

Intelligence artificielle

FOCUS
sur

Le projet de règlement européen

En avril 2021, la Commission européenne publiait son projet de règlement destiné à encadrer juridiquement les systèmes d'intelligence artificielle (IA). Le texte prévoit d'être complété par des exigences fixées dans les législations sectorielles où ces systèmes d'IA sont destinés à être utilisés.

Le projet de règlement pose donc les principes généraux qui devront encadrer ce domaine technologique afin de « *répondre à la nécessité de garantir aux utilisateurs et citoyens de l'Union un niveau élevé de protection de la santé, de la sécurité et des droits fondamentaux, tout en fournissant un cadre juridique stable aux fournisseurs d'IA* ». Ainsi, la libre circulation transfrontière des biens et services fondés sur l'IA pourra être garantie, tout en réduisant le risque de voir les États membres imposer des restrictions concernant le développement, la commercialisation ou l'utilisation de systèmes d'IA.

L'objectif de la Commission européenne n'est donc pas de restreindre le développement de la filière, mais bien au contraire d'éviter que la disparité des règles nationales n'entraîne une fragmentation du marché de l'Union tout en instaurant une insécurité juridique pour les opérateurs économiques qui développent ou utilisent des systèmes d'IA. La Commission est bien consciente que le recours à l'intelligence artificielle peut donner des avantages concurrentiels décisifs à l'industrie européenne et produire des résultats bénéfiques dans de nombreux domaines, que ce soit l'environnement, la santé, l'agriculture, l'éducation et la formation, la gestion des infrastructures, l'énergie, etc.

Abréviations fréquemment utilisées

IA : Intelligence Artificielle

EESS : Exigence(s) Essentielle(s) de Santé et de Sécurité

NLF : New Legislative Framework - Nouveau cadre législatif

O.N. : Organisme(s) Notifié(s)

RIA : Règlement Intelligence Artificielle

UE : Union européenne

Sommaire

La définition d'IA	3
Les pratiques interdites en matière d'IA	4
Les systèmes d'IA à haut risque.....	5
Qu'est-ce qu'un système d'IA à haut risque ?	5
Quelles sont les exigences applicables aux systèmes IA à haut risque ?	6
Quelles sont les procédures d'évaluation de la conformité applicables aux systèmes IA à haut risque ?	9
Les systèmes d'IA hors champs des systèmes à haut risque	11
Quelles sont les procédures d'évaluation de la conformité applicables aux systèmes d'IA qui ne sont pas à haut risque ?	11
Quelles sont les obligations des différents acteurs économiques ?	12
Le fournisseur de système d'IA à haut risque	12
Le fournisseur de système d'IA autres	12
Le fabricant de produits intégrant un système d'IA à haut risque	12
Le distributeur et l'importateur du système d'IA à haut risque	13
Le le distributeur et l'importateur de système d'IA autres	13
L'utilisateur de systèmes d'IA à haut risque	14
L'utilisateur de systèmes d'IA autres	14
Les autorités notifiantes et organismes notifiés.....	14
Les États membres et les autorités de surveillance du marché	14
Conclusion.....	15

Introduction

Le projet de règlement destiné à encadrer juridiquement les systèmes d'intelligence artificielle (IA)¹ a été élaboré en s'appuyant sur de nombreuses études et rapports publiés ces dernières années par différents groupes de réflexions sous la direction de la Commission européenne (CE)².

Le règlement devant couvrir l'ensemble des domaines d'applications de ces systèmes d'IA, aussi bien dans le champ de la finance, des services de répressions, de la sécurité des produits ou des institutions nationales en lien avec les affaires sociales (assurance chômage, service à l'éducation et à la formation, etc.), il est à la fois technique par certains aspects et générique pour certaines des exigences attendues.

La proposition de la CE se base sur le « Nouveau Cadre Législatif » (NLF) où les moyens d'atteindre les objectifs juridiques s'appuient majoritairement sur la normalisation et les spécifications communes³.

Enfin, le projet de règlement prévoit des dispositions⁴ qui permettent à la CE de modifier et d'ajuster un certain nombre d'articles. L'objectif assumé est donc de permettre à la réglementation d'évoluer en fonction des retours d'expérience et ainsi de corriger d'éventuelles dérives, contraintes jugées inutiles, ou situations que le législateur n'aurait pas prévues.

Cette volonté d'adaptation est encore renforcée dans les dispositions finales à l'article 84 qui impose une ré-évaluation et un ré-examen périodiques de tout ou partie du règlement :

- une revue de la liste des domaines couverts par les IA à haut risque (Annexe III) chaque année ;
- une revue de l'ensemble du règlement tous les 4 ans ;
- l'évaluation de l'efficacité des codes de conduites pour les IA autorisées qui ne sont pas à haut risque tous les 4 ans.

La définition d'IA

L'IA est définie à l'article 3 comme suit :

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

Elle se caractérise donc par les approches utilisées pour son développement et non à travers une définition rigide. On distingue les approches :

- d'apprentissage automatique,
- fondées sur la logique et les connaissances,
- statistiques.

Le projet de règlement IA s'articule autour de différents types d'IA : celles qui sont interdites, les IA à haut risque qui nécessitent de respecter un certain nombre d'exigences avant de pouvoir être mises sur le marché, et enfin, tous les autres systèmes d'IA qui sont considérés comme ne présentant pas ou peu de risque pour la santé, la sécurité ou les droits fondamentaux.

1. Projet de règlement IA : <https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52021PC0206>.

2. On notera entre autres :

Le livre blanc « Intelligence artificielle – Une approche européenne axée sur l'excellence et la confiance » publié le 19 février 2020 ;

La résolution du Parlement européen du 20 octobre 2020 contenant des recommandations à la Commission concernant un cadre pour les aspects éthiques de l'intelligence artificielle, de la robotique et des technologies connexes.

3. Les spécifications communes sont définies à l'article 41 comme étant les documents mis en place par la Commission européenne en l'absence de normes harmonisées, ou si les normes harmonisées existantes sont insuffisantes. Ces spécifications communes sont adoptées via des actes d'exécution, juridiquement contraignants.

4. La définition de l'IA, l'annexe III précisant les domaines des systèmes d'IA à haut risque, le contenu du dossier technique et la procédure d'évaluation de la conformité applicable aux systèmes d'IA à haut risque sont modifiables via des actes délégués (cf. articles 4, 7, 11 et 43).

Qu'est-ce que le « fournisseur » du système d'IA ?

