou d'organes de l'Union pour aider les autorités publiques compétentes à examiner et à évaluer la véracité des preuves en rapport avec les demandes d'asile, de visa et de séjour autorisations et réclamations associées concernant l'éligibilité des personnes physiques demandant un statut.

d bis) les systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou d'agences, d'offices ou d'organismes de l'Union chargés de la gestion de la migration, de l'asile et du contrôle des frontières pour contrôler, surveiller ou traiter des données dans le cadre d'activités de gestion des frontières, pour la à des fins de détection, de reconnaissance ou d'identification de personnes physiques

d ter) Systèmes d'intelligence artificielle destinés à être utilisés par ou pour le compte d'autorités publiques compétentes ou d'agences, d'offices ou d'organismes de l'Union chargés de la gestion des migrations, de l'asile et du contrôle des frontières pour la prévision ou la prédiction des tendances liées aux mouvements migratoires et au franchissement des frontières

8. Administration de la justice et processus démocratiques :

un) Systèmes d'intelligence artificielle destinés à être utilisés par une autorité judiciaire ou un organe administratif ou en leur nom pour assister une autorité judiciaire ou un organe administratif dans la recherche et l'interprétation des faits et du droit et dans l'application du droit à un ensemble concret de faits ou utilisés de manière similaire dans les modes alternatifs de résolution des conflits.

aa) Systèmes d'intelligence artificielle 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

Cela n'inclut pas les systèmes d'IA dont les résultats ne sont pas directement exposés aux personnes physiques, tels que les outils utilisés pour organiser, optimiser et structurer les campagnes politiques d'un point de vue administratif et logistique.

(ab) les systèmes d'intelligence artificielle destinés à être utilisés par les plateformes de médias sociaux qui ont été désignées comme de très grandes plateformes en ligne au sens de l'article 33 du règlement UE 2022/2065, dans leurs systèmes de recommandation pour recommander au destinataire du service généré par l'utilisateur contenus disponibles sur la plateforme.

Article 5, paragraphe 1, points a) à c), da) à d quater), article 5, paragraphe 1 bis, considérants 14 à 17 et 26 bis à 26 quinquies	CA 11

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

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

(16) La mise sur le marché, la mise en service ou l'utilisation de certains systèmes d'IA ayant pour objectif ou pour effet de fausser sensiblement le comportement humain, susceptible de provoquer des dommages physiques ou psychologiques, devrait être interdite. Cette limitation doit être comprise comme incluant les neurotechnologies assistées par des systèmes d'IA qui sont utilisées pour surveiller, utiliser ou influencer les données neuronales recueillies par le biais d'interfaces cerveau-ordinateur dans la mesure où elles déforment matériellement le comportement d'une personne physique d'une manière qui provoque ou est susceptible de causer à cette personne ou à une autre personne un préjudice important. De tels systèmes d'IA déploient des composants subliminaux que les individus ne peuvent pas percevoir ou exploiter les vulnérabilités des individus et des groupes spécifiques de personnes en raison de leurs traits de personnalité connus ou prédits, de leur âge, de leurs incapacités physiques ou mentales, de leur situation sociale ou économique. Ils le font avec l'intention ou l'effet de déformer matériellement le comportement d'une personne et d'une manière qui cause ou est susceptible de causer un préjudice important à cette personne ou à une autre personne ou à des groupes de personnes, y compris des préjudices qui peuvent s'accumuler au fil du temps. L'intention de fausser le comportement ne peut être présumée si la distorsion résulte de facteurs externes au système d'IA qui échappent au contrôle du fournisseur ou de l'utilisateur, tels que des facteurs qui peuvent ne pas être raisonnablement prévus et atténués par le fournisseur ou le déployeur du système d'IA. Dans tous les cas, il n'est pas nécessaire que le fournisseur ou le déployeur ait l'intention de causer un préjudice important, tant que ce préjudice résulte des pratiques de manipulation ou d'exploitation activées par l'IA. L'interdiction de telles pratiques d'IA complète les dispositions contenues dans la directive [directive 2005/29/CE sur les pratiques commerciales déloyales, telle que modifiée par la directive (UE) 2019/216], selon laquelle les pratiques commerciales déloyales sont interdites, qu'elles soient ou non réalisées en ayant recours à des systèmes d'IA ou autrement. Dans un tel cadre, les pratiques commerciales licites, par exemple dans le domaine de la publicité, qui sont conformes au droit de l'Union ne devraient pas en elles-mêmes être considérées comme violant l'interdiction. La recherche à des fins légitimes en rapport avec de tels systèmes d'IA ne devrait pas être étouffée par l'interdiction, si cette recherche n'équivaut pas à une utilisation du système d'IA dans les relations homme-machine qui expose

de nuire à des personnes physiques et ces recherches sont menées conformément aux normes éthiques reconnues pour la recherche scientifique et sur la base du consentement éclairé spécifique des personnes qui y sont exposées ou, le cas échéant, de leur tuteur légal.

(16 bis) Les systèmes d'intelligence artificielle qui catégorisent les personnes physiques en les affectant à des catégories spécifiques, selon des caractéristiques sensibles ou protégées connues ou présumées, sont particulièrement intrusifs, violent la dignité humaine et présentent un risque élevé de discrimination. Ces caractéristiques comprennent le sexe, l'identité de genre, la race, l'origine ethnique, le statut de migrant ou de citoyen, l'orientation politique, l'orientation sexuelle, la religion, le handicap ou tout autre motif pour lequel la discrimination est interdite en vertu de l'article 21 de la Charte des droits fondamentaux de l'UE, ainsi que conformément à l'article 9 du règlement (UE) 2016/769. De tels systèmes devraient donc être interdits.

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

(26 bis) Systèmes d'intelligence artificielle utilisés par les autorités répressives ou en leur nom pour effectuer des prédictions, des profils ou des évaluations des risques sur la base du profilage de personnes physiques ou de l'analyse de données sur la base de traits et de caractéristiques de personnalité, y compris l'emplacement de la personne, ou le comportement criminel antérieur de personnes physiques ou groupes de personnes dans le but de prédire la survenance ou la récurrence d'une ou de plusieurs infractions pénales réelles ou potentielles ou d'autres comportements sociaux ou infractions administratives criminalisés, y compris les systèmes de prédiction de la fraude, présentent un risque particulier de discrimination à l'encontre de certaines personnes ou groupes de personnes. personnes, car elles violent la dignité humaine ainsi que le principe juridique clé de la présomption d'innocence. De tels systèmes d'IA devraient donc être interdits.

(26 ter) L'extraction aveugle et non ciblée de données biométriques provenant de médias sociaux ou d'images de vidéosurveillance pour créer ou étendre des bases de données de reconnaissance faciale ajoute au sentiment de surveillance de masse et peut conduire à des violations flagrantes des droits fondamentaux, y compris le droit au respect de la vie privée. L'utilisation de systèmes d'IA à cette fin devrait donc être interdite.

