

RÉGLEMENT SUR L'INTELLIGENCE ARTIFICIELLE

AI ACT

Analyse Détaillée

Octobre 2024



ACN

Alliance pour la confiance numérique

SOMMAIRE

INTRODUCTION	1.
I - LA DÉFINITION DES SYSTÈMES D'INTELLIGENCE ARTIFICIELLE (SIA) ET LEUR CONTRÔLE : UNE APPROCHE GRADUÉE PAR LES RISQUES	3.
A - Des pratiques interdites et fortement condamnée	3.
B - Des pratiques contrôlées : l'utilisation de SIA à haut risque et de modèles d'IA à usage général	4.
C - Un contrôle sophistiqué assuré par une gouvernance à plusieurs échelles	5.
II - L'ENCADREMENT RIGOUREUX DES SIA À HAUT RISQUE ET DES MODÈLES D'IA À USAGE GÉNÉRAL	9.
A - De strictes exigences pour les SIA à haut risque et leur fournisseur	9.
B - La démonstration de la conformité du SIA à haut risque	12.
C - Le traitement particulier des modèles d'IA à usage général	13.
III - LE SOUTIEN À L'INNOVATION POUR L'ENSEMBLE DES SIA	15.
A - La création de bacs à sable réglementaire pour tester les SIA	15.
B - Une obligation de transparence pour tous les SIA	16.
C - Un encouragement à l'adoption volontaire d'exigences plus strictes	17.
CONCLUSION	18.
ANNEXES	20.

INTRODUCTION

Le règlement sur l'intelligence artificielle (IA)¹, ou *AI Act*, a été officiellement publié au journal officiel de l'UE le 12 juillet 2024 et est entré en vigueur le 1er août 2024. Ce règlement s'adresse à l'ensemble des opérateurs de système d'intelligence artificielle (SIA) qui mettent sur le marché européen ou en service (ci-après « mis sur le marché ») des systèmes d'IA (SIA) et des modèles d'IA à usage général.

L'IA, en tant que technologie aux usages multiples, fait l'objet de pratiques hétérogènes. Afin de les harmoniser, l'*AI Act* établit des règles relatives au développement et à l'utilisation de SIA au sein de l'UE. L'objectif est de faire prospérer une IA axée sur l'humain et digne de confiance. Au-delà d'une harmonisation des règles relatives à l'utilisation de l'IA, l'*AI Act* vient poser les fondements d'une réglementation en matière d'IA qui n'existe pas au sein des Etats membres. Première de son genre, elle apporte en réalité de nombreuses réponses aux interrogations posées par cette nouvelle technologie.

Le règlement vient notamment poser une première définition de l'intelligence artificielle longtemps débattue. Il la définit sous un angle technologique comme « *un système automatisé [...] conçu pour fonctionner à différents niveaux d'autonomie et [qui] peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs*

explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, quedes prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnement physiques ou virtuels » (article 3.1).

En complément de cette définition technique, l'*AI Act* retient qu'en fonction de son contexte d'utilisation, l'IA peut être source de risques pour les droits fondamentaux européens promus par la Charte européenne des droits de l'Homme. L'*AI Act* considère, par exemple, que l'utilisation de SIA de notation sociale dans certains contextes (système qui évalue ou classe les personnes en fonction de plusieurs points de données liées à leur comportement social) peut conduire à l'exclusion de certains groupes (considérant 31) et peut porter atteinte aux droits à la dignité et à la non-discrimination.

L'*AI Act* vient donc réguler l'usage de la technologie plutôt que la technologie elle-même. Pour réguler l'usage de l'IA et faire prospérer en Europe une IA digne de confiance, l'UE fait le choix de compléter sa définition technique par une dimension éthique qui met en équilibre la protection des droits fondamentaux et le contexte d'utilisation.

¹ RÈGLEMENT (UE) 2024/1689 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle). Disponible sur le lien suivant : https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=OJ:L_202401689

Aussi, lors de l'élaboration de l'*AI Act*, le monde a vu émerger l'IA générative, un sous-groupe de l'IA capable de générer du texte, des images ou encore des vidéos en réponse à une demande écrite ou vocale. Pour compléter les travaux sur l'IA qui étaient en cours, l'UE a fait le choix de réguler l'IA générative en encadrant l'utilisation des modèles d'IA qui font fonctionner l'IA générative. L'*AI Act* a donc été mis à jour au moment d'entrer en trilogue pour intégrer la notion de « modèle d'IA à usage général ». De la même manière que pour les SIA, l'*AI Act* régule l'utilisation de ces modèles et mettant en balance la protection des droits fondamentaux et le contexte d'utilisation. Cependant, pour s'assurer que la régulation de ces modèles soit effective, l'*AI Act* confie la surveillance des risques qu'ils peuvent générer à un groupe d'experts.

Ainsi, plus le risque induit par l'IA est important, plus les obligations sont fortes et plus leur non-respect a de conséquences. En effet, l'*AI Act* vient sanctionner le non-respect à ses dispositions par des amendes records : l'utilisation d'un SIA interdit par le règlement entraîne une sanction pouvant aller jusqu'à 7% du chiffre d'affaires annuel mondial de l'entreprise concernée ou trente-cinq millions d'euros.

Cependant, pour promouvoir une IA digne de confiance, il faut également soutenir son développement et la structuration d'une filière de l'IA européenne forte. L'*AI Act* ne se contente donc pas d'imposer aux fournisseurs d'IA le respect de ses exigences mais vient également soutenir l'innovation en matière d'IA, notamment pour les plus petites structures.

Des mécanismes sont prévus pour que la mise en conformité avec le règlement ne soit pas financièrement handicapante pour les PME et pour que les SIA et les modèles d'IA puissent être testés sereinement.

Par conséquent, l'*AI Act* affiche un double objectif : s'assurer que l'IA développée en Europe comporte une dimension éthique et que ces IA fassent référence internationalement. Pour y parvenir, l'*AI Act* vient définir les SIA et leur contrôle en faisant le choix d'une approche par les risques. Le texte se concentrant sur les SIA à haut risque et les modèles d'IA à usage général, ceux-ci doivent respecter un certain nombre d'exigences strictes et prouver qu'ils y sont conformes. Enfin, l'*AI Act* pose un cadre de soutien à l'innovation pour tous les SIA développés en UE.

La définition des systèmes d'intelligence artificielle (SIA) et leur contrôle : une approche graduée par les risques

Dans un premier temps, l'AI Act pose plusieurs définitions : celle des pratiques interdites, des pratiques à risques et de la gouvernance de l'IA au sein de l'Union Européenne (UE).

A - Des pratiques interdites et fortement condamnées

Certaines pratiques en matière d'IA sont interdites par l'AI Act car elles sont considérées comme dangereuses pour les droits et libertés des citoyens européens. La Commission européenne vient interdire les SIA délibérément manipulateurs (à comprendre comme des systèmes opérant de la manipulation cognitivo comportementale), les SIA exploitant les vulnérabilités d'une personne dans le but de l'influencer ou de lui causer des préjudices physiques ou psychologiques (article 5). Plus concrètement, l'AI Act interdit la notation sociale, le profilage pour déterminer la probabilité qu'une infraction pénale soit commise, l'évaluation des émotions dans les espaces de travail et les institutions d'éducation (sauf pour des raisons de sûreté) et la catégorisation biométrique.

La Commission interdit également la reconnaissance faciale en « temps réel » dans des espaces accessibles au public à des fins répressives, sauf dans certains cas. Les forces de l'ordre peuvent user de l'identification biométrique seulement pour :

- La recherche ciblée de victimes d'enlèvement et de personnes disparues, de la traite et de l'exploitation sexuelle d'êtres humains,
- La prévention d'une d'attaque terroriste,
- La localisation ou l'identification d'une personne soupçonnée d'avoir commis une infraction pénale punissable d'une peine d'au moins quatre ans.

L'utilisation de SIA d'identification biométrique en temps réel doit être proportionnée au contexte (gravité, probabilité et ampleur du préjudice) et aux possibles conséquences sur les droits et libertés des personnes concernées (article 5.2). L'utilisation de ces SIA est également conditionnée à la réalisation d'une analyse d'impact sur les droits fondamentaux, à l'enregistrement de ce système dans la base de données consacrées de l'UE et à l'obtention d'une autorisation judiciaire préalable, sauf en cas d'urgence (article 5.3).

Les Etats membres définissent ensuite les règles applicables à l'utilisation des SIA d'identification biométrique « en temps réel » dans les espaces publics.