La notion de « fournisseur » remplace celle de « fabricant » généralement établie dans les autres réglementations sectorielles telles que celles pour les machines ou les équipements de protection individuelle. Il s'agit du concepteur du système d'IA qui est responsable de sa mise sur le marché ou mise en service au titre du projet de règlement IA tel que défini à l'article 3 :

(2) « fournisseur », une personne physique ou morale, une autorité publique, une agence ou tout autre organisme qui développe ou fait développer un système d'IA en vue de le mettre sur le marché ou de le mettre en service sous son propre nom ou sa propre marque, à titre onéreux ou gratuit.

À noter que le règlement introduit également la notion de « petit fournisseur » qui bénéficie de mesures spécifiques de soutien à son activité à l'article 55 :


« petit fournisseur », un fournisseur qui est une micro ou petite entreprise au sens de la recommandation 2003/361/CE de la Commission

Selon la recommandation citée, la petite entreprise est définie comme une entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros, là où la microentreprise est définie comme une entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros.

Les pratiques interdites en matière d'IA

Le projet de règlement définit clairement les pratiques interdites en ce qui concerne le développement, la mise sur le marché et l'utilisation d'IA. La Commission européenne rend illégale :

- « la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui a recours à des techniques subliminales au-dessous du seuil de conscience d'une personne pour altérer substantiellement son comportement d'une manière qui cause ou est susceptible de causer un préjudice physique ou psychologique à cette personne ou à un tiers » ;
- « la mise sur le marché, la mise en service ou l'utilisation d'un système d'IA qui exploite les éventuelles vulnérabilités dues à l'âge ou au handicap physique ou mental d'un groupe de personnes donné » ;
- « la mise sur le marché, la mise en service ou l'utilisation, par les pouvoirs publics ou pour leur compte, de systèmes d'IA destinés à évaluer ou à établir un classement de la fiabilité de personnes physiques au cours d'une période donnée en fonction de leur comportement social ou de caractéristiques personnelles ou de personnalité connues ou prédites » ;

 **Note EUROGIP :** ce domaine spécifique étant interdit pour les seuls pouvoirs publics, il serait donc autorisé pour des entreprises privées. Ainsi certains acteurs économiques seraient en mesure de noter leurs salariés, ou encore un réseau social pourrait établir des profils sociaux.

- « l'utilisation de systèmes d'identification biométrique à distance « en temps réel » dans des espaces accessibles au public à des fins répressives, sauf si et dans la mesure où cette utilisation est strictement nécessaire » (criminalité, terrorisme, recherche de victimes).

À noter que l'utilisation de systèmes biométriques en temps réel est possible dans le projet de règlement :

- Sur autorisation préalable octroyée par une autorité judiciaire ou administrative indépendante de l'État membre dans lequel cette utilisation doit avoir lieu ;
- Si les modalités nécessaires à la demande, à la délivrance et à l'exercice des autorisations sont clairement spécifiées dans l'État membre.

Qu'est-ce qu'une « autorité répressive » ?

Cette notion est définie à l'article 3 comme suit :

(40) « autorités répressives »,

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

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

(41) « fins répressives », des fins ayant trait aux activités menées par les autorités répressives pour la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Les systèmes d'IA à haut risque

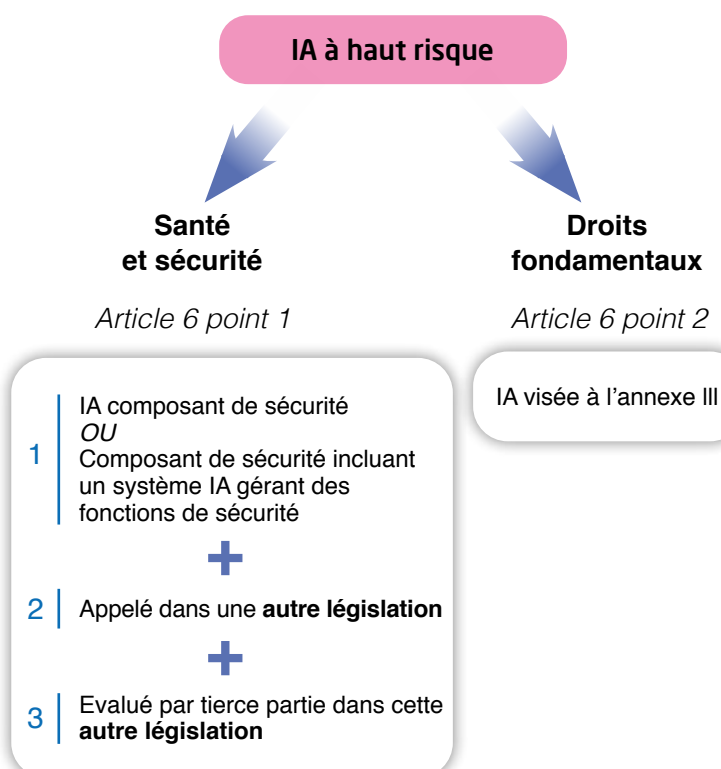
Le projet de règlement se concentre essentiellement sur ce type de système d'IA. Outre les critères faisant basculer un système d'IA dans la catégorie à haut risque, de nombreuses exigences traitent des obligations des différents opérateurs économiques quant à leur mise à disposition et leur utilisation ainsi que des procédures d'évaluation de la conformité à mettre en œuvre.

Qu'est-ce qu'un système d'IA à haut risque ?

L'article 6 précise qu'un système IA mis sur le marché ou mis en service est à haut risque dans deux situations :

- Soit le système IA est utilisé dans un domaine listé à l'Annexe III⁵ ;
- Soit il répond à la double condition suivante :
 - Le système IA est destiné à être utilisé comme composant de sécurité d'un produit couvert par une autre législation, ou est lui-même le composant de sécurité couvert par une autre législation ; **ET**
 - Le produit intégrant le système IA en tant que composant de sécurité, ou le système d'IA lui-même, est soumis à une évaluation de conformité par tierce partie dans la législation de l'Union correspondante.

On pourrait donc résumer le second tiret de la façon suivante : **un composant de sécurité IA est dit à haut risque si et seulement si le composant ou son intégration dans le produit final est soumis à évaluation par Organisme Notifié (O.N.) dans la législation du produit concerné.**



5. Les principaux domaines visés par cette annexe concernent pour exemple : l'identification biométrique, la gestion et l'exploitation des infrastructures critiques, l'éducation et la formation professionnelle, les actions dans le giron des autorités répressives, l'administration et le processus démocratique.