(26 quater) La base scientifique des systèmes d'IA visant à détecter les émotions, les caractéristiques physiques ou physiologiques telles que les expressions faciales, les mouvements, la fréquence du pouls ou la voix suscite de vives inquiétudes. Les émotions ou les expressions des émotions et les perceptions de celles-ci varient considérablement selon les cultures et les situations, et même au sein d'un même individu. Parmi les principaux défauts de ces technologies figurent la fiabilité limitée (les catégories d'émotions ne sont ni exprimées de manière fiable ni associées sans équivoque à un ensemble commun de mouvements physiques ou physiologiques), le manque de spécificité (les expressions physiques ou physiologiques ne correspondent pas parfaitement aux émotions catégories) et la généralisabilité limitée (les effets de contexte et de culture ne sont pas suffisamment pris en compte). Problèmes de fiabilité et

par conséquent, des risques majeurs d'abus peuvent survenir, en particulier lors du déploiement du système dans des situations réelles liées à l'application de la loi, à la gestion des frontières, au lieu de travail et aux établissements d'enseignement. Par conséquent, la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA destinés à être utilisés dans ces contextes pour détecter l'état émotionnel des individus devrait être interdite.

(26 quinquies) Les pratiques interdites par la législation de l'Union, y compris la législation sur la protection des données, la législation sur la non-discrimination, la législation sur la protection des consommateurs et le droit de la concurrence, ne devraient pas être affectées par le présent règlement.

TITRE II

PRATIQUES INTERDITES D'INTELLIGENCE ARTIFICIELLE

Article 5

1. Les pratiques d'intelligence artificielle suivantes sont interdites :

(un) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui déploie des techniques subliminales au-delà de la conscience d'une personne ou des techniques délibérément manipulatrices ou trompeuses, dans le but ou pour effet de fausser matériellement le comportement d'une personne ou d'un groupe de personnes en nuire à la capacité de la personne de prendre une décision éclairée, l'amenant ainsi à prendre une décision qu'elle n'aurait pas prise autrement d'une manière qui cause ou est susceptible de causer à cette personne, à une autre personne ou à un groupe de personnes un préjudice important ;

L'interdiction d'un système d'IA qui déploie des techniques subliminales visées au premier alinéa ne s'applique pas aux systèmes d'IA destinés à être utilisés à des fins thérapeutiques autorisées sur la base du consentement éclairé spécifique des personnes qui y sont exposées ou, lorsque le cas échéant, de leur tuteur légal b) la mise sur le marché, la mise en service ou l'utilisation d'un

système d'IA qui exploite l'une des vulnérabilités d'une personne ou d'un groupe spécifique de personnes, y compris les caractéristiques de cette personne ou de ce groupe de personnes» traits de personnalité connus ou prévus ou situation sociale ou économique, âge, capacité physique ou mentale, dans le but ou pour effet de fausser sensiblement le comportement de cette personne ou d'une personne appartenant à ce groupe d'une manière qui cause ou est susceptible de causer à cette personne ou à une autre personne un préjudice important ;

b bis) la mise sur le marché, la mise en service ou l'utilisation de systèmes de catégorisation biométrique qui catégorisent les personnes physiques selon des attributs ou caractéristiques sensibles ou protégés ou sur la base de l'inférence de ces attributs ou caractéristiques. Cette interdiction ne s'applique pas aux systèmes d'IA destinés à être utilisés à des fins thérapeutiques autorisées sur la base du consentement éclairé spécifique des personnes qui y sont exposées ou, le cas échéant, de leur tuteur légal.

(c) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA par les autorités pu~~bliques ou en leur nom pour la notation sociale,~~ l'évaluation ou la classification de la fiabilité de personnes phy~~siques ou de groupes de p~~ersonnes physiques sur une certaine période de temps en fonction de leur un comportement social ou des caractéristiques personnelles ou de personnalité connues, inférées ou prédites, le score social menant à l'un ou l'autre des éléments suivants :

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

(ii) préjudiciable ou défavorable de certaines personnes physiques ou groupes de celles-ci qui est injustifié ou disproportionné par rapport à leur comportement social ou à sa gravité ;

d bis) la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA pour effectuer des évaluations des risques de personnes physiques ou de groupes de personnes afin d'évaluer le risque d'une personne physique de commettre une infraction ou de récidiver ou de prévoir l'apparition ou la réapparition d'un une infraction pénale ou administrative réelle ou potentielle fondée sur le profilage d'une personne physique ou sur l'évaluation des traits et caractéristiques de la personnalité, y compris l'emplacement de la personne, ou le comportement criminel passé de personnes physiques ou de groupes de personnes physiques
personnes;

(d ter) La mise sur le marché, la mise en service ou l'utilisation de systèmes d'intelligence artificielle qui créent ou étendent des bases de données de reconnaissance faciale par le grattage non ciblé d'images faciales provenant d'Internet ou de séquences de vidéosurveillance ;

(d quater) la mise sur le marché, la mise en service ou l'utilisation de systèmes d'IA pour déduire les émotions d'une personne physique dans les domaines de l'application de la loi, de la gestion des frontières, sur le lieu de travail et dans les établissements d'enseignement.

1a. Le présent article n'affecte pas les interdictions qui s'appliquent lorsqu'une pratique d'intelligence artificielle enfreint une autre législation de l'UE, y compris l'acquis de l'UE en matière de protection des données, de non-discrimination, de protection des consommateurs ou de concurrence.

Article 5, paragraphe 1, point d), article 5, paragraphes 2 à 4, Article 5, paragraphe 1, point e), et considérants 18 à 26	CA 11A

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

(i) la recherche ciblée de victimes potentielles spécifiques d'actes criminels, y compris les enfants disparus ;

(ii) la prévention d'une menace spécifique, substantielle et imminente contre la vie ou la sécurité physique de personnes physiques ou d'un attentat terroriste ; iii) la

détection, la localisation, l'identification ou la poursuite d'un auteur ou d'un suspect d'une infraction pénale visée à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI du Conseil62 et passible dans l'État membre concerné d'une peine privative de liberté ou d'une peine privative de liberté ordonnance de détention pour une durée maximale d'au moins trois ans, telle que déterminée par la législation de cet État membre.