Dans le cas où ces interdictions ne seraient pas respectées, l'entreprise concernée s'expose à une amende allant jusqu'à trente-cinq millions d'euros ou 7% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Si cette infraction est commise par une institution, un organe ou un organisme de l'UE, l'amende maximale est d'un million et demi d'euros. C'est la sanction la plus importante posée par l'AI Act. En parallèle de la définition de ces interdictions, le règlement identifie et autorise d'autres pratiques à risques qu'il vient strictement encadrer.

B - Des pratiques contrôlées : l'utilisation de SIA à haut risque et de modèles d'IA à usage général

L'approche par les risques (défini comme « la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci » à l'article 3.1) retenue par la Commission européenne signifie qu'elle considère que, combinés à certains contextes, certains SIA présentent un risque pour les droits fondamentaux des utilisateurs.

Il existe deux groupes de SIA à haut risque. Tout d'abord, un SIA à haut risque est un SIA qui :

- Est un produit ou un composant de sécurité d'un produit au sens de la législation européenne harmonisée sur la sécurité des produits et des équipements (annexe I Section A du règlement),
- Et qui doit faire l'objet d'une évaluation de conformité par un tiers (article 6.1).

Pour ces systèmes, une implication indirecte est prévue. Les textes référant à ces domaines techniques devront être adaptés à l'AI Act par les autorités de régulation compétentes.

Ensuite, en plus des SIA couverts par la législation sur la sécurité des produits et des équipements, la Commission liste un ensemble de domaines dans lesquels l'utilisation d'un SIA est à haut risque. Les domaines retenus sont les domaines stratégiques des politiques sociales et économiques : l'éducation, l'emploi, l'accès aux services privés essentiels et aux prestations sociales essentielles, la répression, la migration, l'asile et la gestion des frontières, ainsi que l'administration de la justice et des processus démocratiques. En plus de ces domaines, une attention particulière est portée au domaine de la biométrie (annexe III point 1 du règlement). La liste de ces domaines sera mise à jour annuellement par la Commission (article 112).

A l'inverse, les SIA utilisés dans les domaines stratégiques des politiques sociales et économiques ne sont pas à haut risque s'ils ne présentent pas de risque pour la santé, la sécurité ou les droits fondamentaux des personnes physiques.

Les SIA utilisés dans les domaines stratégiques des politiques sociales et économiques sont donc autorisés s'ils visent à accomplir une tâche procédurale ou préparatoire, à améliorer le résultat d'une activité humaine ou à aider à la prise de décision.

Des lignes directrices concernant ces listes seront publiées par la Commission au plus tard dix-huit mois après l'entrée en vigueur du texte, soit en février 2026 (article 6.5).

Ensuite, les institutions européennes ont ajusté l'élaboration du texte pour prendre en compte l'avènement de l'IA générative. Pour l'intégrer au règlement, les institutions ont choisi de la traiter par l'angle des modèles d'IA à usage général.

Ceux-ci disposent de capacités à forts impacts, c'est à dire que la quantité cumulée de calcul utilisé pour son entraînement, mesurée en opérations en virgule flottante, est supérieure à 10^{25} (article 51). Ou bien, le modèle d'IA à usage général a été identifié et désigné par une décision de la Commission, désigné d'office ou à la suite d'une alerte qualifiée du groupe scientifique (article 51). La surveillance et le contrôle de ces modèles revient à la Commission par le biais du Bureau de l'IA (article 88).

Pour les systèmes d'IA à haut risque ainsi que pour les modèles d'IA à usage général, un ensemble d'obligations strictes doivent être respectées pour être conforme au règlement. Afin de faire respecter ces obligations, un système de contrôle sophistiqué a été élaboré.

C - Un contrôle sophistiqué assuré par une gouvernance à plusieurs échelles

Pour s'assurer de la mise en œuvre et du contrôle de l'application de l'AI Act, plusieurs organes sont créés et/ou investis aux niveaux communautaire et national.

A l'échelle européenne, l'AI Act crée le Bureau de l'IA ainsi que le Comité de l'IA qui détiennent tous deux un rôle central. Le Bureau de l'IA est l'entité qui développe, pour la Commission, l'expertise et les capacités de l'Union en matière d'IA. Il est notamment chargé de la surveillance des modèles d'IA à usage général s'ils présentent un risque systémique. Les Etats membres sont tenus de soutenir le Bureau de l'IA dans l'accomplissement de ses tâches (article 64).

En parallèle du Bureau, le Comité de l'IA développe également une expertise en matière d'IA dans le but de conseiller et d'assister la Commission, mais a aussi vocation à conseiller et à assister les Etats membres dans l'application du texte. Pour ce faire, il facilite la coopération et la coordination via l'harmonisation des pratiques administratives et l'élaboration de critères communs entre les entités européennes et nationales concernées. Le Comité de l'IA est impliqué dans la création des bacs à sable réglementaires et fournit des avis et des alertes liés aux modèles d'IA (article 65). Il se compose des Etats membres, du Contrôleur européen pour la protection des données (CEPD) en tant qu'observateur et son secrétariat est assuré par le Bureau de l'IA.

Tout autorité, organe ou expert peut être invité aux réunions de ses sous-groupes. Il existe au moins deux sous-groupes : un premier en charge de la coopération et l'échange entre les autorités de surveillance du marché et un second chargé de la coopération administrative pour la surveillance du marché.

Le Bureau de l'IA et le Comité de l'IA sont soutenus par un Forum consultatif composé d'experts issus du monde industriel et universitaire (article 67) désignés par la Commission pour un mandat de deux ans. Ceux-ci produisent des avis, des recommandations et des contributions sur demande du Bureau et du Comité. L'Agence des droits fondamentaux, l'Agence de l'UE pour la cybersécurité (ENISA), le Comité européen de normalisation (CEN), le Comité européen de normalisation électrotechnique (CENELEC) et l'Institut européen de normalisation des télécommunications (ETSI) siègent de manière permanente au Forum. La présidence est assurée par deux co-présidents élus pour une durée de deux ans, renouvelable deux fois. Chaque année, le Forum publiera un rapport sur ses activités.

Le Bureau et le Comité de l'IA sont aussi soutenus par un groupe scientifique d'experts indépendants (article 68). Il est créé par acte d'exécution et ses membres sont sélectionnés par la Commission selon leur expertise. Ce groupe a pour rôle principal d'alerter le Bureau de l'IA en cas de risque systémique posé par un modèle d'IA à usage général (article 90).

Pour cela, il met au point des outils et des méthodologies pour évaluer les capacités de ces modèles. Les Etats membres peuvent aussi faire appel à ce groupe d'experts pour être conseillés pour l'application du règlement. Ce service peut être payant.

Au niveau national, le règlement impose aux Etats membres d'établir ou de désigner des autorités nationales compétentes et de déterminer les tâches qui leur incombent. Parmi elles, au moins une autorité notifiante (qui notifie, désigne les organismes de certification) et une autorité de surveillance du marché (article 70). Les points de contact unique de ces entités et la manière de les contacter devront être rendu publics au plus tard douze mois à compter de la date d'entrée en vigueur, soit le 2 août 2025.

Les autorités de surveillance de marché peuvent fournir des orientations et des conseils sur la mise en œuvre du règlement, en particulier pour les PME et les start up. Pour les produits couverts par la législation harmonisée sur la sécurité des produits et des équipements (annexe I section A), les autorités de surveillance du marché désignées par ces règlements sont compétentes pour l'AI Act.

C'est le cas également pour les établissements financiers : c'est l'autorité responsable de la surveillance financière de ces établissements qui est responsable. Pour les autres SIA, une autre autorité de surveillance de marché peut être désignée.

