**Artificial Intelligence Act (AI Act)**

**Contribution de Numeum**

(encadré « take-aways »)

# **Contexte**

Dans la continuité du livre blanc sur l’intelligence artificielle (IA), la Commission européenne a présenté, le mercredi 21 avril, une proposition de règlement pour l’établissement de règles harmonisées en matière d’IA, aussi intitulée Artificial Intelligence Act. Avec cette initiative, la Commission propose de nouvelles règles visant à faire de l'Europe *« la place mondiale de l’IA de confiance »*. La proposition prévoit notamment :

* Des exigences relatives aux utilisations de l'IA à haut risque ;
* L’interdiction de certaines utilisations de l’IA ;
* L’autorégulation sur les IA dites « à faible risque » ;
* La création d’un Conseil de l’IA animé par les 27 Etats membres.

Syntec Numérique et TECH IN France soutiennent la Commission dans son ambition de stimuler le développement et l'adoption de l'IA et des nouvelles technologies, tout en veillant à ce que les risques potentiels soient traités de manière adéquate.

Ainsi, la volonté de la Commission européenne de créer un système européen à même de garantir la confiance des citoyens et stimuler l’adoption des usages IA, tout en assurant celle des entreprises dans le déploiement de leurs produits et applications IA et la capacité d’innovation en Europe, nous apparaît une stratégie ambitieuse et adaptée aux enjeux de développement du potentiel de l’IA en Europe.

L’UE a les moyens de devenir un acteur mondial de l’IA. Cela suppose qu’elle encourage l'amélioration de l'accès aux données et la collaboration entre les entreprises, ce qui contribuera à la transformation numérique de l'Europe. L’UE et les Etats membres doivent pleinement s’engager dans cette transition, par des investissements massifs dans les technologies et les infrastructures qui permettront à l'Europe de développer ses atouts en matière d’IA, notamment pour la formation des chercheurs et ingénieurs ainsi que l’accompagnement de l’évolution des métiers concernés. **Nos deux organisations appellent à continuer à façonner une approche européenne de l’IA ouverte et inclusive qui favorise l’innovation tout en assurant la sauvegarde des droits fondamentaux.**

Compte tenu de la diversité des applications et des technologies de l'IA, nous saluons le fait que la Commission adopte une approche ciblée et fondée sur les risques. Une telle approche devrait être basée sur des définitions claires et prendre en compte le risque posé par le déploiement d'un système d'IA, le domaine d'application, le type de déploiement et la nature des risques.

Dans cette optique, Syntec Numérique, TECH IN France et leurs adhérents souhaitent réitérer ici l’attention portée à l’adoption d’une **approche pragmatique et équilibrée dans la définition du nouveau cadre règlementaire par la Commission européenne.**

Enfin, nos deux organisations souhaitent poursuivre leur implication vis-à-vis des travaux et des réflexions conduits par la Commission européenne, le Parlement et le Conseil dans le cadre de cette initiative.

# **L’approche par les risques**

La Commission européenne propose de développer et graduer la régulation européenne en matière d’IA selon une approche basée sur le niveau de « risque », avec une classification à quatre niveaux : les pratiques d’IA interdites (Article 5), les systèmes d’IA à haut risque (Titre 3), les systèmes d’IA avec des obligations de transparence spécifiques (Titre 4) et toutes les autres systèmes IA (sans risques).