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

a) la nature de la situation donnant lieu à l'utilisation éventuelle, notamment la gravité, la probabilité et l'ampleur du dommage causé en l'absence d'utilisation du système; b) les conséquences

de l'utilisation du système pour les droits et libertés de toutes les personnes concernées, notamment la gravité, la probabilité et l'ampleur de celles-ci conséquences

En outre, l'utilisation de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives pour l'un des objectifs visés au paragraphe 1, point d), respecte les garanties et conditions nécessaires et proportionnées en ce qui concerne l'utilisation, notamment en ce qui concerne les limitations temporelles, géographiques et personnelles En ce qui concerne les paragraphes 1,

3. point d) et 2, chaque utilisation individuelle à des fins répressives d'un système d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public est soumise à une autorisation préalable délivrée par une autorité judiciaire ou par une autorité administrative indépendante de l'État membre dans lequel l'utilisation doit avoir lieu, délivrée sur demande motivée et selon les modalités de droit national visées au paragraphe 4. Toutefois, dans une situation d'urgence dûment justifiée, l'utilisation du système peut être commencée sans autorisation et l'autorisation ne peut être demandée que pendant ou après l'utilisation. L'autorité judiciaire ou administrative compétente n'accorde l'autorisation que lorsqu'elle s'est assurée, sur la base de preuves objectives ou d'indications claires qui lui sont présentées, que l'utilisation du système d'identification biométrique à distance «en temps réel» en cause est nécessaire et proportionnée à la réalisation l'un des objectifs spécifiés au paragraphe 1, point d), tel qu'identifié dans la demande. Pour statuer sur la demande, l'autorité judiciaire ou administrative compétente tient compte des éléments visés au paragraphe 2.

4. Un État membre peut décider de prévoir la possibilité d'autoriser totalement ou partiellement l'utilisation de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives dans les limites et sous les conditions énumérées aux paragraphes 1 , point d), 2 et 3. Cet État membre établit dans sa législation nationale les modalités nécessaires pour la demande, la délivrance et l'exercice, selon

ainsi que la surveillance relative aux autorisations visées au paragraphe 3. Ces règles précisent également pour lesquels des objectifs énumérés au paragraphe 1, point d), y compris lesquelles des infractions pénales visées au point iii) de celui-ci , les autorités compétentes peuvent être autorisées à utiliser ces systèmes à des fins répressives

(C'est) la mise en service ou l'utilisation de systèmes d'intelligence artificielle pour l'analyse d'images enregistrées d'espaces accessibles au public par le biais de systèmes d'identification biométrique à distance «post», à moins qu'ils ne soient soumis à une autorisation préjudicielle conformément au droit de l'Union et strictement nécessaires à la recherche ciblée lié à une infraction pénale grave spécifique telle que définie à l'article 83, paragraphe 1, du TFUE qui a déjà eu lieu à des fins répressives.

(18) L'utilisation de systèmes d'intelligence artificielle pour l'identification biométrique à distance "en temps réel" de personnes physiques dans des espaces accessibles au public est particulièrement intrusive pour les droits et libertés des personnes concernées et peut, en définitive, affecter la vie privée d'une grande partie de la population, évoquent un sentiment de surveillance constante, donnent aux acteurs déployant l'identification biométrique dans les espaces accessibles au public une position de pouvoir incontrôlable et dissuadent indirectement l'exercice de la liberté de réunion et d'autres droits fondamentaux au cœur de l'État de droit. Les imprécisions techniques des systèmes d'IA destinés à l'identification biométrique à distance des personnes physiques peuvent conduire à des résultats biaisés et entraîner des effets discriminatoires. Ceci est particulièrement pertinent en ce qui concerne l'âge, l'origine ethnique, le sexe ou les handicaps. En outre, l'immédiateté de l'impact et les possibilités limitées de vérifications ou de corrections supplémentaires liées à l'utilisation de tels systèmes fonctionnant en "temps réel" comportent des risques accrus pour les droits et libertés des personnes concernées par les activités répressives . L'utilisation de ces systèmes dans des lieux accessibles au public devrait donc être interdite. De même, les systèmes d'intelligence artificielle utilisés pour l'analyse de séquences enregistrées d'espaces accessibles au public par le biais de systèmes d'identification biométrique à distance « post » devraient également être interdits, sauf autorisation préjudicielle d'utilisation dans le cadre de l'application de la loi, lorsque cela est strictement nécessaire pour les personnes ciblées. perquisition liée à une infraction pénale grave déterminée qui a déjà eu lieu, et uniquement sous réserve d'une autorisation préjudicielle.

(19) L'utilisation de ces systèmes à des fins répressives devrait donc être interdite, sauf dans trois situations limitativement énumérées et étroitement définies, dans lesquelles l'utilisation est strictement nécessaire pour atteindre un intérêt public substantiel, dont l'importance l'emporte sur les risques. Ces situations impliquent la recherche de victimes potentielles d'actes criminels, y compris des enfants disparus ; certaines menaces à la vie ou à la sécurité physique de personnes physiques ou d'un attentat terroriste ; et la détection, la localisation, l'identification ou la poursuite des auteurs ou suspects des infractions pénales visées dans la décision-cadre 2002/584/JAI du Conseil18 si ces infractions pénales sont passibles dans l'État membre concerné d'une peine privative de liberté ou d'une mesure de sûreté d'une durée maximale période d'au moins trois ans et tels qu'ils sont définis dans la législation de cet État membre.

Un tel seuil pour la peine privative de liberté ou l'ordonnance de placement en détention conformément au droit national contribue à garantir que l'infraction doit être suffisamment grave pour justifier potentiellement l'utilisation de systèmes d'identification biométrique à distance "en temps réel". De plus, sur les 32

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).

infractions pénales énumérées dans la décision-cadre 2002/584/JAI du Conseil, certaines sont en pratique susceptibles d'être plus pertinentes que d'autres, dans la mesure où le recours à l'identification biométrique à distance "en temps réel" sera vraisemblablement nécessaire et proportionné à des degrés très divers pour la poursuite concrète de la détection, de la localisation, de l'identification ou de la poursuite d'un auteur ou d'un suspect des différentes infractions pénales énumérées et compte tenu des différences probables dans la gravité, la probabilité et l'ampleur du préjudice ou des éventuelles conséquences négatives.

(20) Afin de garantir que ces systèmes sont utilisés de manière responsable et proportionnée, il est également important d'établir que, dans chacune de ces trois situations limitativement énumérées et étroitement définies, certains éléments doivent être pris en compte, notamment en ce qui concerne la nature de la situation à l'origine de la demande et les conséquences de l'utilisation pour les droits et libertés de toutes les personnes concernées et les garanties et conditions prévues avec l'utilisation. En outre, l'utilisation de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins répressives devrait être soumise à des limites appropriées dans le temps et dans l'espace, eu égard en particulier aux preuves ou indices concernant les menaces, la victimes ou auteurs. La base de données de référence des personnes doit être appropriée pour chaque cas d'utilisation dans chacune des trois situations mentionnées ci-dessus.

(21) Chaque utilisation d'un système d'identification biométrique à distance "en temps réel" dans des espaces accessibles au public à des fins répressives devrait être soumise à une autorisation expresse et spécifique d'une autorité judiciaire ou d'une autorité administrative indépendante d'un État membre. Cette autorisation doit en principe être obtenue préalablement à l'utilisation, sauf dans des situations d'urgence dûment justifiées, c'est-à-dire des situations où la nécessité d'utiliser les systèmes en question est telle qu'il est effectivement et objectivement impossible d'obtenir une autorisation avant de commencer utiliser. Dans de telles situations d'urgence, l'utilisation devrait être limitée au strict minimum nécessaire et soumise à des garanties et conditions appropriées, telles que déterminées dans le droit national et précisées dans le contexte de chaque cas d'utilisation urgente par l'autorité répressive elle-même.