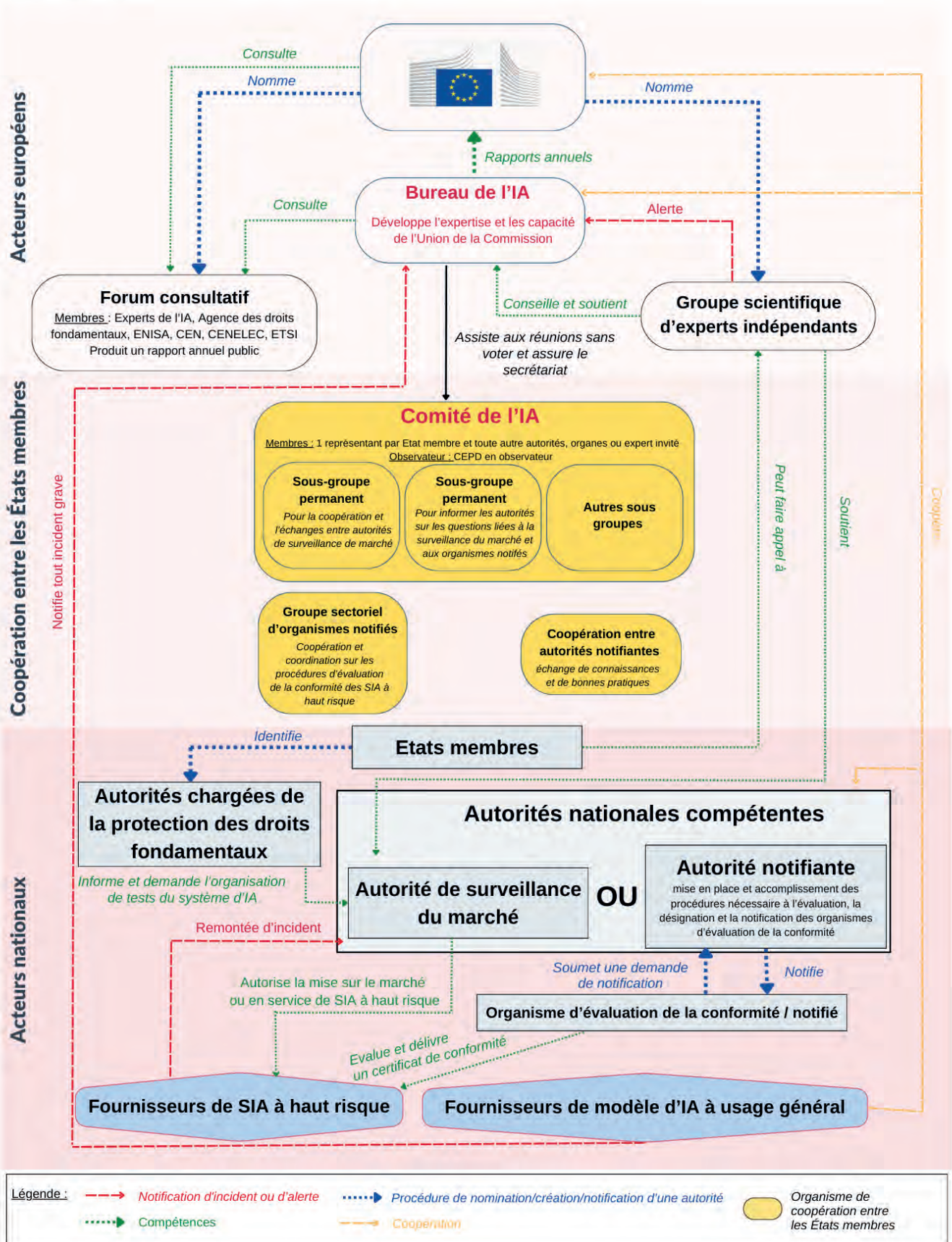
Enfin, pour les SIA à haut risque utilisés dans les domaines de la biométrie, de la répression, de la migration, de l'asile, de la gestion des contrôles aux frontières et de l'administration de la justice et des processus démocratiques, c'est l'autorité de contrôle de la protection des données désignée par le Règlement général sur la protection des données (RGPD) qui fait référence. En France, c'est donc la CNIL qui fait office d'autorité de surveillance du marché pour ces SIA. Pour les institutions européennes, c'est le Contrôle européen de la protection des données (CEPD) qui est compétente.

C'est l'autorité de surveillance de marché qui fait office de point de contact unique pour les institutions européennes. Par conséquent, elle dispose de vastes moyens pour s'assurer du respect du règlement. Elle peut, par exemple, demander à accéder au code source du SIA (article 74), demander au fournisseur qui aurait mal classé son SIA de prendre des mesures correctives (article 80) ou encore demander le retrait, le rappel, voire prescrire un SIA si elle a des raisons suffisantes de penser qu'il présente un risque. L'autorité de surveillance de marché joue également un rôle actif dans les essais en conditions réelles des SIA (article 76).

Enfin, l'autorité de surveillance de marché est soutenue par les autorités de protection des droits fondamentaux dans le contrôle des SIA à haut risque. Ces autorités ou ces organismes publics qui supervisent ou qui protègent les droits fondamentaux sont désignés par chaque Etat membre au plus tard le 2 novembre 2024 (article 77).

L'AI Act a donc introduit un cadre général pour les SIA et leurs utilisations au sein de l'Union européenne. Après avoir interdit certaines pratiques, l'AI Act souhaite avoir un contrôle sur tous les SIA qui pourraient présenter un risque pour les droits et libertés fondamentales européennes. Un cadre de gouvernance sophistiqué et à échelles multiples a donc été établi pour s'assurer que les obligations posées sont respectées. Ces obligations concernent principalement les SIA à haut risque et les modèles d'IA à usage général.

Gouvernance de l'IA prévue par l'AI Act



L'encadrement rigoureux des SIA à haut risque et des modèles d'IA à usage général

Une série d'obligations est posée par l'AI Act. Ces obligations s'adressent essentiellement aux fournisseurs de SIA à haut risque et de modèles d'IA à usage général et concernent leur développement ainsi que leur mise en conformité avec le règlement.

A - De strictes exigences pour les SIA à haut risque et leur fournisseur

Les fournisseurs doivent répondre à un ensemble d'exigences s'ils souhaitent pouvoir commercialiser leurs SIA en UE. La première d'entre elles est de signaler son SIA comme étant à haut risque (article 16) de manière visible (sur l'emballage, dans la documentation technique, ...). Le fournisseur s'assure ensuite que son SIA à haut risque répond, entre autres, à deux types d'exigences : la gestion des risques et l'information.

1. La gestion des risques

Pour s'assurer de surveiller, de contrôler et d'atténuer les risques, le fournisseur doit d'abord s'assurer que son SIA a été correctement entraîné, validé et testé sur des jeux de données protégés, pertinents, représentatifs et, dans la mesure du possible, exempts d'erreurs et complets (article 10). Dans la mesure où cela est strictement nécessaire aux fins de la détection et de la correction des biais, des données à caractères personnelles au sens du RGPD peuvent être exceptionnellement collectées.

Pour être entraîné, le SIA à haut risque peut effectuer des essais en conditions réelles (article 60) après approbation de l'autorité de surveillance de marché, obtention du consentement des participants concernés et pendant une durée maximale de six mois (renouvelable une fois).

Des précisions sur l'essai en conditions réelles seront apportées par la Commission par acte d'exécution. Les SIA à haut risque peuvent également accéder aux bacs à sable réglementaires de l'IA pour être testés.

Le SIA doit être développé pour avoir un niveau approprié de précision, être robuste, résilient et résistant à des cyberattaques (article 15). Cela inclut aussi que les biais dû à l'apprentissage continu (les boucles de rétroactions) soient traités tout au long du cycle de vie du SIA. Les SIA à haut risque qui ont été certifiés, ou pour lesquels une déclaration de conformité a été délivrée dans le cadre d'un schéma de cybersécurité conformément au *European Cybersecurity Act* sont présumées conformes à cette exigence (article 42).

Ensuite, le fournisseur doit tenir à jour un système de gestion des risques avant que le SIA soit mis sur le marché et tout au long de son cycle de vie (article 9) et même après sa commercialisation (article 72). Cela signifie que le SIA a été testé avant d'être mis sur le marché pour s'assurer qu'il fonctionne conformément à sa destination et dans les cas de mauvaise utilisation raisonnablement prévisible. Les événements du SIA doivent également être enregistrés tout au long de son cycle de vie afin que les situations qui pourraient présenter un risque ou modifier substantiellement le SIA soient journalisées. Cela permet de faciliter la surveillance et le fonctionnement du SIA. Pour les SIA d'identification biométrique, des exigences supplémentaires sont demandées : la période de chaque utilisation (date et heure du début de chaque utilisation) doit être enregistrée tout comme la base de données de référence utilisée pour vérifier les données d'entrées pour lesquelles la recherche a abouti à une correspondance et les personnes physiques ayant participé à la vérification des résultats (article 12).

En cas d'incident grave, les fournisseurs de SIA à haut risque doivent notifier les autorités de surveillance du marché au plus tard quinze jours après que le lien de causalité ou que la probabilité raisonnable de l'existence d'un tel lien ait été établi. Si l'incident est une infraction de grande ampleur, la notification doit se faire dans les deux jours suivants l'incident. Ce délai passe à dix jours en cas de décès d'une personne. L'autorité de surveillance dispose, quant à elle, de sept jours pour réagir. La Commission élaborera, au plus tard, le 2 août 2025, des orientations spécifiques sur la remontée d'incident.