Note EUROGIP : *La Commission européenne traite donc les objectifs de prise en compte du risque liés au droits fondamentaux via l'Annexe III là où les aspects santé et sécurité sont couverts par la notion de composant de sécurité. Il est pour autant dommage d'avoir alourdi cette approche du composant de sécurité en le liant à une nécessaire évaluation de conformité par tierce partie dans les autres législations sectorielles.*

Cela crée donc potentiellement une distorsion de traitement d'un système IA en fonction des dites législations produit : un même système IA utilisé comme composant de sécurité pourra être considéré comme système à haut risque par son traitement dans la réglementation équipement de protection individuelle, mais en être exclu pour une application couverte par la réglementation dispositifs médicaux ou ATEX.

Cette définition introduit également un risque juridique accru pour le fournisseur de système IA qui devra avoir une connaissance exhaustive des réglementations sectorielles pour lesquelles son IA sera potentiellement utilisée, afin de savoir si le système d'IA est à considérer à haut risque ou non.

Il eut été bien plus simple et cohérent de considérer tout système IA assurant des fonctions de sécurité⁶ comme étant des systèmes à haut risque.

Quelles sont les exigences applicables aux systèmes d'IA à haut risque ?

L'ensemble du chapitre 2 du projet de règlement traite des exigences techniques auxquelles doivent répondre les systèmes d'IA à haut risque. Ces exigences doivent garantir que ces systèmes, disponibles dans l'Union, présentent un risque minimum pour la santé, la sécurité et les droits fondamentaux des citoyens de l'Union.

A cette fin, il est essentiel de disposer d'informations pertinentes sur le système d'IA à haut risque tout au long de son cycle de vie. Le projet impose donc qu'il y ait :

- mise en place d'un système de gestion de risque (article 9),
- pour les IA « apprenantes », mise en place d'une gouvernance de données (article 10),
- réalisation du dossier technique conformément à l'Annexe IV (article 11),

- mise en place d'un dispositif de journaux d'enregistrement (article 12),
- fourniture d'une notice d'utilisation garantissant la transparence et l'information aux utilisateurs (article 13),
- mise en place du contrôle humain (article 14),
- fiabilité des IA (article 15).

Documentation technique (article 11)

Avant toute mise sur le marché ou mise en service d'un système d'IA à haut risque, il est nécessaire que le fournisseur du système élabore la documentation technique. Celle-ci permet de démontrer que l'ensemble des exigences applicables aux systèmes d'IA à haut risque ont bien été respectées.

Comme pour les autres législations sectorielles, la documentation technique peut être exigée par les autorités de surveillance du marché afin de s'assurer que le système IA est bien conforme au règlement. Il s'agit donc d'un document clé pour prouver la bonne prise en compte des obligations du fournisseur d'IA.

Le contenu du dossier technique est spécifié en Annexe IX du projet de règlement IA et contient :

- la description générale du système IA, incluant la destination du système, ses interactions possibles, les versions logicielles, les caractéristiques techniques du matériel informatique sur lequel le système peut être utilisé, la notice d'utilisation, etc. ;
- une description détaillée des éléments du système d'IA et du processus de développement (la logique générale du système d'IA et des algorithmes, la description de l'architecture du système, les procédures de validation et de test utilisées, la gouvernance des données, la démonstration de l'exactitude, de la robustesse et du respect des exigences liées à la cybersécurité, etc.) ;
- des informations détaillées sur la surveillance, le fonctionnement et le contrôle du système d'IA, y compris les mesures relatives au contrôle humain ;
- une description détaillée du système de gestion des risques ;
- le suivi des modifications apportées au système ;
- une copie de la déclaration UE de conformité ;
- la liste des normes harmonisées ou des spécifi-

6. La notion de fonction de sécurité est bien définie côté machines dans la norme EN ISO 12100 : 2010 - *Principes généraux de conception - Appréciation du risque et réduction du risque*, au §30 : « fonction d'une machine dont la défaillance peut provoquer un accroissement immédiat du (des) risque(s) ». Cette définition peut être transposable à l'ensemble des réglementations sectorielles tant sa portée est générale.

cations techniques utilisées pour évaluer la conformité du système d'IA ;

- une description détaillée du dispositif en place pour évaluer les performances du système d'IA après sa commercialisation conformément à l'article 61.

Le projet de règlement apporte des précisions concernant les attendus vis-à-vis de certains des aspects du dossier technique comme détaillé ci-après.

Le système de gestion des risques (article 9)

Il s'agit, *in fine*, d'un support qui établit et documente le processus d'appréciation et de réduction des risques du système IA et qui doit être tenu à jour. Le principe est similaire à ceux décrits dans l'EN ISO 12100 : 2010 *Sécurité des machines — Principes généraux de conception — Appréciation du risque et réduction du risque*. Il s'agit d'un processus itératif qui, pour les risques susceptibles d'apparaître lorsque le système d'IA à haut risque est utilisé conformément à sa destination, vise à :

- identifier,
- estimer,
- évaluer,
- réduire les risques par l'adoption de mesures appropriées.

La réduction du risque doit se faire selon les principes d'intégration de la sécurité à la conception, puis, pour la part du risque impossible à éliminer, via des mesures d'atténuation du risque et enfin par la fourniture des informations nécessaires à l'utilisateur, voire à la formation des opérateurs.

Le système de gestion des risques doit également prendre en compte les mesures nécessaires pour tes-

ter le système IA avec les procédures appropriées durant le processus de développement, et avant la mise sur le marché ou la mise en service du système IA.

Données et gouvernance des données (article 10)

L'exigence concernant la gouvernance des données n'est applicable qu'aux systèmes d'IA entraînés par apprentissage avec des jeux de données. Le projet de règlement insiste sur la nécessité d'en garantir la qualité, que ce soit par le choix de la conception des jeux de données, ou par leur collecte et leur traitement.

Il est également nécessaire de pouvoir garantir l'exactitude et la complétude des jeux de données.

Enregistrement et journaux d'enregistrement (article 12)

Les systèmes d'IA à haut risque se doivent d'avoir des fonctionnalités permettant l'enregistrement automatique des événements pendant le fonctionnement. Celles-ci garantissent la traçabilité du fonctionnement du système d'IA tout au long de son cycle de vie, notamment pour sa « surveillance après commercialisation » telle que définie à l'article 61.

La nature et la fréquence de ces enregistrements ne sont pas spécifiées. Il sera laissé le soin aux concepteurs de normes et de spécifications communes de définir les moyens de répondre à cette exigence.