En outre, l'autorité répressive devrait, dans de telles situations, chercher à obtenir une autorisation dans les meilleurs délais, tout en indiquant les raisons pour lesquelles elle n'a pas pu la demander plus tôt.

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

(23) L'utilisation de systèmes d'intelligence artificielle pour l'identification biométrique à distance "en temps réel" de personnes physiques dans des espaces accessibles au public à des fins répressives implique nécessairement le traitement de données biométriques. Les règles du présent règlement qui interdisent, sous réserve de certaines exceptions, une telle utilisation, qui sont fondées sur l'article 16 du TFUE, devraient s'appliquer en tant que lex specialis à l'égard des règles relatives au traitement des données biométriques prévues à l'article 10 de la directive (UE) 2016 /680, réglementant ainsi de manière exhaustive cette utilisation et le traitement des données biométriques concernées. Par conséquent, une telle utilisation et un tel traitement ne devraient être possibles que dans la mesure où ils sont compatibles avec le cadre fixé par le présent règlement, sans qu'il soit possible, en dehors de ce cadre, pour les autorités compétentes, lorsque

~~ils agissent à des fins répressives, utilisent ces systèmes et traitent les données y afférentes pour les motifs énumérés à l'article 10 de la directive (UE) 2016/680. Dans ce contexte, le présent règlement n'a pas pour objet de fournir la base juridique du traitement des données à caractère personnel au titre de l'article 8 de la directive 2016/680. Toutefois, l'utilisation de systèmes d'identification biométrique à distance «en temps réel» dans des espaces accessibles au public à des fins autres que répressives, y compris par les autorités compétentes, ne devrait pas être couverte par le cadre spécifique relatif à une telle utilisation à des fins répressives établi par la présente Régulation. Une telle utilisation à des fins autres que répressives ne devrait donc pas être soumise à l'exigence d'une autorisation au titre du présent règlement et des règles détaillées applicables du droit national qui peuvent lui donner effet.~~

(24) Tout traitement de données biométriques et d'autres données à caractère personnel impliqué dans l'utilisation de systèmes d'IA pour l'identification biométrique, autre qu'en rapport avec l'utilisation de systèmes d'identification biométrique à distance "en temps réel" dans des ~~espaces accessibles au public à des fins~~ répressives tels que réglementés par l~~e présent règlement, y compris lorsque ces systèmes sont utilisés par les autorités compétentes dans des espaces accessibles au public à des fins autre~~s que répressives, devraient continuer à se conformer à toutes les exigences résultant de l'article 9, paragraphe 1, du règlement (UE) 2016/679, de l'article 10(1) du règlement (UE) 2018/1725 et article 10 de la directive (UE) 2016/680, selon le cas.

(25) Conformément à l'article 6 bis du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au TUE et au TFUE, l'Irlande n'est pas liée par les règles prévues à l'article 5, paragraphe 1, points d), paragraphes 2 et 3, du présent règl~~ement, adop~~tées sur la base de l'article 16 du TFUE, qui concernent le traitement de données à caractère personnel par les États membres dans le cadre de l'exercice d'activités relevant du chapitre 4 ou du chapitre 5 du titre V de la troisième partie du TFUE, lorsque l'Irlande n'est pas liée par les règles régissant les formes de coopération judiciaire en matière pénale ou de coopération policière qui exigent le respect des dispositions prévues sur la base de l'article 16 du TFUE.

(26) Conformément aux articles 2 et 2 bis du protocole n° 22 sur la position du Danemark, annexé au TUE et au TFUE, le Danemark n'est pas lié par les règles énoncées à l'article 5, paragraphe 1, point d), (2) et (3) du pré~~sent règlemen~~t adoptés sur la base de l'article 16 du TFUE, ou soumis à leur application, qui ont trait au traitement de données à caractère personnel par les États membres lors de l'exercice d'activités relevant du champ d'application du chapitre 4 ou du chapitre 5 du titre V de la troisième partie du TFUE.

Article 3 – paragraphe 1 – points 1 à 44 i, 45 quater à 45 septies, articles 4, 4 bis et 4 quinquies, annexe I et considérants 6 à 9 ter	CA 12

(6) La notion de système d'IA dans le présent règlement devrait être clairement définie et étroitement alignée sur les travaux des organisations internationales travaillant sur l'intelligence artificielle afin de garantir la sécurité juridique, l'harmonisation et une large acceptation, tout en offrant la flexibilité nécessaire pour s'adapter aux évolutions technologiques rapides dans ce domaine. champ. De plus, il devrait être basé sur des caractéristiques clés de l'intelligence artificielle, telles que ses capacités d'apprentissage, de raisonnement ou de modélisation, afin de la distinguer des systèmes logiciels ou des approches de programmation plus simples. Les systèmes d'IA sont conçus pour fonctionner avec différents niveaux d'autonomie, ce qui signifie qu'ils ont au moins un certain degré d'indépendance des actions par rapport aux contrôles humains et qu'ils ont la capacité de fonctionner sans intervention humaine. Le terme "basé sur la machine" fait référence au fait que les systèmes d'IA fonctionnent sur des machines. La référence à des objectifs explicites ou implicites souligne que les systèmes d'IA peuvent fonctionner selon des objectifs explicites définis par l'homme ou selon des objectifs implicites. Les objectifs du système d'IA peuvent être différents de la finalité prévue du système d'IA dans un contexte spécifique. La référence aux prédictions inclut le contenu, qui est considéré dans le présent règlement comme une forme de prédiction comme l'un des résultats possibles produits par un système d'IA. Aux fins du présent règlement, les environnements doivent être compris comme les contextes dans lesquels les systèmes d'IA fonctionnent, tandis que les résultats générés par le système d'IA, c'est-à-dire les prévisions, les recommandations ou les décisions, répondent aux objectifs du système, sur la base des apports de ledit environnement. Une telle sortie influence en outre ledit environnement, même en y introduisant simplement de nouvelles informations.