* Syntec Numérique et TECH IN France se félicitent que la Commission adopte une approche fondée sur le risque et reste attentif à ce que les nouvelles exigences soient suffisamment simples et claires, et que la mise en œuvre de l’initiative soit suffisamment ambitieuse pour accompagner l'Europe à devenir un pôle mondial de l'IA. Dans nos prises de positions précédentes sur le livre blanc sur l’IA[[1]](#footnote-1), nous plaidions pour l’adoption d’une approche proportionnée visant à réguler les cas d'utilisation à haut risque et non la technologie d'IA.
* Dans ce cadre, il semble essentiel que le champ d’application, les définitions et la distinction entre les acteurs soient précisés. Certaines définitions (« intelligence artificielle », « wifi », « technique subliminale », « pratiques manipulatrices », etc.) restent très larges ou trop vagues, comme, à titre d’exemple, la définition des systèmes IA à haut risque ainsi que la liste des techniques couvertes (Annexe I). Avec une définition et une liste aussi étendue, le risque est de faire entrer de nombreuses applications dans le champ d’application du Titre III et ainsi de faire peser d’importantes obligations à certains acteurs. Une telle définition semble avoir pour effet de faire peser d’importantes obligations à de nombreux acteurs ce qui pourrait avoir pour conséquence un ralentissement de l’innovation. Une balance bénéfice/risque des évolutions technologiques devrait être mise en place en vue de promouvoir l’innovation. En effet, en l’état des mesures proposées par ce texte, il existe un risque de limitation de l’innovation.
* Nous regrettons que le texte ne connaisse pas plus de dispositions de partage de bonnes pratiques qui pourraient permettre de mieux promouvoir le développement de solutions innovantes et de confiance.
* Pour mettre à jour la liste des systèmes d’IA à haut risque (Annexe III), la Commission prévoit l’adoption d’actes délégués. Bien qu’il soit nécessaire pour le règlement de tenir compte des évolutions technologiques, ces actes délégués pourraient être source d’insécurité juridique.
* Certaines exigences à haut risque peuvent être difficiles à mettre en œuvre, si aucune norme n'est disponible à temps. D’autant plus que les éditeurs de logiciels ne sont pas forcément familiarisés avec le cadre de sécurité des produits proposé par la Commission.
* La façon dont les règles s’appliquent, et les conditions pour cela, à l'IA à usage général pourrait également être clarifiée ; le fournisseur ne peut en effet pas savoir à l'avance si l'utilisation sera à haut risque et ne peut pas dicter l'utilisation exacte du système par l'utilisateur.

* Concernant les utilisations de l’IA à faible risque, nous soutenons les obligations minimales de transparence.

Le règlement prévoit que les autorités de surveillance des marchés puissent accéder aux ensembles de données de formation, de validation et de test utilisés par le fournisseur. Lorsque cela est nécessaire et sur demande motivée pour évaluer la conformité du système d'IA à haut risque avec les exigences du règlement, les autorités de surveillance peuvent se voir accorder l'accès au code source du système d'IA. A ce stade, cela soulève un certain nombre de questions.

* Étant donné qu’un modèle commercial spécifique peut être réglementé par diverses autorités de marché lorsqu’une entreprise opère sur plusieurs marchés simultanément, il sera essentiel de clarifier quelle autorité de surveillance sera autorisée à superviser l'IA développée pour un type d’activités donné. De plus, les sanctions devraient être imposées sur la base d'un catalogue clair, basé sur des infractions spécifiques énumérées.
* Nous nous interrogeons sur la justification technique d’accéder aux codes sources du fournisseur dans le cadre du règlement. L’accès aux codes sources constitue un risque pour le fournisseur lui-même Il semble difficile de mettre à disposition un code source même à une autorité publique ou à un organisme notifié. Non pas par crainte de la divulgation de ce code source par ces entités mais ces mesures ne semblent pas respecter les dispositions en matière de cybersécurité et ne paraissent pas respecter le principe de proportionnalité au regard de l’utilité de cette démarche.
* Le règlement impose une obligation d’utiliser des ensembles de données sans erreur (article 10), ce qui est en pratique irréalisable.
* Aussi, il convient de se demander quel traitement sera donné aux systèmes d’IA uniquement alimentés par les données des clients, et non par celles du fournisseur.

# Responsabilités des fournisseurs et des utilisateurs

La proposition de la Commission européenne comprend une série d’obligations incombant aux fournisseurs de systèmes d’IA avant leur mise sur le marché. Après avoir déterminé que le système d’IA peut être considéré à haut risque, le fournisseur doit entreprendre une procédure d’évaluation de conformité et s’assurer que son système d’IA remplit toutes les obligations en termes de transparence, de gouvernance des données, etc. L’utilisateur de l’IA est quant à lui soumis à des obligations liées à la bonne utilisation du produit ou du service.