L'exigence principale demandée par le règlement aux fournisseurs est qu'un contrôle humain soit toujours établi, c'est-à-dire qu'au moins une personne physique contrôle le SIA à haut risque et les conséquences de ses propositions. Les personnes en charge du contrôle doivent pouvoir aller jusqu'à interrompre le système de manière sécurisée. Pour les SIA d'identification biométrique à distance, le contrôle doit être effectué par au moins deux personnes.

2. Une exigence de transparence et d'information

Le règlement demande aux fournisseurs de répondre à une exigence de transparence et d'information. Cela signifie que les résultats du SIA doivent être transparents et interprétables. Pour cela le déployeur (compris comme l'utilisateur) doit pouvoir comprendre le SIA qu'il utilise. Le fournisseur doit donc accompagner son SIA d'une notice d'utilisation (capacités, limites, durée de vie, mesures de contrôle humain, ...) (article 13).

Ensuite, une documentation technique du SIA doit être établie avant sa mise sur le marché et doit être tenue à jour (article 11). Les éléments de la documentation technique sont listés par le règlement (annexe IV) et s'ajoutent aux exigences de la réglementation sur la sécurité des produits et des équipements si le SIA entre dans son champ.

La Commission fournira, par acte d'exécution, un modèle de plan de documentation technique (article 61). Les PME peuvent fournir une documentation technique simplifiée (annexe IV).

Les SIA à haut risque doivent également avoir été enregistrés dans la base de données de l'UE dédiée (article 71). Cette base de données est créée et tenue à jour par les Etats membres et la Commission dans le but de répertorier les SIA à haut risque sur le sol européen. Les éléments de cette base de données ne sont accessibles, en principe, qu'aux autorités de surveillance du marché et la Commission sauf si le fournisseur a donné son consentement pour que ces informations soient rendues publiques.

3. Autres obligations

Les fournisseurs de SIA à haut risque doivent également mettre en place un système de gestion de la qualité (article 17) à travers des politiques, des procédures et des instructions qui déterminent la stratégie de mise en conformité et son entretien. Les fournisseurs assurent également la conservation de la documentation pendant dix ans (article 18), la tenue des journaux (article 19), la soumission à la procédure d'évaluation de conformité (article 43), la déclaration UE de conformité (article 47), l'apposition du marquage CE (article 48), l'enregistrement (article 49), la fourniture de la preuve de la conformité à la demande d'une autorité nationale compétente et la mise en place de mesures correctives (article 20).

En effet, en cas de non-conformité présumée, le SIA devra être retiré, désactivé ou rappelé et les causes devront être identifiées.

Concernant l'utilisation de SIA pour l'identification biométrique à distance, une autorisation doit être demandée au préalable ou au plus tard quarante-huit heures suivant son utilisation lorsque ce SIA a pour objectif la recherche ciblée d'une personne soupçonnée d'avoir commis une infraction pénale ou condamnée pour avoir commis une infraction pénale (article 26).

B - La démonstration de la conformité du SIA à haut risque

Une fois ces exigences mises en œuvre, le fournisseur doit pouvoir démontrer que son système d'IA à haut risque est conforme au règlement. Pour cela, plusieurs possibilités s'offrent à lui.

S'il existe des normes harmonisées ou que des normes couvrent une partie des exigences du règlement et que le SIA à haut risque y est conforme, alors le système est présumé conforme aux exigences de ce règlement (article 40).

Si de telles normes n'existent pas ou que la Commission estime qu'elles sont insuffisantes, elle peut, par acte d'exécution, adopter des spécifications communes (article 41). Dès lors, les SIA à haut risque qui seraient conformes à ces spécifications communes sont considérés conformes aux exigences de l'AI Act. La Commission a déjà déposé une demande de normalisation au CEN CENELEC (en charge de la normalisation européenne), le 22 mai 2023, pour que des normes harmonisées soient élaborées.

Ensuite, s'il n'existe ni normes harmonisées ni spécifications communes ou qu'elles ne sont pas appliquées, alors les fournisseurs doivent suivre la procédure d'évaluation de conformité prévue par le règlement (l'article 43). Pour les SIA utilisés dans les domaines stratégiques des politiques sociales et économiques, l'évaluation se fait par un contrôle interne et ne nécessite pas l'intervention d'un organisme notifié. Les SIA à haut risque utilisés dans le domaine de la biométrie doivent cependant procéder à une évaluation du système de gestion de la qualité et de la documentation technique par un organisme notifié (annexe VII).

Enfin, pour les SIA à haut risque couverts par les actes portant sur la sécurité des produits et des équipements, le fournisseur suit la procédure d'évaluation de la conformité requise par ces actes juridiques qui doit être effectuée par un organisme notifié. Les organismes notifiés en vertu des actes portant sur la sécurité des produits et des équipements sont habilités à contrôler la conformité des SIA à haut risque.

Des certificats de conformité sont ensuite délivrés par les organismes notifiés. Ils sont valables pour une durée maximale de cinq ans pour les SIA couverts par les actes portant sur la sécurité des produits et des équipements, et quatre ans pour le SIA à haut risque relevant des domaines stratégiques des politiques sociales et économiques. Les certificats sont cependant renouvelables pour la même durée.

Il est possible de déroger à la procédure d'évaluation de conformité sur demande dûment justifiée pour des « raisons exceptionnelles de sécurité publique ou pour assurer la protection de la vie privée et de la santé humaine, la protection de l'environnement et la protection d'actifs industriels et d'infrastructures d'importance majeure » pour une durée déterminée (article 46).

En cas de modifications substantielles, les SIA à haut risque doivent être soumis à une nouvelle procédure d'évaluation de la conformité, les modifications apportées au système d'IA à haut risque et à ses performances par l'apprentissage ne constituant pas une modification substantielle.

La Commission peut également décider, par acte délégué, de rendre obligatoire la procédure d'évaluation de conformité la plus exigeante à l'ensemble des SIA à haut risque.

Une fois l'évaluation de conformité effectuée, le fournisseur établit une déclaration de conformité qui doit être disponible pendant dix ans. Une seule déclaration de conformité est nécessaire si le SIA à haut risque est soumis à d'autres actes législatifs d'harmonisation. Enfin, la dernière étape de la démonstration de la mise en conformité est l'apposition du marquage CE de façon visible, lisible et indélébile sur les systèmes d'IA à haut risque, son emballage ou les documents qui l'accompagnent (article 48). Le système d'IA à haut risque peut désormais être enregistré (article 49) dans la base de données de l'UE (article 71) puis mis sur le marché de l'Union européenne.

La non-conformité d'un SIA à haut risque à ces dispositions entraîne une amende administrative pouvant aller jusqu'à quinze

millions d'euros, ou 3% du chiffre d'affaires annuel mondial du fournisseur.

Aussi, la fourniture d'informations inexactes, incomplètes ou trompeuses aux organismes notifiés ou aux autorités nationales lorsqu'elles en font la demande entraîne une amende administrative pouvant aller jusqu'à sept millions et demi d'euros ou 1% du chiffre d'affaires annuel mondial. Pour les PME et les start up, la plus petite somme des deux est retenue. Le régime des sanctions est précisé par les Etats membres.

Pour les institutions, organes et organismes de l'UE, le non-respect de ces exigences entraîne une amende administrative pouvant aller jusqu'à sept-cent cinquante mille euros. Lorsque des systèmes d'IA à haut risque sont 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 au plus tard six ans après l'entrée en vigueur de l'AI Act.

C - Le traitement particulier des modèles d'IA à usage général

Afin de réguler l'IA générative, l'AI Act vient encadrer les modèles d'IA à usage général. Les exigences imposées aux fournisseurs de modèle d'IA à usage général sont moindres que celles demandées aux fournisseurs de SIA à haut risque.

Comme pour les SIA à haut risque, les fournisseurs de modèles d'IA à usage général doivent tenir une documentation technique à jour du modèle (article 53) qui doit contenir les mesures d'entraînement et d'essai ainsi que les résultats de son évaluation.

Cette documentation technique doit être mise à disposition des fournisseurs qui souhaitent intégrer le modèle d'IA à usage général à leur système. Les fournisseurs de modèles d'IA doivent également mettre en place une politique de mise en conformité à la législation de l'Union en matière de droit d'auteur.

Enfin, les fournisseurs doivent mettre à la disposition du public un résumé du contenu utilisé pour entraîner le modèle d'IA (article 53) ainsi qu'un résumé suffisamment détaillé du contenu utilisé pour entraîner le modèle.