A noter que des spécifications additionnelles sont données concernant l'enregistrement pour le système d'IA destiné à être utilisé pour l'identification biométrique à distance « en temps réel » et « a posteriori » des personnes physiques.

Qu'est-ce que la surveillance après commercialisation ?

Cette notion est définie à l'article 3 comme suit :

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

Dans les faits, le fournisseur de système d'IA à haut risque doit mettre en place un système pour collecter les informations pertinentes auprès des utilisateurs, ou via d'autres sources (comme une collecte directe depuis le système d'IA). Ce système de surveillance doit ainsi permettre d'évaluer si le système d'IA à haut risque continue à respecter les exigences du règlement.

Transparence et fourniture d'informations aux utilisateurs (article 13)

Cette exigence vise à définir le degré d'information nécessaire sur le système d'IA à haut risque pour permettre aux utilisateurs d'interpréter les résultats du système et de l'utiliser de manière appropriée.

Il est donc nécessaire que le système d'IA soit accompagné d'une notice d'utilisation comprenant, outre l'identité et les coordonnées du fournisseur du système d'IA, les éléments suivants :

- les caractéristiques et capacités du système IA selon sa destination, sa performance et son niveau de fiabilité, y compris en ce qui concerne la cybersécurité ;
- les circonstances pouvant amener l'IA à entraîner des risques pour la santé, la sécurité ou les droits fondamentaux ;
- les spécifications relatives à l'apprentissage (données d'entrées, jeux de données d'entraînement, validation, etc.) ;
- les mesures de contrôle humain tel que définis à l'article 14 ;
- les mesures de maintenance.

Contrôle humain (article 14)

Le contrôle humain a pour objectif de réduire les risques pour la santé, la sécurité ou les droits fondamentaux qui peuvent apparaître malgré le fait que le système d'IA à haut risque est utilisé conformément aux spécifications données dans la notice d'instruction. Il doit garantir que « *le système est soumis à des contraintes opérationnelles intégrées qui ne peuvent*

pas être ignorées par le système lui-même ». Autrement dit, l'opérateur doit pouvoir garder le contrôle sur le système IA à tout moment.

Ce contrôle humain est assuré par des mesures identifiées et intégrées par le fournisseur dans le système d'IA : un moyen doit être prévu pour que l'utilisateur contrôle le système IA en l'arrêtant, en le corrigeant, en l'ignorant, ou par toute autre action appropriée.

Le projet de règlement insiste sur les prérequis pour que l'utilisateur soit en mesure d'utiliser le contrôle humain, lesquels sont de différentes natures :

- Tout d'abord, l'utilisateur doit être en mesure d'appréhender les capacités et les limites du système afin de pouvoir effectuer la surveillance adéquate (à quels moments du processus son attention est-elle nécessaire) et de détecter les anomalies ou dysfonctionnements. Cela implique donc que la notice d'instruction fournisse les éléments suffisants.
- Ensuite, il doit être conscient qu'il se fie de façon « *naturelle ou excessive aux décisions du système d'IA* ».



Note EUROGIP : *Il paraît étonnant d'introduire ce concept de conscience de la dépendance à la décision d'un dispositif qui est censé assurer la sécurité de l'opérateur. Dans le domaine des machines par exemple, l'objectif est bien de pouvoir se fier aux dispositifs de sécurité mis en place pour éviter notamment une charge mentale trop importante lorsque l'utilisateur réalise l'ensemble de ses tâches. Normalement, c'est le respect du niveau de fiabilité requis du dispositif de sécurité et sa bonne implémentation qui donne ce niveau de confiance. Doit-on en déduire que le « contrôle humain » est nécessaire car il n'est pas souhaitable de se fier à la décision du système IA ?*

L'intervention de l'utilisateur pour assurer la sécurité est-elle demandée dans l'article 14 point 2 ?

« 2. Le contrôle humain vise à prévenir ou à réduire au minimum **les risques pour la santé, la sécurité ou les droits fondamentaux** qui peuvent apparaître [...] en particulier lorsque de tels risques persistent nonobstant l'application d'autres exigences énoncées dans le présent chapitre. »

Avec cette formulation, il semble que l'utilisateur d'une machine doive contrôler en permanence l'IA à haut risque, pour les aspects liés à la santé et à la sécurité. Il devrait donc assurer la sécurité dans la prise de décision du système d'IA, ce qui est contraire au principe de sécurité intégrée.

Si l'exigence est réalisable pour les aspects liés aux droits fondamentaux (car l'action de l'opérateur pourrait être menée a posteriori dans un délai raisonnable sans impact), elle ne semble pas pertinente pour ce qui est des risques liés à la santé et à la sécurité puisqu'ils requièrent un traitement en « temps réel ». Cette disposition nécessiterait d'être modifiée.

- L'utilisateur doit également être en mesure d'interpréter correctement les résultats du système, qui peuvent dépendre d'outils ou de méthodes d'interprétation précisés par le fournisseur. Il semble que cet aspect est lié à la transparence de la notice d'instruction qui fournit, entre autres, ces éléments.
- Enfin, il doit être en mesure de décider et d'intervenir sur le fonctionnement du système d'IA via les commandes prévues.

Exactitude, robustesse et cybersécurité (article 15)

Cette exigence traite de la nécessité pour le système d'IA à haut risque d'être conçu avec la fiabilité et la robustesse nécessaires pour fonctionner correctement durant tout son cycle de vie. Les aspects cybersécurité doivent naturellement être pris en compte en étant capable de résister aux tentatives d'exploitation des vulnérabilités du système. Les niveaux de fiabilité doivent d'ailleurs être mentionnés dans la notice d'instruction.

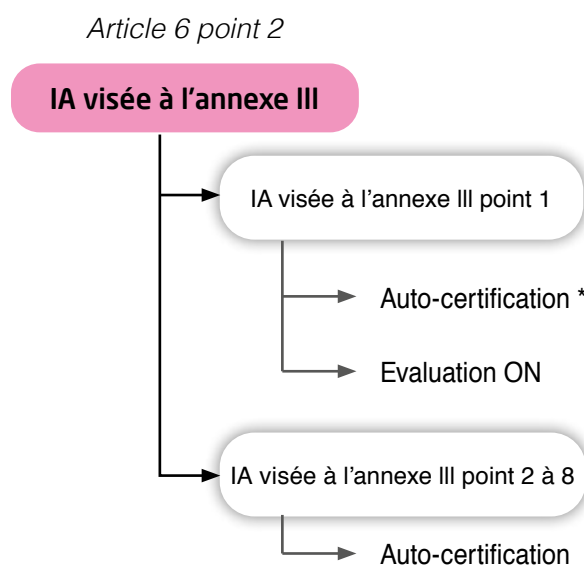
Des solutions techniques redondantes sont attendues (telles que des plans de sauvegarde ou des mesures de sécurité après défaillance) afin de garantir la robustesse des systèmes IA à haut risque.