(6 bis) Les systèmes d'IA disposent souvent de capacités d'apprentissage automatique qui leur permettent de s'adapter et d'effectuer de nouvelles tâches de manière autonome. L'apprentissage automatique fait référence au processus informatique d'optimisation des paramètres d'un modèle à partir de données, qui est une construction mathématique générant une sortie basée sur des données d'entrée. Les approches d'apprentissage automatique comprennent, par exemple, l'apprentissage supervisé, non supervisé et par renforcement, en utilisant une variété de méthodes, y compris l'apprentissage en profondeur avec des réseaux de neurones. Le présent règlement vise à faire face aux nouveaux risques potentiels qui pourraient survenir en déléguant le contrôle aux systèmes d'IA, en particulier aux systèmes d'IA susceptibles d'évoluer après le déploiement. La fonction et les sorties de bon nombre de ces systèmes d'IA sont basées sur des relations mathématiques abstraites difficiles à comprendre, à surveiller et à retracer pour les humains. Ces caractéristiques complexes et opaques (élément de la boîte noire) ont un impact sur la responsabilité et l'explicabilité. Des techniques comparativement plus simples telles que les approches fondées sur la connaissance, l'estimation bayésienne ou les arbres de décision peuvent également entraîner des lacunes juridiques qui doivent être comblées par le présent règlement, en particulier lorsqu'elles sont utilisées en combinaison avec des approches d'apprentissage automatique dans des systèmes hybride

(6 ter) Les systèmes d'IA peuvent être utilisés comme système logiciel autonome, intégré dans un produit physique (embarqué), utilisé pour assurer la fonctionnalité d'un produit physique sans

y être intégré (non embarqué) ou utilisé comme composant d'IA d'un système plus vaste. Si ce système plus vaste ne fonctionnait pas sans le composant d'IA en question, l'ensemble du système plus vaste devrait être considéré comme un système d'IA unique au titre du présent règlement.

(7) La notion de données biométriques utilisée dans le présent règlement est conforme à la notion de données biométriques telle que définie à l'article 4, paragraphe 14, du règlement (UE) 2016/679 du Parlement européen et du Conseil. Les données biométriques sont des données supplémentaires résultant d'un traitement technique spécifique relatif aux signaux physiques, physiologiques ou comportementaux d'une personne physique, tels que les expressions faciales, les mouvements, la fréquence du pouls, la voix, les frappes au clavier ou la démarche, qui peuvent ou non permettre ou confirmer la identification unique d'une personne physique.

(7 bis) La notion d'identification biométrique telle qu'elle est utilisée dans le présent règlement devrait être définie comme la reconnaissance automatisée de caractéristiques humaines physiques, physiologiques, comportementales et psychologiques telles que le visage, les mouvements des yeux, les expressions faciales, la forme du corps, la voix, la parole, la démarche , posture, fréquence cardiaque, tension artérielle, odeur, frappes au clavier, réactions psychologiques (colère, angoisse, chagrin, etc.) dans le but d'établir l'identité d'un individu en comparant les données biométriques de cet individu aux données biométriques stockées d'individus dans une base de données (identification un-à-plusieurs), que la personne ait donné son consentement ou non.

(7 ter) La notion de catégorisation biométrique telle qu'utilisée dans le présent règlement devrait être définie comme l'attribution de personnes physiques à des catégories spécifiques ou la déduction de leurs caractéristiques et attributs tels que le sexe, le sexe, l'âge, la couleur des cheveux, la couleur des yeux, les tatouages, l'origine ethnique ou sociale, santé, capacité mentale ou physique, comportement ou personnalité, traits de caractère langue, religion ou appartenance à une minorité nationale ou orientation sexuelle ou politique sur la base de leurs données biométriques ou biométriques, ou qui peuvent être déduites de ces données

(8) La notion de système d'identification biométrique à distance telle qu'elle est utilisée dans le présent règlement devrait être définie de manière fonctionnelle, comme un système d'IA destiné à l'identification de personnes physiques à distance par la comparaison des données biométriques d'une personne avec les données biométriques contenues dans une référence base de données, et sans savoir au préalable si la personne ciblée sera présente et pourra être identifiée, quels que soient la technologie, les processus ou les types de données biométriques utilisés, à l'exclusion des systèmes de vérification qui se contentent de comparer les données biométriques d'un individu aux données biométriques fournies précédemment (Un par un). Compte tenu de leurs différentes caractéristiques et modalités d'utilisation, ainsi que des différents risques encourus, il convient de distinguer les systèmes d'identification biométrique à distance «en temps réel» et «post». Dans le cas des systèmes « temps réel », la saisie des données biométriques, la comparaison et l'identification se font de manière instantanée, quasi instantanée ou en tout cas sans délai significatif. À cet égard, il ne devrait y avoir aucune possibilité de contourner les règles du présent règlement relatives à l'utilisation «en temps réel» des systèmes d'IA en question en prévoyant des retards mineurs. Les systèmes 'en temps réel' impliquent l'utilisation de matériel 'en direct' ou 'quasi-'en direct', tel que des séquences vidéo, généré par une caméra ou un autre dispositif doté de fonctionnalités similaires. Dans le cas des systèmes «post», en revanche, les données biométriques ont déjà été saisies et la comparaison et l'identification n'interviennent qu'après un délai important. Il s'agit de matériel, tel que des images ou des séquences vidéo générées par des caméras de télévision en circuit fermé ou des appareils privés, qui ont été générées avant l'utilisation du système à l'égard des personnes physiques concernées. Étant donné que la notion de biométrie

l'identification est indépendante du consentement de l'individu, cette définition s'applique même lorsque des avis d'avertissement sont placés dans le lieu sous surveillance du système d'identification biométrique à distance, et n'est pas annulée de facto par le pré-enrôlement.

(8 bis) L'identification des personnes physiques à distance s'entend comme une distinction entre les systèmes d'identification biométrique à distance et les systèmes de vérification individuelle à proximité utilisant des moyens d'identification biométrique, dont le seul but est de confirmer si une personne physique spécifique se présentant pour identification est autorisée ou non, par exemple pour accéder à un service, un appareil ou des locaux.

(9) Aux fins du présent règlement, la notion d'espace accessible au public doit être comprise comme faisant référence à tout lieu physique accessible au public, que le lieu en question soit privé ou public et quelles que soient les éventuelles restrictions de capacité. Par conséquent, la notion ne couvre pas les lieux qui sont de nature privée et normalement pas librement accessibles aux tiers, y compris les autorités chargées de l'application de la loi, sauf si ces parties ont été spécifiquement invitées ou autorisées, telles que les maisons, les clubs privés, les bureaux, les entrepôts et les usines. Les espaces en ligne ne sont pas couverts non plus, car ce ne sont pas des espaces physiques. Toutefois, le simple fait que certaines conditions d'accès à un espace particulier puissent s'appliquer, telles que des billets d'entrée ou des restrictions d'âge, ne signifie pas que l'espace n'est pas accessible au public au sens du présent règlement. Par conséquent, outre les espaces publics tels que les rues, les parties concernées des bâtiments gouvernementaux et la plupart des infrastructures de transport, des espaces tels que les cinémas, les théâtres, les terrains de sport, les écoles, les universités, les parties concernées des hôpitaux et des banques, les parcs d'attractions, les festivals, les magasins et les centres commerciaux les centres sont normalement également accessibles au public. L'accessibilité d'un espace donné au public doit toutefois être déterminée au cas par cas, en tenant compte des spécificités de la situation individuelle en cause.