Tout incident devra être communiqué au Bureau de l'IA et aux autorités nationales compétentes. Ces obligations ne s'appliquent pas aux modèles d'IA qui sont publiés dans le cadre d'une licence libre et ouverte.

Pour se conformer aux exigences du règlement, le fournisseur de modèle d'IA à usage général peut appliquer une norme européenne harmonisée élaborée par la Commission. Cependant, si le modèle présente un risque systémique, le fournisseur devra l'évaluer sur la base de protocoles et d'outils normalisés et réaliser des essais contradictoires pour identifier et atténuer le risque systémique.

La conformité d'un modèle d'IA à usage général est également permise par l'application d'un code de bonnes pratiques, produit et harmonisé par le Bureau de l'IA, en attendant l'élaboration de normes harmonisées. Les fournisseurs sont libres de respecter le code complet. Ces codes concernent :

- Les moyens d'assurer que les informations demandées aux fournisseurs de modèle d'IA à usage général comportant un risque systémique sont mises à jour à la lumière des évolutions du marché et des technologies,
- Le niveau approprié de détail pour le résumé du contenu utilisé pour l'entraînement,
- L'identification du type et de la nature des risques systémiques au niveau de l'Union, y compris leurs origines,
- Les mesures, procédures et modalités d'évaluation et de gestion des risques systémiques au niveau de l'Union.

Les codes de bonnes pratiques devront être établis avant le 2 mai 2025. Si dix mois après l'entrée en vigueur du règlement, soit le 2 juin 2025, un code de bonnes pratiques n'est pas mis au point ou si le Bureau de l'IA estime qu'il n'est pas approprié, la Commission peut prévoir des règles communes pour le remplacer.

Enfin, les fournisseurs de modèles d'IA qui ne respectent pas les exigences du règlement s'exposent à une amende pouvant aller jusqu'à 3% du chiffre d'affaires annuel mondial ou quinze millions d'euros. La Commission considère qu'une exception doit être faite pour les fournisseurs de modèles d'IA à usage général qui ont été mis sur le marché avant le 2 août 2025. La Commission permet aux fournisseurs de ces modèles de prendre les mesures nécessaires pour se conformer aux obligations prévues par le règlement au plus tard le 2 août 2027.



Le soutien à l'innovation pour l'ensemble des SIA

En parallèle des obligations imposées aux fournisseurs de SIA à haut risque et de modèles d'IA à usage général, l'AI Act vise à soutenir le développement de l'IA au sein de l'UE. L'AI Act vient donc créer des bacs à sable réglementaire pour tous les SIA. De plus, le règlement n'impose aux autres fournisseurs de SIA qu'une obligation de transparence et encourage l'adoption volontaire de mesures plus exigeantes.

A - La création de bacs à sable réglementaire pour tester les SIA

Avec l'AI Act, l'UE peut désormais soutenir l'innovation en matière d'IA à travers des bacs à sable réglementaires de l'IA (article 57). Ainsi, dès deux ans après l'entrée en vigueur du règlement, soit le 1er août 2026, au moins un bac à sable réglementaire par Etat membre devra être opérationnel. Ces bacs à sable peuvent être établis conjointement avec d'autres Etats membres. La création de bacs à sable régionaux et locaux est également possible. Au niveau européen, c'est le Contrôleur européen de la protection des données (CEPD) qui peut créer un bac à sable réglementaire pour les institutions, organes et organismes de l'Union, en tant qu'autorité compétente.

Les bacs à sable réglementaires de l'IA sont créés dans le but de permettre un environnement contrôlé pour favoriser l'innovation et faciliter le développement, l'entraînement, la mise à l'essai et la validation de systèmes d'IA innovants pendant une durée limitée avant leur mise sur le marché.

Ces bacs à sable peuvent comprendre des essais en conditions réelles supervisés. Les bacs à sable réglementaires existent également pour renforcer la sécurité juridique, faciliter le partage de bonnes pratiques entre les autorités compétentes et les fournisseurs, faciliter leur accès au marché de l'UE et créer un écosystème européen performant de l'IA (article 62).

Le fonctionnement des bacs à sable n'a pas été précisément défini par le règlement. Mais, il est déjà prévu que l'accès aux bacs à sable réglementaires soit gratuit pour les PME. Tous les SIA peuvent y avoir accès, y compris les SIA à haut risque et les modèles d'IA à usage général. La Commission adoptera des actes d'exécution pour préciser leurs modalités de fonctionnement et notamment les critères d'éligibilité et de sélection, les procédures de demande, de surveillance, de sortie et d'expiration ainsi que les conditions applicables aux participants.

Aussi, le traitement de données à caractère personnel dans les tests peut être autorisé mais leur utilisation est strictement conditionnée (article 59) à leur protection et au développement de SIA visant à préserver l'intérêt public.

Le processus ou la participation peuvent être suspendus lorsqu'un risque « significatif pour la santé, la sécurité et les droits fondamentaux » apparaît et qu'aucune atténuation efficace n'est possible. Aucune amende administrative ne peut être infligée au fournisseur dans le cadre de ces bacs à sable réglementaires si

le plan spécifique, les modalités de participation et les orientations de l'autorité nationale compétente (qui font partie des conditions d'entrée) sont suivis de bonne foi.

A l'issue de la participation au bac à sable, un rapport de sortie est établi qui peut servir à démontrer la conformité au règlement. Ce rapport n'a pas vocation à être rendu public, sauf si le fournisseur et l'autorité compétente y consentent. Enfin, les autorités nationales compétentes devront présenter tous les ans au Bureau de l'IA et au Comité de l'IA un rapport annuel sur la tenue du bac à sable réglementaire.

B - Une obligation de transparence pour tous les SIA

La transparence est la seule obligation imposée à l'ensemble des SIA. Ainsi, les fournisseurs de SIA destinés à interagir avec des personnes physiques doivent être conçus et développés de manière à ce que les personnes physiques soient informées qu'elles interagissent avec un SIA, notamment lorsque les personnes sont exposées à un SIA de reconnaissance d'émotions ou de catégorisation biométrique. Seuls les SIA utilisés à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ne sont pas concernés par cette obligation, sauf s'ils sont mis à la disposition du public pour permettre le signalement d'une infraction pénale.

De la même manière, les fournisseurs de SIA et de modèles d'IA à usage général qui génèrent des contenus de synthèse de type

texte, audio, vidéo, y compris l'hypertrucage (article 50.4) veillent à ce que les résultats produits par les systèmes d'IA soient marqués comme ayant été générés ou manipulés par une IA (article 50.2). Cette obligation s'applique également aux SIA qui génèrent ou manipulent des images ou des contenus audio ou vidéo présentant une ressemblance avec des personnes, des objets, des lieux ou d'autres entités ou événements existants et pouvant être perçus à tort comme authentiques ou véridiques (article 50.3).

Mise à part cette exigence de transparence, l'UE n'impose aucune obligation supplémentaire aux autres SIA mais encourage l'adoption volontaire de mesures plus exigeantes.

C - Un encouragement à l'adoption volontaire de mesures plus exigeantes

Enfin, le Bureau de l'IA et les Etats membres encouragent l'élaboration et l'adoption de codes de conduite destinés à favoriser l'application volontaire de tout ou partie des exigences relatives aux SIA à haut risque (article 95). Les fournisseurs sont libres d'adopter tout ou partie de ces exigences. Ces codes de conduite doivent comprendre des indicateurs de performance clés et des objectifs allant de l'éthique, à la durabilité environnementale, à l'inclusivité et l'égalité de genre, à la maîtrise de l'IA et la prévention de l'impact négatif du SIA sur des personnes vulnérables.

Ces codes peuvent être élaborés par des fournisseurs, des déployeurs ou par des organisations les représentant.

Ces codes sont volontairement généraux et ne contiennent pas de recommandations techniques. Les fournisseurs sont donc libres de respecter les objectifs qu'ils se seraient eux-mêmes fixés par les moyens qu'ils souhaitent.

C ONCLUSION

En conclusion, la volonté de la Commission européenne, par cet ambitieux projet, n'est pas seulement d'encadrer réglementairement les SIA au sein de l'UE. Elle souhaite avant tout permettre à l'UE de voir se développer sur son territoire des idées innovantes en matière d'IA qui respectent les valeurs fondamentales européennes et dignes de confiance grâce à l'investissement de bacs à sable réglementaires.