Lorsqu'il y a phase d'apprentissage suite à la mise sur le marché ou la mise en service, il est nécessaire de prendre en compte les phénomènes de biais dus à l'utilisation de résultats comme données d'entrée pour les opérations futures (« boucles de rétroaction »).

Quelles sont les procédures d'évaluation de la conformité applicables aux systèmes d'IA à haut risque ?

Globalement, la procédure d'évaluation de la conformité de ces IA doit être effectuée conformément à l'article 43, à l'exception des systèmes d'IA destinés à être utilisés pour évaluer la solvabilité des personnes physiques ou pour établir leur note de crédit. Ces derniers sont soumis à une évaluation particulière issue d'une autre législation, qui ne fait pas l'objet de développements dans la présente note.

Hors cette exception, la procédure d'évaluation est dépendante du type de système d'IA à haut risque.



** Normes harmonisées et/ou spécification technique commune pleinement utilisées*

1. Pour les systèmes d'IA définis à l'article 6 point 2 (systèmes utilisés dans les domaines listés à l'Annexe III), les procédures suivantes s'appliquent :

- Si le système d'IA est utilisé dans le domaine de l'annexe III point 1 (Identification biométrique et catégorisation des personnes physiques), alors le fournisseur peut choisir entre :

- la procédure d'évaluation de la conformité fondée sur le contrôle interne visée à l'annexe VI (auto-certification par le fournisseur). Cette procédure est valable uniquement dans le cas où les normes harmonisées, ou les spécifications communes ont été pleinement appliquées ;

- la procédure d'évaluation de la conformité par tierce partie via un O.N. (conformément à l'Annexe VII). À noter que si le système IA est destiné à être mis en service par les autorités répressives, alors l'autorité de surveillance du marché agit en tant qu'O.N.

- Si le système d'IA est utilisé dans le domaine de l'annexe III point 2 à 8, la procédure d'auto-certification s'appliquerait quand bien même les normes harmonisées, ou les spécifications communes n'auraient pas été respectées.

2. Pour les systèmes d'IA définis à l'article 6 point 1 (IA intégrées dans des produits couverts par les législations de l'Union listées en Annexe II section A), les procédures définies selon les modalités requises par ces actes juridiques s'appliquent.

Note EUROGIP : In fine, l'O.N. en charge de l'évaluation de la conformité selon le projet de règlement IA suivra celle applicable par l'O.N. de la législation sectorielle du produit où le système IA sera intégré.

Concrètement, et en se basant sur le Guide bleu⁷ qui détaille, entre autres, l'ensemble des procédures d'évaluation en les catégorisant par « modules », le système IA à haut risque utilisé dans la réglementation Machines⁸ serait évalué selon le module B (examen UE de type) ou le module H (conformité sur la base de l'assurance complète de la qualité) par l'O.N. au titre du règlement IA.

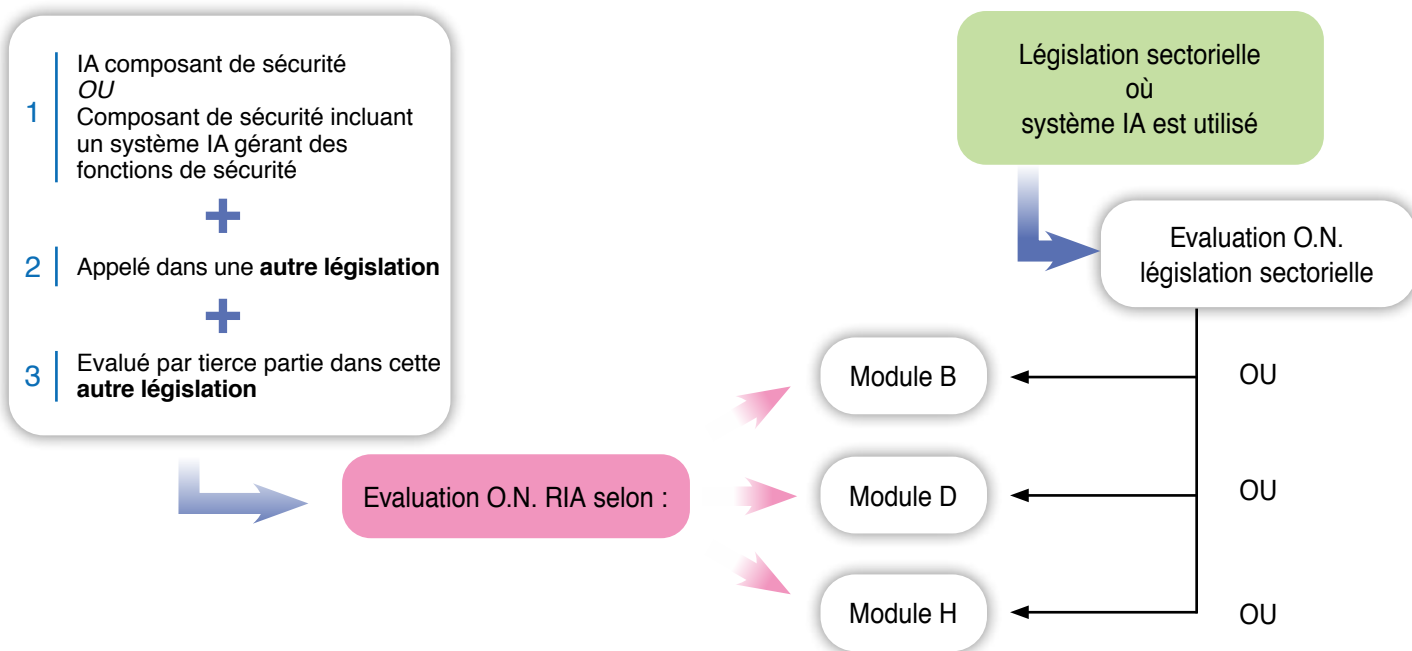
Il est à noter que dans le cadre des systèmes IA définis à l'article 6 point 1, l'O.N. chargé de l'évaluation de la conformité du produit où est intégré le système IA peut être habilité à effectuer l'évaluation de la conformité selon le règlement IA (et donc à contrôler les exigences applicables au système d'IA à haut risque). Il doit cependant répondre aux exigences applicables à l'O.N. règlement IA énoncées à l'article 33 concernant uniquement les points relatifs à l'indépendance du personnel (article 33 point 4), à leur capacité à réaliser les tâches qui leur incombent (article 33 point 9) et de la compétence de leur personnel (article 33 point 10).