(9 bis) Il est important de noter que les systèmes d'IA devraient s'efforcer de respecter les principes généraux établissant un cadre de haut niveau qui promeut une approche cohérente centrée sur l'humain pour une IA éthique et digne de confiance, conformément à la Charte des droits de l'homme.
Droits fondamentaux de l'Union européenne et les valeurs sur lesquelles l'Union est fondée, y compris la protection des droits fondamentaux, l'action humaine et la surveillance, la robustesse et la sécurité techniques, la confidentialité et la gouvernance des données, la transparence, la non-discrimination et l'équité et le bien-être sociétal et environnemental

(9 ter) La «connaissance de l'IA» fait référence aux compétences, aux connaissances et à la compréhension qui permettent aux fournisseurs, aux utilisateurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le cadre du présent règlement, de procéder à un déploiement éclairé des systèmes d'IA, ainsi que prendre conscience des opportunités et des risques de l'IA et des dommages éventuels qu'elle peut causer et ainsi promouvoir son contrôle démocratique. La connaissance de l'IA ne devrait pas se limiter à l'apprentissage des outils et des technologies, mais devrait également viser à doter les fournisseurs et les utilisateurs des notions et des compétences nécessaires pour garantir le respect et l'application du présent règlement. Il est donc nécessaire que la Commission, les États membres ainsi que les fournisseurs et les utilisateurs de systèmes d'IA, en coopération avec toutes les parties prenantes concernées, favorisent le développement d'un niveau suffisant de connaissances en matière d'IA, dans tous les secteurs de la société, pour les personnes de tous âges , y compris les femmes et les filles, et que les progrès à cet égard sont suivis de près.

Article 3

Définitions

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

(1) « système d'intelligence artificielle » (système d'IA), un système basé sur une machine conçu pour fonctionner avec différents niveaux d'autonomie et qui peut, pour des objectifs explicites ou implicites, générer des résultats tels que des prédictions, des recommandations ou des décisions dans des environnements virtuels ou physiques.

(1a) "risque", la combinaison de la probabilité d'occurrence d'un dommage et de la gravité de ce dommage ;

(1b) "risque significatif", un risque qui est significatif en raison de la combinaison de sa gravité, de son intensité, de sa probabilité d'occurrence et de la durée de ses effets, et de sa capacité à affecter un individu, plusieurs personnes ou à affecter une personne en particulier groupe de personnes;

(1c) « modèle de base », un modèle d'IA qui est formé sur de vastes données à grande échelle, est conçu pour la généralité des résultats et peut être adapté à un large éventail de tâches distinctes ;

(1j) "système d'IA à usage général", un système d'IA qui peut être utilisé et adapté à un large éventail d'applications pour lesquelles il n'a pas été intentionnellement et spécifiquement conçu ;

(1e) "grandes séries d'entraînement" désigne le processus de production d'un puissant modèle d'IA qui nécessite des ressources informatiques au-dessus d'un seuil très

(2) élevé. "fournisseur": une personne physique ou morale, une autorité publique, une agence ou un autre organisme qui développe un système d'IA ou qui fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, que ce soit à titre onéreux ou gratuit ;

(3) ~~"petit fournisseur": un fournisseur qui est une micro ou une petite entreprise au sens de la recommandation 2003/361/E de la Commission~~

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

(5) «représentant autorisé», toute personne physique ou morale établie dans l'Union qui a reçu un mandat écrit d'un fournisseur d'un système d'IA pour, respectivement, exécuter et exécuter en son nom les obligations et les procédures établies par le présent Régulation;

(6) "importateur", toute personne physique ou morale établie dans l'Union qui met sur le marché ou met en service un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie en dehors de l'Union ;

(7) "distributeur": toute personne physique ou morale de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur, qui met un système d'IA à disposition sur le marché de l'Union sans affecter ses propriétés ;

(8) "opérateur", le fournisseur, le déployeur, le mandataire, l'importateur et le distributeur ;

(8a) "personne affectée": toute personne physique ou groupe de personnes qui sont soumises ou autrement affectées par un système d'IA ;

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

(dix) «mise à disposition sur le marché», toute fourniture d'un système d'IA en vue de sa distribution ou de son utilisation sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit;

(11) «mise en service», la fourniture d'un système d'IA pour une première utilisation directement au déployeur ou pour son propre usage sur le marché de l'Union aux fins prévues ;

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

(13) "utilisation abusive raisonnablement prévisible": l'utilisation d'un système d'IA d'une manière qui n'est pas conforme à sa destination, comme indiqué dans les instructions d'utilisation établies par le fournisseur, mais qui peut résulter d'un comportement humain raisonnablement prévisible ou d'une interaction avec d'autres systèmes, y compris d'autres systèmes d'IA ;

14) "composant de sécurité d'un produit ou d'un système", conformément à la législation d'harmonisation de l'Union énumérée à l'annexe II, un composant d'un produit ou d'un système qui remplit une fonction de sécurité critique pour ce produit ou système, ou la défaillance ou dont le dysfonctionnement met en danger la santé et la sécurité des personnes ou des biens

(15) "instructions d'utilisation", les informations fournies par le fournisseur pour informer le déployeur, notamment, de la destination et de l'utilisation correcte d'un système d'IA, ainsi que des informations sur les précautions à prendre ; y compris le cadre géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé ;

(16) « rappel d'un système d'IA », toute mesure visant à obtenir le retour au fournisseur d'un système d'IA qui a été mis à la disposition des déployeurs ;

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

(18) "performance d'un système d'IA", la capacité d'un système d'IA à atteindre l'objectif auquel il est destiné ;

(19) "autorité notifiante": l'autorité nationale responsable de la mise en place et de la mise en œuvre des 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», le processus visant à démontrer si les exigences énoncées au titre III, chapitre 2, du présent règlement relatives à un système d'IA ont été respectées;

(21) « organisme d'évaluation de la conformité », un organisme qui effectue des activités d'évaluation de la conformité par un tiers, y compris les essais, la certification et l'inspection ;

(22) «organisme notifié», un organisme d'évaluation de la conformité notifié conformément au présent règlement et autre législation d'harmonisation pertinente de l'Union ;

(23) "modification substantielle", une modification ou une série de modifications du 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 des risques par le fournisseur et à la suite de quoi la conformité du système d'IA aux exigences énoncées au titre III, chapitre 2, du le présent règlement est affecté ou entraîne une modification de la destination pour laquelle le système d'IA a été évalué

(24) «marquage CE de conformité» (marquage CE), un marquage physique ou numérique par lequel un fournisseur indique qu'un système d'IA ou un produit avec un système d'IA intégré est conforme aux exigences énoncées au titre III, chapitre 2, du présent règlement et autre législation applicable de l'Union harmonisant les conditions de commercialisation des produits («législation d'harmonisation de l'Union») prévoyant son apposition;

(25) «surveillance après commercialisation», toutes les activités menées par les fournisseurs de systèmes d'IA pour collecter et examiner de manière proactive l'expérience acquise lors de l'utilisation des systèmes d'IA qu'ils mettent sur le marché ou mettent en service dans le but d'identifier tout besoin d'appliquer immédiatement les mesures nécessaires les actions correctives ou préventives ;

(26) «autorité de surveillance du marché», l'autorité nationale exerçant les activités et prenant les mesures conformément au règlement (UE) 2019/1020;