* Cette répartition des responsabilités entre les fournisseurs et les utilisateurs d’IA manque de clarté, ce qui pourrait poser des difficultés. Les éditeurs de logiciels intégrant des fonctionnalités d’IA à leurs produits ne sont pas en mesure d’anticiper la façon dont ces systèmes d’IA seront mis en œuvre par leurs clients. Ils ne peuvent donc pas anticiper le degré de risque et entreprendre une évaluation de conformité pour des utilisations hypothétiques de leurs produits, et sur lesquelles ils ont peu de contrôle. Les données entrainées par les systèmes d’IA sont généralement celles de leurs clients, ce qui les empêchent de soumettre les jeux de données aux règles de gouvernance énoncées dans la proposition (Article 10).
* La question de l’organisation informatique de l’entreprise utilisatrice et de la multiplicité des briques logiciels se pose également. De nombreux systèmes d’IA se basent sur des data sets différents. Il est à ce titre possible d’avoir plusieurs jeux de données différents pour une même utilisation. Si le fournisseur fournit l’outil, il ne peut prédire la façon dont les données seront traitées. Le cas le plus évident est celui du machine learning qui est capable de reproduire un comportement grâce à des algorithmes, eux-mêmes alimentés par un grand nombre de données. Lorsqu’il est confronté à de nombreuses situations, l'algorithme apprend quelle est la décision à adopter et créé un modèle.
* Concernant la distinction des technologies d’IA, le cas par cas reste clé. La question de la responsabilité se pose d’autant plus que certaines utilisations d’IA sont à la main des utilisateurs. Il n’est pas rare que l’entreprise utilisatrice développe avec le fournisseur son système d’IA et qu’il ajoute par la suite de nouvelles briques technologiques. Dans ce cas précis, le fournisseur n’est pas toujours impliqué dans le formatage ex ante. De plus, dans certains secteurs (par exemple le secteur bancaire), il est compliqué d’avoir accès aux données et donc de comprendre comment les datasets sont construits.
* L’article 28, qui prévoit de faire basculer la responsabilité du fournisseur vers l’utilisateur dans certaines circonstances (notamment quand l’utilisateur reprend sous son nom le système d’IA pour le placer sur le marché), ne semble pas adapté. Une répartition plus claire des responsabilités entre le fournisseur et l’utilisateur correspondrait davantage à la réalité du déploiement de l’IA et à sa mise sur le marché. Il s’agit avant tout de déterminer quelle est l’entité la plus compétente pour déterminer le niveau de risque de l’IA. Cette répartition pourrait s’inspirer du RGPD, en reconnaissant que l’évaluation de conformité doit être entreprise par l’entité définissant l’usage de l’IA dans un des domaines identifiés à l’Annexe III. A ce titre, l’entité déterminant l’usage du système d’IA pourrait s’apparenter au concept de « contrôleur » dans le RGPD. En appliquant la dichotomie contrôleur/processeur à l’utilisation de l’IA, le contrôleur aurait le statut de l’utilisateur d’IA (par exemple, une banque appliquant un système d’IA pour les octrois de prêts), et le processeur serait le développeur/fournisseur du système d’IA. Il ne s’agit pas pour les fournisseurs de se décharger de leurs responsabilités, dans la mesure où ils restent pertinents pour expliquer comment le système d’IA a été élaboré (Article 13), ses capacités et ses limites, ainsi que les conditions optimales de son utilisation.
* Les articles 9, 19 et 43 prévoit pour les opérateurs l’obligation de mener des analyses de risque et de conformité à l’ensemble des législations applicables. Au vu des similitudes que le AI Act peut avoir avec le RGPD, on peut indiquer qu’une analyse d’impact relative à la protection des données (AIPD) est nécessaire dans les cas notamment où un projet comprend une innovation technologique et en la matière quel que soit le nombre de conditions remplies, une telle analyse est préconisée lors de l’utilisation d’une IA. On peut se demander si l’AIPD prévu à l’article 35 du RGPD sera complétée ou si une autre analyse sera prévue. On peut se demander quelle sera l’articulation de l’analyse de risques et de conformité fixée par le texte et l’AIPD prévue à l’article 35 du RGPD. La question du rôle élargi du DPO pourrait également se poser. Enfin, il convient de se demander qui sera en charge au sein de l’organisation de procéder à l’évaluation de la conformité et de rendre des avis sur les projets faisant appel à l’IA.