Note EUROGIP : L'obligation de participation aux activités de la coordination européenne des O.N. règlement IA (article 33 point 11) n'étant pas listée, un risque de non harmonisation des pratiques entre les différentes législations n'est pas à exclure.

Au-delà des développements ci-dessus, le projet de règlement IA impose de repasser la procédure d'évaluation de la conformité dès lors qu'il y a modification substantielle du système IA.

Le projet de règlement prévoit également une **dérogation à la procédure d'évaluation de la conformité** (article 47).

Une autorité de surveillance du marché peut autoriser à titre exceptionnel (pour des raisons liées à la sécurité publique, la protection de l'environnement, d'infrastructures d'importance majeure, etc.) la mise sur le marché ou la mise en service de système IA à



7. Guide bleu : https://eurogip.fr/wp-content/uploads/2019/12/Guide_bleu_EPI_2016-FR-1.pdf

8. Projet de règlement machines présenté par la Commission européenne le 21 avril 2021 : https://eurogip.fr/wp-content/uploads/2021/08/Proposition-Reglement-machines-et-produits-connexes_avril-2021.pdf.

Pour plus de détails concernant ce projet voir le Focus d'EUROGIP rédigé sur le sujet : <https://eurogip.fr/wp-content/uploads/2021/09/Eurogip-166F-Focus-projet-reglement-machines-2021.pdf>.

Article 43.3 alinéa 3, ambigu ?

L'article 43 point 3, 3^{ème} alinéa fait mention du cas où une auto-certification par le fabricant du composant de sécurité intégrant le système IA est possible et dans quelles conditions :

« Lorsque les actes juridiques énumérés à l'annexe II, section A, confèrent au fabricant du produit la faculté de ne pas faire procéder à une évaluation de la conformité par un tiers, à condition que ce fabricant ait appliqué toutes les normes harmonisées couvrant toutes les exigences pertinentes, ce fabricant ne peut faire usage de cette faculté que s'il a également appliqué les normes harmonisées ou, le cas échéant, les spécifications communes visées à l'article 41 couvrant les exigences énoncées au chapitre 2 du présent titre. »

La Commission européenne fait référence ici aux procédures d'évaluation de la conformité existant dans certaines législations sectorielles, telle que la Directive Machines 2006/42/CE, où l'évaluation de certains produits par tierce partie n'est pas obligatoire dès lors que les normes harmonisées pertinentes ont été pleinement appliquées.

La rédaction interroge toutefois quant à l'utilisation du terme « fabricant » puisque le concepteur d'un système d'IA est désigné par le terme de « fournisseur » dans l'ensemble du projet de RIA.

S'agit-il d'une coquille dans la rédaction ou bien le législateur souhaite-t-il ici traiter du cas particulier du fabricant d'un produit intégrant un système IA qu'il aurait lui-même conçu ?

Dans ce cas, il y aurait redondance avec les exigences de l'article 24 qui relève de la même problématique.

haut risque sur le territoire de l'État membre concerné. Cette autorisation est limitée dans le temps, afin de permettre à la procédure d'évaluation de la conformité d'être menée à bien.

Pour autant, cette autorisation de mise sur le marché ou de mise en service est accordée sous conditions. Tout d'abord, l'autorité de surveillance du marché doit être « **convaincue** » que les exigences applicables au système d'IA à haut risque sont bien respectées. Dès lors, doit-on conclure qu'une évaluation sommaire aura été préalablement réalisée sous la supervision de l'autorité de surveillance du marché ?

Ensuite, l'autorité de surveillance du marché doit informer la Commission européenne et les autres États membres de l'autorisation qu'elle a délivrée. En l'absence d'objection sous quinzaine, la décision est réputée justifiée. Autrement, et en fonction des consultations qui auraient lieu entre les diverses parties, la Commission européenne peut demander le retrait de cette autorisation.

La durée de validité des attestations d'évaluation UE de type délivrées par les O.N. est de 5 ans, comme pour la plupart des réglementations sectorielles. Néanmoins, elle peut être prolongée de 5 ans

lors de chaque ré-évaluation. Du fait de la terminologie employée⁹, **il semble donc nécessaire de procéder à une nouvelle évaluation complète tous les 5 ans.**

Les systèmes d'IA hors champs des systèmes à haut risque

Quelles sont les procédures d'évaluation de la conformité applicables aux systèmes d'IA qui ne sont pas à haut risque ?

Le projet de règlement prévoit que les systèmes d'IA autorisés et qui n'entrent pas dans la classification à haut risque sont évalués selon un « **Code de conduite** » tel que défini à l'article 69.


Il s'agit pour la Commission européenne d'encourager les fournisseurs de ce type de systèmes à :

- appliquer de façon volontaire tout ou partie des exigences associées aux systèmes d'IA à haut risque des articles 8 à 15 ;

9. Le cas échéant, dans les législations sectorielles, il est fait mention de « renouvellement » des attestations émises par les O.N. pour prolonger leur durée de validité. Le projet de RIA n'emploie pas cette terminologie, mais lui préfère la notion de « ré-évaluation ».

- mettre en place des exigences additionnelles pouvant être associées à l'environnement, à l'accessibilité, etc.

Cela peut donc conduire à l'élaboration de programmes de certification dans une optique vertueuse et allant au-delà de ce qui est réglementairement attendu. Pour autant, les modalités de mise en place de ces « codes de conduite » et de leur vérification ne sont pas clairement établis.

 **Note EUROGIP :** *S'il est bien précisé que ceux-ci peuvent être élaborés par les fournisseurs de système d'IA, les utilisateurs et toutes autres parties prenantes, on peut s'interroger sur les structures d'encadrement devant être mises en place. Ces codes de conduite devront-ils être réalisés sous l'égide des bureaux de normalisation (et donc soumis aux mêmes règles de décision) ? La Commission européenne aura-t-elle un droit de regard¹⁰ ?*

Quelles sont les obligations des différents acteurs économiques ?