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

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

(29) « données d'entraînement », les données utilisées pour l'entraînement d'un système d'IA en ajustant ses paramètres app~~renables, y compris les poids d'un réseau de neurone~~s ;

(30) « données de validation », les données utilisées pour fournir une évaluation du système d'IA formé et pour régler ses paramètres non apprenables et son processus d'apprentissage, entre autres, afin d'éviter un sous-ajustement ou un surajustement ; considérant que l'ensemble de données de validation est un ensemble de données distinct ou fait partie de l'ensemble de données d'apprentissage, soit en tant que division fixe ou variable ;

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

(32) « données d'entrée », les données fournies à ou directement acquises par un système d'IA sur la base desquelles le système produit un résultat ;

(33) «données biométriques», les données biométriques telles que définies à l'article 4, point 14), du Règlement (UE) 2016/679 ; les don~~nées à caractère personnel résultant de traitements techniques spécifiques relatifs aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment l'identification unique de cette personne physique, telles que des images faciales ou des données dactyloscopique~~s ;

(33 bis) "données biométriques": les données résultant d'un traitement technique spécifique relatives aux signaux physiques, physiologiques ou comportementaux d'une personne physique; –

(33 ter) "identification biométrique": la reconnaissance automatisée de caractéristiques humaines physiques, physiologiques, comportementales et psychologiques aux fins d'établir l'identité d'un individu en comparant les données biométriques de cet individu aux données biométriques stockées des individus dans une base de données (un à un -nombreuses pièces d'identité);

(33c) "vérification biométrique", la vérification automatisée de l'identité de personnes physiques en comparant les données biométriques d'un individu aux données biométriques fournies précédemment (vérification individuelle, y compris l'authentification)

(33e) "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 ;

(34) "système de reconnaissance des émotions", un système d'intelligence artificielle destiné à identifier ou à déduire les émotions, les pensées, les états d'esprit ou les intentions d'individus ou de groupes sur la base de leurs données biométriques et biométriques ;

(35) «la catégorisation biométrique consiste à affecter des personnes physiques à des catégories spécifiques, ou à déduire leurs caractéristiques et attributs sur la base de leurs données biométriques ou fondées sur la biométrie, ou qui peuvent être déduites de ces données;

(36) «système d'identification biométrique à distance», un système d'IA destiné à identifier des personnes physiques à distance par la comparaison des données biométriques d'une personne avec les données biométriques contenues dans une base de données de référence, et sans que le déployeur du système d'IA ne sache au préalable si la personne sera présente et pourra être identifiée, hors systèmes de vérification

(37) « système d'identification biométrique à distance en temps réel », un système d'identification biométrique à distance dans lequel la saisie des données biométriques, la comparaison et l'identification se produisent toutes sans retard significatif. Cela comprend non seulement une identification instantanée, mais égal~~ement~~ des délais courts limités afin d'éviter le contournement.

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

(39) "espace accessible au public": tout lieu physique public ou privé accessible au public, que certaines conditions d'accès puissent s'appliquer ou non, et quelles que soient les restrictions de capacité potentielles ;

(40) « autorité chargée de l'application de la loi » signifie :

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

b) tout autre organisme ou entité chargé par le droit d'un État membre d'exercer l'autorité publique et les pouvoirs publics aux fins de la prévention, de la recherche, de la détection ou de la poursuite d'infractions pénales ou de l'exécution de sanctions pénales, y compris la protection contre et la prévention de menaces à la sécurité publique;

(41) "application de la loi": les activités menées par les autorités chargées de l'application de la loi ou en leur nom pour la prévention, l'enquête, la détection ou la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la protection contre et la prévention des menaces à la sécurité publique ;

(42) «autorité nationale de surveillance», une autorité publique à laquelle un État membre confie la responsabilité de la mise en œuvre et de l'application du présent règlement, de la coordination des activités confiées à cet État membre, de la fonction de point de contact unique pour la Commission et de la représentation l'État membre au sein du conseil d'administration de l'Office AI ;

(43) "autorité nationale compétente", toute autorité nationale chargée de l'application du présent règlement,

(44) « incident grave » désigne tout incident ou dysfonctionnement d'un système d'IA qui entraîne directement ou indirectement, aurait pu entraîner ou pourrait entraîner l'un des événements suivants :

(a) le décès d'une personne ou une atteinte grave à la santé d'une personne, à ~~des biens ou à l'environnement, (b)~~
une perturbation ~~grave et irréversible~~ de la gestion et de l'exploitation d'infrastructures critiques.
(b bis) une violation des
droits fondamentaux protégés par le droit de l'Union ; (bb) des dommages graves
aux biens ou à l'environnement ;

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

(44 ter) "données non personnelles", des données autres que des données personnelles ;

(44 quater) "profilage", toute forme de traitement automatisé de données à caractère personnel au sens de l'article 4, point 4), du règlement (UE) 2016/679; ou dans le cas des autorités répressives – au point 4 de l'article 3 de la directive (UE) 2016/680 ou, dans le cas de
Institutions, organes ou organismes de l'Union, au point 5 de l'article 3 du règlement (UE) 2018/1725 ;

(44 quinquies) "deep fake": un contenu audio, image ou vidéo manipulé ou synthétique qui semblerait faussement authentique ou véridique, et qui présente des représentations de personnes semblant dire ou faire des choses qu'elles n'ont pas dites ou faites, produites à l'aide de techniques d'intelligence artificielle , y compris l'apprentissage automatique et l'apprentissage en profondeur ; .

(44 sexies) "infraction généralisée":

(un) tout acte ou omission contraire au droit de l'Union qui protège les intérêts des particuliers, qui a porté atteinte ou est susceptible de porter atteinte aux intérêts collectifs de personnes résidant dans au moins deux États membres autres que l'État membre
État, dans lequel :

(i) l'acte ou l'omission est né ou a eu lieu ;

(ii) le prestataire concerné ou, le cas échéant, son mandataire est établi ; ou,

(iii) le déployeur est constitué, lorsque l'infraction est commise par le déployeur ;

(b) tous les actes ou omissions contraires au droit de l'Union qui protègent les intérêts des particuliers, qui ont porté atteinte, portent atteinte ou sont susceptibles de porter atteinte aux intérêts collectifs des personnes et qui présentent des caractéristiques communes, notamment la même pratique illicite, le même intérêt violés et qui se produisent simultanément, commis par le même opérateur, dans au moins trois États membres
États;

(44 septies) "infraction de grande ampleur de dimension européenne": une infraction de grande ampleur qui a porté atteinte ou est susceptible de porter atteinte aux intérêts collectifs de particuliers dans au moins les deux tiers des États membres, représentant ensemble au moins les deux tiers des la population de l'Union.