L'AI Act s'appliquera progressivement. Les dispositions générales relatives aux définitions de l'IA et les pratiques interdites s'appliqueront dès le 2 février 2025. Ensuite, les dispositions relatives aux autorités notifiantes et aux organismes notifiés, aux modèles d'IA à usage général, à la gouvernance et aux sanctions seront mises en œuvre dans l'année qui suit son entrée en vigueur et devra être effective au plus tard le 2 août 2025. Le reste de ses dispositions s'appliqueront dès le 2 août 2026, à quelques exceptions près (article 111) :

- Les SIA qui sont des composants de systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice et mis sur le marché avant le 2 août 2027 ont jusqu'au 31 décembre 2030 pour se conformer l'AI Act,

- Les fournisseurs de SIA à haut risque destinés à être utilisés par des autorités publiques doivent être conformes au règlement au plus tard le 2 août 2030,
- Les fournisseurs de modèles d'IA à usage général mis sur le marché avant le 2 août 2025 doivent être conformes à l'AI Act au plus tard le 2 août 2027,
- Les dispositions relatives à la définition des SIA à haut risque ne s'appliqueront qu'à partir du 2 août 2026.

Toutes ces mesures permettent de renforcer le cadre de la confiance numérique en construction en Europe. L'AI Act, en plus de son caractère inédit, vient compléter un édifice de sécurisation varié de l'espace numérique européen (Cybersecurity Act, NIS 2, DORA, Cyber Resilience Act, Cyber Solidarity Act, ...). Les réflexions autour de l'intelligence artificielle sont désormais lancées et permettront, par un investissement adapté, de faire de l'UE un acteur majeur en la matière. La stratégie de l'Union européenne pour l'IA consiste à investir près d'un milliard d'euros par an dans l'IA via les programmes Europe numérique et Horizon Europe.

Plus largement, l'objectif de l'Union européenne en matière d'IA est d'attirer plus de vingt milliards d'euros d'investissements annuels pendant les dix prochaines années pour stimuler l'excellence dans le domaine de l'IA. La maîtrise de cette technologie, et plus largement de la révolution en cours, est essentielle.

L'IA doit être maîtrisée et optimisée pour permettre à l'UE de bénéficier de son plein potentiel tout en se prémunissant des dangers et risques qu'elle porte. La maîtrise de l'IA est la clé de la maîtrise de l'avenir numérique de l'UE et de la protection des droits fondamentaux européens face à une concurrence internationale accrue.

Annexe I - Abréviations

IA	Intelligence artificielle
SIA	Système d'IA
UE	Union européenne
ENISA	Agence de l'UE pour la cybersécurité
CEN	Comité européen de normalisation
CENELEC	Comité européen de normalisation électrotechnique
ETSI	Institut européen de normalisation des télécommunications
RGPD	Règlement général sur la protection des données
CNIL	Commission nationale de l'informatique et des libertés

Annexe II - Glossaire

Définitions

Système d'IA :

un système automatisé conçu pour fonctionner à différents niveaux d'autonomie, qui peut faire preuve d'une capacité d'adaptation après son déploiement et qui, pour des objectifs explicites ou implicites, déduit, à partir des données d'entrée qu'il reçoit, la manière de générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels.

Risque :

la combinaison de la probabilité d'un préjudice et de la sévérité de celui-ci.

Fournisseur :

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

Déploieur :

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

Mandataire :

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

Importateur :

une personne physique ou morale située ou établie dans l'Union qui met sur le marché un système d'IA qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers.

Distributeur :

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

Opérateur :

un fournisseur, fabricant de produits, déployeur, mandataire, importateur ou distributeur.

Mise sur le marché :

la première mise à disposition d'un système d'IA ou d'un modèle d'IA à usage général sur le marché de l'Union.

Mise à disposition sur le marché :

la fourniture d'un système d'IA ou d'un modèle d'IA à usage général destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit.

Mise en service :

la fourniture d'un système d'IA par le fournisseur directement à au déployeur en vue d'une première utilisation ou pour usage propre dans l'Union, conformément à la destination du système.

Destination :

l'utilisation à laquelle un système d'IA est destiné par le fournisseur, y compris le contexte et les conditions spécifiques d'utilisation, telles que précisées dans les informations communiquées par le fournisseur dans la notice d'utilisation, les indications publicitaires ou de vente et les déclarations, ainsi que dans la documentation technique.

Mauvaise utilisation raisonnablement prévisible :

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

Composant de sécurité :

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

Notice d'utilisation :

les indications communiquées par le fournisseur pour informer le déployeur, en particulier, de la destination et de l'utilisation correcte d'un système d'IA.

Rappel d'un système d'IA :

toute mesure visant à assurer le retour au fournisseur d'un système d'IA mis à la disposition des déployeurs ou à le mettre hors service ou à désactiver son utilisation.

Retrait d'un système d'IA :

toute mesure visant à empêcher qu'un système d'IA se trouvant dans la chaîne d'approvisionnement ne soit mis à disposition sur le marché.

Performance d'un système d'IA :

la capacité d'un système d'IA à remplir sa destination.

Autorité notifiante :

l'autorité nationale chargée de mettre en place et d'accomplir les procédures nécessaires à l'évaluation, à la désignation et à la notification des organismes d'évaluation de la conformité et à leur contrôle.

Evaluation de la conformité :

la procédure permettant de démontrer que les exigences relatives à un système d'IA à haut risque énoncées au chapitre II, section 2, ont été respectées.

Organisme d'évaluation de la conformité :

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

Organisme notifié :

un organisme d'évaluation de la conformité notifié en application du présent règlement et d'autres actes législatifs d'harmonisation de l'Union pertinents, énumérés à l'annexe I, section B.

Modification substantielle :

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

Marquage CE :

un marquage par lequel le fournisseur indique qu'un système d'IA est conforme aux exigences du chapitre II, section 2, et d'autres actes législatifs d'harmonisation de l'Union applicables énumérés à l'annexe I qui en prévoient l'application.

Système de surveillance après commercialisation :

l'ensemble des activités réalisées par les fournisseurs de systèmes d'IA pour recueillir et analyser les données issues de l'expérience d'utilisation des systèmes d'IA qu'ils mettent sur le marché ou mettent en service de manière à repérer toute nécessité d'appliquer immédiatement une mesure préventive ou corrective.

Autorité de surveillance du marché :

l'autorité nationale assurant la mission et prenant les mesures prévues par le règlement (UE) 2019/1020.

Norme harmonisée :

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

Spécification commune :

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

Données d'entraînement :

les données utilisées pour entraîner un système d'IA en ajustant ses paramètres entraînaibles.

Données de validation :

les données utilisées pour fournir une évaluation du système d'IA entraîné et pour régler ses paramètres non entraînaibles ainsi que son processus d'apprentissage, afin, notamment, d'éviter tout sous-ajustement ou surajustement.

Jeu de données de validation :

un jeu de données distinct ou une partie du jeu de données d'entraînement, sous la forme d'une division variable ou fixe.

Données de test :

les données utilisées pour fournir une évaluation indépendante du système d'IA afin de confirmer la performance attendue de ce système avant sa mise sur le marché ou sa mise en service.

Données d'entrée :

les données fournies à un système d'IA ou directement acquises par celui-ci et à partir desquelles il produit un résultat.

Données biométriques :

les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, elles que des images faciales ou des données dactyloscopiques.

Identification biométrique :

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

Vérification biométrique :

la vérification "un à un" automatisée, y compris l'authentification, de l'identité des personnes physiques en comparant leurs données biométriques à des données biométriques précédemment fournies.

Catégories particulières de données à caractère personnel :

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

Données opérationnelles sensibles :

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

Système de reconnaissance des émotions :

un système d'IA permettant la reconnaissance ou la déduction des émotions ou des intentions de personnes physiques sur la base de leurs données biométriques.

Système de catégorisation biométrique :

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

Système d'identification biométrique à distance :

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

Système d'identification biométrique à distance en temps réel :

un système d'identification biométrique à distance dans lequel l'acquisition des données biométriques, la comparaison et l'identification se déroulent sans décalage temporel significatif et qui comprend non seulement l'identification instantanée, mais aussi avec un léger décalage afin d'éviter tout contournement des règles.

Système d'identification biométrique à distance a posteriori :

un système d'identification biométrique à distance autre qu'un système d'identification biométrique à distance en temps réel.

Espace accessible au public :

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

Autorités répressives :

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

Activités répressives :

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

Bureau de l'IA :

la fonction de la Commission consistant à contribuer à la mise en œuvre, au suivi et à la surveillance des systèmes d'IA et de la gouvernance de l'IA effectués par le Bureau européen de l'intelligence artificielle, établi par la décision de la Commission du 24 janvier 2024 ; les références faites au Bureau de l'IA dans le présent règlement s'entendent comme faites à la Commission.