Les obligations du fournisseur de système d'IA à haut risque :

L'article 16 définit les obligations du fournisseur du système d'IA à haut risque, lesquelles doivent être respectées avant la mise sur le marché ou la mise en service dudit système. Outre les obligations de conformité aux exigences associées à ce type de système d'IA (cf. développements précédents), ou de la mise en place d'actions correctives si certaines venaient à ne plus être respectées, le fournisseur doit avoir mis en place la procédure d'évaluation de la conformité idoine telle que définie à l'article 43.


Le fournisseur doit également mettre en place un système de gestion de la qualité tel que décrit à l'article 17. Ce dernier, **constitué de procédures et d'instructions écrites**, doit permettre de **garantir le bon respect des exigences** du projet de règlement dans le temps. Il comprend les procédures de gestion des modifications du système d'IA, les procédures de développement, de vérification et de validation, les procédures liées à la gestion de la communication avec

les autorités nationales, etc. **Il s'agit donc pour le fournisseur de l'outil lui permettant de structurer son activité.**

Le fournisseur devra ensuite établir la déclaration UE de conformité du système IA conformément à l'article 48 et apposer le marquage CE, soit sur le produit, soit sur l'emballage ou tout type de document accompagnant le système d'IA. À noter que lorsque l'évaluation de conformité a été réalisée par un O.N., son numéro d'identification devra être accolé au marquage CE.

Il est également nécessaire que le fournisseur réalise l'enregistrement de son système d'IA à haut risque dans la base de données communautaire¹¹ mise en place par la Commission européenne.

Enfin, le fournisseur doit faire part de tout incident grave¹² survenu sur son système IA à haut risque mis sur le marché. Cette notification doit se faire aux autorités de contrôle de l'État membre où est survenu l'incident et doit être effectuée dans les 15 jours après la survenue de ce dernier.

 **Note EUROGIP :** *Le projet de règlement IA réserve cette notification uniquement aux incidents ayant un impact sur les droits fondamentaux et non pas sur les risques liés à la santé ou à la sécurité.*

Les obligations du fournisseur de système d'IA autres

Il ne semble pas qu'il y ait d'obligations liées à la mise sur le marché ou la mise en service de systèmes d'IA qui ne seraient pas à haut risque, ni en matière de déclaration UE de conformité, ni même de marquage « CE ».

Les obligations du fabricant de produits intégrant un système d'IA à haut risque

L'article 24 introduit des obligations pesant sur **les fabricants de produits qui intègrent un système IA à haut risque sous son propre nom**. Ceux-ci sont soumis au règlement IA au même titre qu'un fournisseur de système IA. Si l'exigence, en soit, est peu explicite, elle fait toutefois écho au considérant 55 :

10. L'article 84 suggère que les autorités européennes évaluent périodiquement l'impact et l'efficacité des codes de conduite.
11. L'Article 60 spécifie que la Commission européenne crée et tient à jour une base de données pour l'enregistrement des IA à haut risque. Les informations attendues sont listées dans l'Annexe VIII du projet de règlement et seront accessibles librement au public.
12. L'Article 62 détaille le dispositif de notification des incidents graves et des dysfonctionnements.

« Lorsqu'un système d'IA à haut risque qui est un composant de sécurité d'un produit couvert par un acte législatif sectoriel pertinent du nouveau cadre législatif n'est pas mis sur le marché ou mis en service indépendamment du produit, le fabricant du produit final tel que défini par l'acte législatif pertinent du nouveau cadre législatif devrait se conformer aux obligations du fournisseur établies dans le présent règlement et garantir notamment que le système d'IA intégré dans le produit final est conforme aux exigences du présent règlement. »

On en conclut en pratique qu'un fabricant de machine incluant un système d'IA à haut risque n'ayant pas été mis préalablement sur le marché devra appliquer les exigences du règlement IA en plus du règlement Machines. Il serait donc chargé de l'évaluation de la conformité selon les deux réglementations.

Il s'agit *in fine* de l'application de l'article 28 concernant le transfert de responsabilité de fournisseur de système d'IA à des opérateurs économiques mettant sur le marché des systèmes d'IA sous leur propre nom.

Les obligations du distributeur et de l'importateur du système d'IA à haut risque

Les obligations du distributeur et de l'importateur de système d'IA à haut risque sont similaires à celles définies dans d'autres réglementations sectorielles. Les articles 26 et 27 en font des acteurs responsables dans la mise à disposition sur le marché européen de systèmes conformes.

Ils doivent notamment s'assurer que les systèmes d'IA à haut risque disposent du marquage CE, d'une déclaration de conformité, de la documentation et des instructions requises pour l'utilisateur final, et que la documentation technique a bien été constituée par le fournisseur.

Ils doivent également garantir que le transport et le stockage sous leur responsabilité ne compromettent pas la conformité du système d'IA à haut risque.

Dès lors qu'ils ont un doute sur la conformité du système, les importateurs et distributeurs ne doivent

pas le mettre à disposition sur le marché. En cas de risque avéré, ils doivent en informer les autorités de surveillance du marché, ainsi que le fournisseur, et mettre en place les actions correctives nécessaires qui peuvent aller jusqu'au rappel du système¹³.

En complément de ces obligations, les importateurs doivent s'assurer que la procédure d'évaluation de la conformité idoine a bien été réalisée. Ils doivent également être en mesure de fournir l'ensemble des documents démontrant la conformité du système sur demande motivée des autorités de surveillance du marché. Cela comprend notamment l'accès aux journaux automatiquement générés par le système d'IA à haut risque.

Enfin, ils indiquent leur nom et l'adresse postale à laquelle ils peuvent être contactés, soit sur le système d'IA, soit sur son emballage ou la documentation l'accompagnant.

Si un importateur ou un distributeur réalise une modification substantielle, un changement de destination, ou qu'il appose son nom ou sa marque sur le système d'IA à haut risque, il en devient le fournisseur et endosse l'ensemble des obligations lui incombant. Comme rappelé dans le considérant 66, le régulateur considère que ces systèmes doivent faire l'objet d'une nouvelle évaluation de la conformité. « *En outre, pour les systèmes d'IA qui continuent à « apprendre » après avoir été mis sur le marché ou mis en service (c'est-à-dire qui adaptent automatiquement la façon dont les fonctions sont exécutées), il est nécessaire de prévoir des règles établissant que les modifications de l'algorithme et de ses performances qui ont été prédéterminées par le fournisseur et évaluées au moment de l'évaluation de la conformité ne devraient pas constituer une modification substantielle.* »

Les obligations du distributeur et de l'importateur de système d'IA autres

De la même manière qu'aucune exigence n'est applicable aux fournisseurs de système d'IA n'entrant pas dans la catégorie des systèmes à haut risque, **il n'y a aucune obligation liée à la mise à disposition sur le marché pour les distributeurs ou importateurs de ce type de systèmes.**

13. L'article 27 section 4 fait référence à cette obligation pour le distributeur de mettre en place les actions correctives et / ou rappel des systèmes en cas de risque avéré. Il y est également indiqué que cette obligation s'applique aussi à l'importateur. Pour autant, l'Article 26 dédié aux obligations de l'importateur n'en fait pas mention.