(44 nonies) "bac à sable réglementaire": un environnement contrôlé établi par une autorité publique qui facilite le développement, l'essai et la validation en toute sécurité 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 en vertu de la réglementation surveillance;

(44 decies) "infrastructure critique": un actif, une installation, un équipement, un réseau ou un système, ou une partie d'un actif, d'une installation, d'un équipement, d'un réseau ou d'un système, qui est nécessaire à la fourniture d'un service essentiel au sens de l'article 2, paragraphe 4, de la directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques ;

(45 quater) «notation sociale», l'évaluation ou la classification de personnes physiques sur la base de leur comportement social, de leur statut socio-économique ou de caractéristiques personnelles ou de personnalité connues ou prévues;

(45 quinquies) "comportement social", la manière dont une personne physique interagit avec d'autres personnes physiques ou la société et les influence;

(45 sexies) "état de la technique": le stade de développement de la capacité technique à un moment donné en ce qui concerne les produits, les processus et les services, sur la base des résultats consolidés pertinents de la science, de la technologie et de l'expérience ;

(45 septies) "essais dans des conditions réelles": les essais temporaires d'un système d'IA pour l'usage auquel il est destiné dans des conditions réelles en dehors d'un laboratoire ou d'un autre environnement simulé ;

~~Article 4~~

~~Amendements à l'annexe I~~

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

Article 4 bis

Principes généraux applicables à tous les systèmes d'IA

1. Tous les opérateurs relevant du présent règlement s'efforcent de développer et d'utiliser des systèmes d'IA ou des modèles de base conformément aux principes généraux suivants établissant un cadre de haut niveau qui promeut une approche européenne cohérente centrée sur l'humain en matière d'intelligence artificielle éthique et digne de confiance, qui est pleinement conforme à la Charte ainsi qu'aux valeurs sur lesquelles l'Union est fondée:

a) « agence et surveillance humaines » signifie que les systèmes d'IA doivent être développés et utilisés comme un outil qui sert les personnes, respecte la dignité humaine et l'autonomie personnelle, et qui fonctionne d'une manière qui peut être contrôlée et supervisée de manière appropriée par des humains. b) «robustesse et sécurité techniques» signifie que les systèmes d'IA doivent être développés et utilisés de manière à minimiser les dommages involontaires et inattendus, tout en étant robustes en cas de problèmes imprévus et en étant résistants aux tentatives de modification de l'utilisation ou des performances de l'IA système afin de permettre une utilisation illicite par des tiers malveillants. c) « vie privée et gouvernance des données » signifie que les systèmes d'IA doivent être développés et utilisés conformément aux règles existantes en matière de confidentialité et de protection des données, tout en traitant des données qui répondent à des normes élevées en termes de qualité et d'intégrité. d) "transparence": les systèmes d'IA doivent être développés et utilisés de manière à permettre une traçabilité et une explicabilité appropriées, tout en informant les humains qu'ils communiquent ou interagissent avec un système d'IA et en informant dûment les utilisateurs des capacités et des limites de ce système système d'IA et les personnes concernées sur leurs droits. e) "diversité, non-discrimination et équité": les systèmes d'IA doivent être développés et utilisés de manière à inclure divers acteurs et à promouvoir l'égalité d'accès, l'égalité des sexes et la diversité culturelle, tout en évitant les effets discriminatoires et les préjugés injustes interdits par l'Union ou la législation nationale. f) « bien-être social et environnemental » signifie que les systèmes d'IA doivent être développés et utilisés d'une manière durable et respectueuse de l'environnement ainsi que d'une manière qui profite à tous les êtres humains, tout en surveillant et en évaluant les impacts à long terme sur l'individu , société et démocratie.

2. Le paragraphe 1 est sans préjudice des obligations établies par le droit de l'Union et le droit national en vigueur. Pour les systèmes d'IA à haut risque, les principes généraux sont traduits et respectés par les fournisseurs ou les déployeurs au moyen des exigences énoncées aux articles 8 à 15 et des obligations respectives énoncées au chapitre 3 du titre III du présent règlement.
Pour les modèles de fondation, les principes généraux sont traduits et respectés par les prestataires au travers des exigences prévues aux articles 28 à 28b. Pour tous les systèmes d'IA, l'application des principes visés au paragraphe 1 peut être réalisée, selon le cas, par les dispositions de l'article 28, de l'article 52, ou par l'application de normes harmonisées, de spécifications techniques et de codes de conduite visés à l'article l'article 69, sans créer de nouvelles obligations au titre du présent règlement.

3. La Commission et l'Office de l'IA intègrent ces principes directeurs dans les demandes de normalisation ainsi que des recommandations consistant en des orientations techniques pour aider les fournisseurs et les déployeurs sur la manière de développer et d'utiliser des systèmes d'IA.
Les organismes européens de normalisation tiennent compte des principes généraux visés au paragraphe 1 en tant qu'objectifs axés sur les résultats lors de l'élaboration des normes harmonisées appropriées pour les systèmes d'IA à haut risque visés à l'article 40, paragraphe 2 ter.

Article 4d

Littératie en IA

1. Lors de la mise en œuvre du présent règlement, l'Union et les États membres promeuvent des mesures visant à développer un niveau suffisant de connaissances en IA, dans tous les secteurs et en tenant compte des différents besoins des groupes de prestataires, de déployeurs et de personnes concernées concernés, y compris par l'éducation et la formation , des programmes de formation et de reconversion et tout en garantissant un bon équilibre entre les sexes et les âges, en vue de permettre un contrôle démocratique des systèmes d'IA.

2. Les fournisseurs et les déployeurs de systèmes d'IA prennent des mesures pour garantir un niveau suffisant de connaissances en matière d'IA de leur personnel et des autres personnes chargées de l'exploitation et de l'utilisation des systèmes d'IA en leur nom, en tenant compte de leurs connaissances techniques, de leur expérience, de leur éducation et de leur formation et de la contexte dans lequel les systèmes d'IA doivent être utilisés et compte tenu des personnes ou des groupes de personnes sur lesquels les systèmes d'IA doivent être utilisés.

3. Ces mesures d'alphabétisation consistent notamment en l'enseignement de notions et de compétences de base sur les systèmes d'IA et leur fonctionnement, y compris les différents types de produits et d'utilisations, leurs risques et leurs avantages.

4. Un niveau suffisant de connaissances en matière d'IA est un niveau qui contribue, si nécessaire, à la capacité des fournisseurs et des déployeurs à assurer le respect et l'application du présent règlement.

ANNEXE I

~~TECHNIQUES ET APPROCHES D'INTELLIGENCE ARTIFICIELLE visées à l'article 3, point 1~~

~~(b) Approches d'apprentissage automatique, y compris l'apprentissage supervisé, non supervisé et par renforcement, utilisant une grande variété de méthodes, y compris l'apprentissage~~

~~(c) en profondeur ; Approches basées sur la logique et les connaissances, y compris la représentation des connaissances, la programmation inductive (logique), les bases de connaissances, les moteurs d'inférence et déductifs, le raisonnement (symbolique) et les~~

~~(d) systèmes experts ; Approches statistiques, estimation bayésienne, méthodes de recherche et d'opt~~imisation.