Autorité nationale compétente :

une autorité notifiante ou une autorité de surveillance du Marché.

Incident grave :

un incident ou dysfonctionnement d'un système d'IA entraînant directement ou indirectement :

- le décès d'une personne ou une atteinte grave à la santé d'une personne;
- une perturbation grave et irréversible de la gestion ou du fonctionnement d'infrastructures critiques;
- la violation des obligations au titre du droit de l'Union visant à protéger les droits fondamentaux,
- un dommage grave à des biens ou à l'environnement;

Données à caractère personnel :

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

Données à caractère non personnel :

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

Profilage :

le profilage au sens de l'article 4, point 4, du règlement (UE) 2016/679 ou, dans le cas des autorités répressives, au sens de l'article 3, point 4, de la directive (UE) 2016/680 ou, dans le cas des institutions, organes ou organismes de l'Union, au sens de l'article 3, point 5, du règlement (UE) 2018/1725.

Plan d'essais en conditions réelles :

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

Plan du bac à sable :

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

Bac à sable réglementaire de l'IA :

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

Maîtrise de l'IA :

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

Essais en conditions réelles :

les essais temporaires d'un système d'IA aux fins de sa destination en conditions réelles en dehors d'un laboratoire ou d'un environnement simulé d'une autre manière, visant à recueillir des données fiables et solides et à évaluer et vérifier la conformité du système d'IA aux exigences du présent règlement; les essais en conditions réelles ne sont pas considérés comme constituant une mise sur le marché ni une mise en service du système d'IA au sens du présent règlement, pour autant que toutes les conditions prévues à l'article 57 ou à l'article 60 soient remplies.

Participant :

aux fins des essais en conditions réelles, une personne physique qui participe à des essais en conditions réelles.

Consentement éclairé :

l'expression libre, spécifique, univoque et volontaire, par un participant, de sa volonté de participer à un essai en conditions réelles particulier, après avoir pris connaissance de tous les éléments de l'essai qui lui permettent de prendre sa décision concernant sa participation.

Hypertrucage :

une image ou un contenu audio ou vidéo généré ou manipulé par l'IA, présentant une ressemblance avec des personnes, des objets, des lieux ou d'autres entités ou événements existants et pouvant être perçu à tort comme authentique ou véridique.

Capacités à fort impact :

des capacités égales ou supérieures aux capacités enregistrées dans les modèles d'IA à usage général les plus avancés.

Infraction de grande ampleur :

tout acte ou toute omission contraire au droit de l'Union en matière de protection des intérêts des personnes, qui :

- a porté ou est susceptible de porter atteinte aux intérêts collectifs des personnes résidant dans au moins deux États membres autres que celui:
 - o où l'acte ou l'omission en question a son origine ou a eu lieu;
 - o où le fournisseur concerné ou, le cas échéant, son mandataire, est situé ou établi; ou
 - o où le déployeur est établi, lorsque l'infraction est commise par le déployeur;
- a porté, porte ou est susceptible de porter atteinte aux intérêts collectifs des personnes, qui présente des caractéristiques communes, notamment la même pratique illégale ou la violation du même intérêt, et qui se produit simultanément, commise par le même opérateur, dans au moins trois États membres;

Infrastructure critique :

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

Modèle d'IA à usage général :

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

Risque systémique :

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

Système d'IA à usage général :

un système d'IA fondé sur un modèle d'IA à usage général qui a la capacité de répondre à diverses finalités, tant pour une utilisation directe que pour une intégration dans d'autres systèmes d'IA.

Opération en virgule flottante :

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

Fournisseur en aval :

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

Annexe III - Annexe II du règlement relative à la liste des infractions pénales qui justifient l'utilisation d'un système d'identification biométrique à distance en temps réel dans des espaces accessibles au public

Infractions pénales visées à l'article 5, paragraphe 1, point h) iii) :

- Terrorisme,
- Traite des êtres humains,
- Exploitation sexuelle des enfants et pédopornographie,
- Trafic de stupéfiants ou de substances psychotropes,
- Trafic d'armes, de munitions ou d'explosifs,
- Homicide volontaire, coups et blessures graves,
- Trafic d'organes ou de tissus humains,
- Trafic de matières nucléaires ou radioactives,
- Enlèvement, séquestration ou prise d'otage,
- Crimes relevant de la compétence de la Cour pénale internationale,
- Détournement d'avion ou de navire,
- Viol,
- Criminalité environnementale,
- Vol organisé ou à main armée,
- Sabotage,
- Participation à une organisation criminelle impliquée dans une ou plusieurs des infractions énumérées ci-dessus.

Annexe IV - Annexe III du règlement relative au classement de SIA à haut risque en fonction de leur domaine d'utilisation (article 6.2)

Les systèmes d'IA à haut risque au sens de l'article 6, paragraphe 2, sont les systèmes d'IA répertoriés dans l'un des domaines suivants :

1. Biométrie, dans la mesure où leur utilisation est autorisée par la législation nationale ou de l'Union applicable :

a) systèmes d'identification biométrique à distance.

Cela n'inclut pas les systèmes d'IA destinés à être utilisés à des fins de vérification biométrique dont la seule finalité est de confirmer qu'une personne physique spécifique est la personne qu'elle prétend être ;

b) systèmes d'IA destinés à être utilisés à des fins de catégorisation biométrique, en fonction d'attributs ou de caractéristiques sensibles ou protégés, sur la base de la déduction de ces attributs ou de ces caractéristiques ;

c) systèmes d'IA destinés à être utilisés pour la reconnaissance des émotions.

2. Infrastructures critiques :

a) systèmes d'IA destinés à être utilisés en tant que composants de sécurité dans la gestion et l'exploitation d'infrastructures numériques critiques, du trafic routier ou de la fourniture d'eau, de gaz, de chauffage ou d'électricité.

3. Éducation et formation professionnelle :

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

b) systèmes d'IA destinés à être utilisés pour évaluer les acquis d'apprentissage, y compris lorsque ceux-ci sont utilisés pour orienter le processus d'apprentissage de personnes physiques dans les établissements d'enseignement et de formation professionnelle, à tous les niveaux ;

c) systèmes d'IA destinés à être utilisés pour évaluer le niveau d'enseignement approprié qu'une personne recevra ou sera en mesure d'atteindre, dans le contexte ou au sein d'établissements d'enseignement et de formation professionnelle ;

- d) systèmes d'IA destinés à être utilisés pour surveiller et détecter des comportements interdits chez les étudiants lors d'essais dans le contexte d'établissements d'enseignement et de formation ou en leur sein ;

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

- a) systèmes d'IA destinés à être utilisés pour le recrutement ou la sélection de personnes physiques, en particulier pour publier des offres d'emploi ciblées, analyser et filtrer les candidatures et évaluer les candidats ;
- b) systèmes d'IA destinée à être utilisée pour prendre des décisions influant sur les conditions des relations professionnelles, la promotion ou le licenciement dans le cadre de relations professionnelles contractuelles, pour attribuer des tâches sur la base du comportement individuel, de traits de personnalités ou de caractéristiques personnelles ou pour suivre et évaluer les performances et le comportement de personnes dans le cadre de telles relations.

5. Accès et droit aux services privés essentiels et aux services publics et prestations sociales essentiels :

- a) systèmes d'IA destinés à être utilisés par les autorités publiques ou en leur nom pour évaluer l'éligibilité des personnes physiques aux prestations et services d'aide sociale essentiels, y compris les services de soins de santé, ainsi que pour octroyer, réduire, révoquer ou récupérer ces prestations et services ;
- b) systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit, à l'exception des systèmes d'IA utilisés à des fins de détection de fraudes financières ;
- c) systèmes d'IA destinés à être utilisés pour l'évaluation des risques et la tarification en ce qui concerne les personnes physiques en matière d'assurance-vie et d'assurance maladie ;
- d) systèmes d'IA destinés à évaluer et hiérarchiser les appels d'urgence émanant de personnes physiques ou à être utilisés pour envoyer ou établir des priorités dans l'envoi des services d'intervention d'urgence, y compris par la police, les pompiers et l'assistance médicale, ainsi que pour les systèmes de tri des patients admis dans les services de santé d'urgence.