Les obligations des utilisateurs de systèmes d'IA à haut risque

Conformément à l'article 29, les utilisateurs doivent utiliser le système d'IA à haut risque conformément à la notice d'instruction et mettre en œuvre les moyens de contrôle définis par le fournisseur.

Ils surveillent le fonctionnement du système d'IA à haut risque sur la base de la notice d'utilisation et sont tenus d'arrêter d'utiliser le système d'IA s'ils ont des raisons de penser que celui-ci présente un risque.

Enfin, ils doivent assurer la tenue des journaux générés automatiquement par le système lorsque ces derniers sont sous leur contrôle. La durée de stockage de ces informations n'est cependant pas spécifiée et sera à l'appréciation des utilisateurs en fonction de la destination du système.

On constate donc que le projet de règlement IA régit aussi bien la conception que la partie utilisation des systèmes IA en toute sécurité.

Les obligations des utilisateurs de systèmes d'IA autres

Encore une fois, seules les obligations liées à l'utilisation des systèmes d'IA à haut risque font l'objet d'exigences pour les utilisateurs. **Aucune exigence n'est applicable aux IA autorisées qui ne sont pas à haut risque.**

Les obligations des autorités notifiantes et des organismes notifiés

Les articles 30 à 39 du chapitre 4 détaillent les obligations des autorités notifiantes ainsi que les exigences applicables aux organismes notifiés. Ces articles sont

similaires à ce qui existe dans d'autres législations sectorielles et n'apportent aucune différence majeure.

Une **coordination doit être organisée au niveau européen** et les décisions qui y sont prises doivent être appliquées par l'ensemble des O.N.

Les obligations des États membres et des autorités de surveillance du marché

Le projet de règlement IA introduit un certain nombre de dispositions visant à mettre en place des mesures de soutien à l'innovation¹⁴. Ces mesures doivent permettre le développement de la filière européenne.

Pour ce faire, la Commission européenne permet aux États membres de développer des « bacs à sable réglementaires » en vue de stimuler l'émergence d'acteurs liés à la conception, au développement et à la validation des systèmes d'IA. Il s'agirait donc pour un État membre de créer des régimes dérogatoires au projet de règlement IA, sous la supervision de l'État membre, et pendant une durée limitée.

Il est attendu que les États membres mettant en place ces « bacs à sable réglementaires » se coordonnent et échangent des informations quant au fonctionnement de leurs dispositifs.

Par ailleurs, les missions ainsi que les pouvoirs qui doivent être assumés par les autorités de surveillance du marché sont définis aux articles 63 à 68. Y sont décrits les détails concernant l'accès aux données et à la documentation du fournisseur, y compris le recours à des moyens techniques de tests pour analyser le comportement de certains systèmes d'IA à haut risque.

Le comité européen de l'Intelligence artificielle

Afin d'assister la Commission européenne, il est prévu à l'article 56 de créer un « Comité européen de l'intelligence artificielle ». Celui-ci assure une fonction de soutien et de conseil afin de faciliter la coopération entre autorités de contrôle, d'orienter les décisions des États membres en matière d'IA, voire d'aider les États membres à appliquer le projet de règlement IA.

Ce comité est constitué des directeurs, ou équivalent, des autorités de contrôle nationales et du Contrôleur européen de la protection des données.

14. Il s'agit de l'ensemble des dispositions du Titre V, qui regroupe les articles 53 à 55.

Dans certains cas, l'autorité de surveillance du marché peut être amenée à réaliser une évaluation de la conformité du système IA.

À noter qu'il est également prévu des dispositions spécifiques aux non-conformités formelles constatées par un État membre. Celui-ci devra restreindre ou interdire la mise à disposition du système IA, voire imposer son retrait ou son rappel si la non-conformité persiste.

Enfin, l'article 71 spécifie les montants précis, en fonction de la nature de la non-conformité, que les autorités nationales peuvent appliquer aux fournisseurs ne respectant pas le règlement IA :

- non-respect concernant les interdictions de pratiques concernant l'IA, ou de la gouvernance des données spécifiées à l'article 10 : amende pouvant aller jusqu'à 30M€ ou 6% du chiffre d'affaires mondial de l'entreprise ;

- tout autre non-respect du règlement : amende pouvant aller jusqu'à 20M€ ou 4% du chiffre d'affaires mondial de l'entreprise ;

- communication d'informations inexactes, **incomplètes** ou trompeuses aux O.N. ou autorités de surveillance du marché : amende pouvant aller jusqu'à 10M€ ou 2% du chiffre d'affaires mondial de l'entreprise.

Conclusion

Ce projet de règlement IA doit permettre de structurer toute une filière sur une technologie en plein essor. Le besoin est d'autant plus grand que l'IA s'applique à de nombreux domaines et va, dans les années à venir, s'intégrer à des produits soumis à différentes législations sectorielles qui ne l'ont pas forcément prévu.

De fait, cette réglementation « chapeau » donne des objectifs indispensables à une intégration en toute confiance de ces systèmes d'IA.

Pour autant, elle représente également un énorme défi pour les fournisseurs de ces types de logiciels, dans la mesure où une réflexion en amont leur sera nécessaire avant de se lancer dans l'élaboration de leur solution : il s'agira de définir préalablement à tout développement le domaine d'application précis afin de déterminer les limites du système, d'aboutir à une analyse globale de la maîtrise des données d'entrée et d'éviter toute dérive dans la chaîne de décision du système.



Intelligence artificielle **Focus sur le projet de règlement européen**

EUROGIP - Paris

Avril 2022

Réf. EUROGIP - 170/F

ISBN 979-10-97358-43-3

Directeur de la publication : Raphaël Haeflinger

Auteur : Pierre Belingard

Créé en 1991 par l'Assurance Maladie-Risques professionnels,
EUROGIP est un observatoire et un centre de ressources sur
la prévention et l'assurance des risques professionnels en Europe