# **Impact sur les PME et l’innovation**

La Commission européenne encourage les États membres à mettre à disposition des entreprises des bacs à sable réglementaires pour tester les systèmes d’IA avant leur mise sur le marché. Elle souhaite également réduire le poids réglementaire induit par ce nouveau projet de règlement sur les PME et les start-ups.

* Nous saluons les mesures de soutien à l’innovation proposées par la Commission. La pratique des bacs à sables réglementaires doit être encouragée. Cela permet aux entreprises, notamment les startups et les PME, de tester les nouvelles technologies qu’elles développent avant de les lancer sur le marché. Cette démarche de réglementation permet notamment aux entreprises innovantes de bénéficier d’un allègement des obligations relatives à la protection des données personnelles, afin de tester leurs produits ou services. Dans ce cadre, les entreprises peuvent se faire accompagner pour être conformes aux règles de protection des données tout en innovant, et sans risquer de sanctions. Un tel dispositif est donc positif tant pour les entreprises que pour les citoyens, car l’innovation n’irait pas à l’encontre de leur protection.
* Pour les applications IA qui ne sont pas déjà soumises à une évaluation de conformité, il conviendrait que cette évaluation ex ante prenne la forme d'une auto-évaluation et soit combinée à une évaluation ex post, lorsque des problèmes sont identifiés.
* Il est en effet indispensable que les législations à venir sur l’IA (AI Act, législation sur la responsabilité de l’IA, etc.) soient proportionnées et ne soient pas trop complexes à mettre en œuvre par les PME, afin de ne pas les pénaliser et de stimuler l’innovation, en donnant aux entreprises la sécurité juridique nécessaire. Ce nouveau cadre réglementaire devra également éviter de faire peser sur les entreprises des contraintes disproportionnées.
* Les plus petites entreprises auront besoin de conseils, de soutiens financiers, ainsi que de processus simples et rationalisés pour être en mesure de répondre aux exigences. De manière générale, des coûts de mise en conformité élevés pourraient être attendus et pourraient rester élevés même après la mise sur le marché d'un système d'IA. L'impact pourrait être similaire à celui du RGPD pour les PME et startups, ce qui nous amène à nous interroger sur le niveau de sanction qui semble lourd. Complété avec les sanctions prévues par le RGPD, certaines entreprises pourraient connaître des difficultés importantes.
* Une grande partie des dispositions prévues par la Commission européenne se retrouvent en Annexe. Sanctifier des secteurs pourrait représenter un coût d’entrée trop élevé pour les plus petites entreprises. A titre d’exemple, dans le domaine des infrastructures de transport, le fait d’imposer à une startup de s’aligner avec les dispositions du AI Act avec toutes les obligations post-markets s’y rattachant, l’entreprise pourrait avoir moins d’intérêt à développer son produit en Europe. On prend ici l’exemple des transports de façon global, or, les sources de données sont différentes entre celles du véhicule autonome, des objets connectés sur la voierie ou même de reconnaissance de la couleur d’une carrosserie de véhicule.

# **Accès au marché unique et marquage CE**

**Marquage CE**

La proposition de règlement prévoit que les systèmes d'IA à haut risque portent le marquage CE pour indiquer leur conformité au règlement afin qu'ils puissent circuler librement dans le marché intérieur (article 49 du règlement).

Les fournisseurs de systèmes d'IA à haut risque devront veiller à ce que leurs systèmes soient soumis à la procédure d'évaluation de la conformité (article 43) avant leur mise sur le marché ou leur mise en service. Lorsque leur conformité aux exigences a été démontrée à la suite de cette évaluation de la conformité, les fournisseurs établissent une déclaration UE de conformité conformément à l'article 48 et apposent le marquage CE de conformité conformément à l'article 49.