6. Répression, dans la mesure où leur utilisation est autorisée par la législation nationale ou de l'Union applicable :

- a) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives ou en leur nom pour évaluer le risque qu'une personne physique devienne la victime d'infractions pénales ;

- b) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives, en tant que polygraphes ou outils similaires ;
- c) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer la fiabilité des preuves au cours d'enquêtes ou de poursuites pénales ;
- d) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour évaluer la probabilité qu'une personne physique commette une infraction ou récidive, sans se fonder uniquement sur le profilage des personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680, ou pour évaluer les traits de personnalité, les caractéristiques ou les antécédents judiciaires de personnes physiques ou de groupes ;
- e) systèmes d'IA destinés à être utilisés par les autorités répressives ou par les institutions, organes et organismes de l'Union, ou en leur nom, en soutien aux autorités répressives pour le profilage de personnes physiques visé à l'article 3, paragraphe 4, de la directive (UE) 2016/680 dans le cadre de la détection d'infractions pénales, d'enquêtes ou de poursuites en la matière ou d'exécution de sanctions pénales.

7. Migration, asile et gestion des contrôles aux frontières, dans la mesure où son utilisation est autorisée par la législation nationale ou de l'Union applicable :

- a) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes en tant que polygraphes et outils similaires ;
- b) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou les institutions, organes ou organismes de l'Union, ou en leur nom, pour évaluer un risque, y compris un risque pour la sécurité, un risque de migration irrégulière ou un risque pour la santé, posé par une personne physique qui a l'intention d'entrer ou qui est entrée sur le territoire d'un État membre ;
- c) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou les institutions, organes ou organismes de l'Union, ou en leur nom, pour aider les autorités publiques compétentes à procéder à l'examen des demandes d'asile, de visas et de titres de séjour et des plaintes connexes au regard de l'objectif visant à établir l'éligibilité des personnes physiques demandant un statut, y compris les évaluations connexes de la fiabilité des éléments de preuve ;
- d) systèmes d'IA destinés à être utilisés par les autorités publiques compétentes ou les institutions, organes ou organismes de l'Union, ou en leur nom, dans le cadre de la migration, de l'asile et de la gestion des contrôles aux frontières, aux fins de la détection, de la reconnaissance ou de l'identification des personnes physiques, à l'exception de la vérification des documents de voyage.

8. Administration de la justice et processus démocratiques :

- a) systèmes d'IA destinés à être utilisés par les autorités judiciaires ou en leur nom, pour les aider à rechercher et à interpréter les faits ou la loi, et à appliquer la loi à un ensemble concret de faits, ou à être utilisés de manière similaire lors du règlement extrajudiciaire d'un litige ;
- b) systèmes d'IA destinés à être utilisés pour influencer le résultat d'une élection ou d'un référendum ou le comportement électoral de personnes physiques dans l'exercice de leur vote lors d'élections ou de référendums. Sont exclus les systèmes d'IA auxquels les personnes physiques ne sont pas directement exposées, tels que les outils utilisés pour organiser, optimiser ou structurer les campagnes politiques sous l'angle administratif ou logistique.

Annexe IV - Annexe X du règlement relative aux actes législatifs de l'Union relatifs aux systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice

1. Système d'information Schengen

- a) Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018, p. 1).
- b) Règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018, p. 14)
- c) Règlement (UE) 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018, p. 56).

2. Système d'information sur les visas

- a) Règlement (UE) 2021/1133 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (UE) n° 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 et (UE) 2019/818 en ce qui concerne l'établissement des conditions d'accès aux autres systèmes d'information de l'UE aux fins du système d'information sur les visas (JO L 248 du 13.7.2021, p. 1)
- b) Règlement (UE) 2021/1134 du Parlement européen et du Conseil du 7 juillet 2021 modifiant les règlements (CE) n° 767/2008, (CE) n° 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 et (UE) 2019/1896 du Parlement européen et du Conseil et abrogeant les décisions 2004/512/CE et 2008/633/JAI du Conseil, aux fins de réformer le système d'information sur les visas (JO L 248 du 13.7.2021, p. 11).

3. Eurodac

- a) Règlement (UE) 2024/... du Parlement européen et du Conseil relatif à la création d'"Eurodac" pour la comparaison des données biométriques aux fins de l'application efficace du règlement (UE) .../... [règlement relatif à la gestion de l'asile et de la migration], du règlement (UE) .../... [règlement relatif à la réinstallation] et de la directive 2001/55/CE [directive relative à la protection temporaire], pour l'identification des ressortissants de pays tiers ou apatrides en séjour irrégulier, et relatif aux demandes de comparaison avec les données d'Eurodac présentées par les autorités répressives des États membres et par Europol à des fins répressives, et modifiant les règlements (UE) 2018/1240 et (UE) 2019/818

4. Système d'entrée/de sortie

- a) Règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 (JO L 327 du 9.12.2017, p. 20).

5. Système européen d'information et d'autorisation concernant les voyages

- a) Règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) n° 1077/2011, (UE) n° 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 (JO L 236 du 19.9.2018, p. 1).
- b) Règlement (UE) 2018/1241 du Parlement européen et du Conseil du 12 septembre 2018 modifiant le règlement (UE) 2016/794 aux fins de la création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) (JO L 236 du 19.9.2018, p. 72).

6. Système européen d'information sur les casiers judiciaires concernant des ressortissants de pays tiers et des apatrides

- a) Règlement (UE) 2019/816 du Parlement européen et du Conseil du 17 avril 2019 portant création d'un système centralisé permettant d'identifier les États membres détenant des informations relatives aux condamnations concernant des ressortissants de pays tiers et des apatrides (ECRIS-TCN), qui vise à compléter le système européen d'information sur les casiers judiciaires, et modifiant le règlement (UE) 2018/1726 (JO L 135 du 22.5.2019, p. 1).

7. Interopérabilité

- a) Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas (JO L 135 du 22.5.2019, p. 27).
- b) Règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration (JO L 135 du 22.5.2019, p. 85).

Annexe VI : Annexe XIII du règlement relative aux critères de désignation des modèles d'IA à usage général présentant un risque systémique (article 51)

Aux fins de déterminer si un modèle d'IA à usage général a des capacités ou un impact équivalents à ceux énoncés à l'article 51, paragraphe 1, points a) et b), la Commission tient compte des critères suivants :

- a) le nombre de paramètres du modèle ;
- b) la qualité ou la taille du jeu de données, par exemple mesurée en pré-tokens ;
- c) la quantité de calcul utilisée pour l'entraînement du modèle, mesurée en nombre d'opérations en virgule flottante ou indiquée par une combinaison d'autres variables telles que le coût estimé de l'entraînement, le temps estimé nécessaire à l'entraînement ou la consommation d'énergie estimée pour l'entraînement ;
- d) les modalités d'entrée et de sortie du modèle, telles que la conversion de texte en texte (grands modèles de langage), la conversion de texte en image, la multimodalité et les seuils de l'état de l'art pour déterminer les capacités à fort impact pour chaque modalité, ainsi que le type spécifique d'entrées et de sorties (p. ex.: séquences biologiques) ;
- e) les critères de référence et les évaluations des capacités du modèle, y compris en tenant compte du nombre de tâches ne nécessitant pas d'entraînement supplémentaire, sa capacité d'adaptation à apprendre de nouvelles tâches distinctes, son degré d'autonomie et d'extensibilité, ainsi que les outils auxquels il a accès ;
- f) si le modèle a un impact important sur le marché intérieur en raison de sa portée, qui est présumée lorsqu'il a été mis à la disposition d'au moins 10 000 utilisateurs professionnels enregistrés établis dans l'Union ;
- g) le nombre d'utilisateurs finaux inscrits.

A Propos de L'ACN

L'Alliance pour la Confiance Numérique (ACN) est le syndicat professionnel qui représente les entreprises (leaders mondiaux, PME/TPE, et ETI) du secteur de la confiance numérique et notamment celles de l'identité numérique, de la cybersécurité et de l'IA de confiance. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur. On dénombre 2 178 entreprises réalisant en France 19 Milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (8% de croissance annuelle moyenne depuis 2016). Les 120 membres de l'Alliance pour la Confiance Numérique (ACN), dont 87% de PME/ TPE- ETI, représentent 2/3 du chiffre d'affaires des entreprises françaises de la Confiance Numérique dans le monde (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, laboratoires d'évaluation de sécurité, recherche).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), est membre associé du Campus cyber et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité. Par ailleurs, l'ACN est également membre fondateur de l'association représentant l'écosystème européen de la cybersécurité : ECSO (European CyberSecurity Organisation).

Dernières publications



ACN

Alliance pour la confiance numérique 

SITE :

<https://www.confiance-numerique.fr/>



@ACN_SecNum



ACN - Alliance pour la Confiance Numérique