* En ce qui concerne la portée extraterritoriale du règlement, il sera également attendu que la Commission aborde les aspects de responsabilité liés aux technologies d'IA développées en dehors de l'Union européenne dans le cadre de la proposition de règlement sur l'IA, en vue de compléter le projet de règlement dédié aux aspects de responsabilité juridique du développement de l’IA.

**Monitoring post market**

La proposition définit des exigences communes obligatoires applicables à la conception et au développement de certains systèmes d'IA avant leur mise sur le marché. La Commission propose également de définir la situation après la mise sur le marché des systèmes d'IA en harmonisant la manière dont les contrôles ex post sont effectués. Ainsi, tous les fournisseurs devront disposer d'un système de surveillance après la commercialisation de leur système.

La Commission souhaite ainsi garantir que les risques éventuels liés aux systèmes d'IA qui continuent à "apprendre" après leur mise sur le marché ou leur mise en service puissent être traités plus efficacement et plus rapidement. Dans ce contexte, les fournisseurs seront également tenus de mettre en place un système permettant de signaler aux autorités compétentes tout incident grave ou toute violation du droit national et de l’UE protégeant les droits fondamentaux résultant de l'utilisation de leurs systèmes d'IA.

L'application ex post devra garantir qu'une fois le système d'IA mis sur le marché, les autorités publiques disposent des pouvoirs et des ressources nécessaires pour intervenir au cas où les systèmes d'IA génèrent des risques inattendus, qui justifient une action rapide. Elles contrôleront également le respect par les opérateurs des obligations qui leur incombent. La proposition ne prévoit pas la création automatique d'organismes ou d'autorités supplémentaires au niveau des États membres. Les États membres peuvent donc désigner (et s'appuyer sur l'expertise) des autorités sectorielles existantes, qui seraient également chargées de contrôler et de faire appliquer les dispositions du règlement.

* Il conviendra d’assurer une cohérence entre les différents textes législatifs en cours et à venir, notamment sur l’accès et le partage des données (Data Act, Data governance Act, etc.) et sur l’IA (Règlement sur la responsabilité civile, Règlement sur la responsabilité du fait des produits, etc.).
* Aujourd’hui, les domaines d’application et usages potentiels d’une IA sont de plus en plus divers (compréhension du langage naturel, reconnaissance visuelle, robotique, système autonome, machine learning). Dans le cas du machine learning, la qualité des données, le training pattern de ces données et donc les data sets proposés à la machine, sont essentiels.
* Comme indiqué précédemment, les entreprises qui fournissent les solutions d’IA n’ont pas forcément la possibilité d’y accéder une fois créées. A titre d’exemple, l’entreprise A fournit une solution d’IA à une entreprise B pour évaluer l’impact d’un produit sur un consommateur (on peut citer l’exemple d’un produit cosmétique). Si l’entreprise A doit vérifier le système ex post, cela signifie aussi que l’entreprise B donne accès de ses datasets à l’entreprise A. Les considérations relatives à l’accès à la propriété intellectuelle peuvent se poser, ce qui pourra poser des difficultés dans le monitoring post- market.
* Si le monitoring post-market est possible dans le B2C, il est plus complexe dans le B2B.On peut également considérer que cela pourrait engendrer des effets de bord pour le déploiement de ces technologies. Ceci est d’autant plus complexe qu’ouvrir l’accès à ses datasets pour une entreprise se heurte aussi à la question de la plus-value économique pour cette entreprise et de la proriété intellectuelle.

# **Gouvernance**

Pour garantir l’application du règlement, la Commission propose la création d'un conseil européen de l'IA (European Artificial Intelligence Board), composé de 27 autorités nationales et de l’EDPS (autorité de protection des données des institutions européennes). Présidé par la Commission européenne, le Board rédigera des lignes directrices à destination des Etats membres. Comme pour le RGPD, chaque Etat désignera son autorité chargée de la bonne application du règlement. Une autorité de supervision devra aussi êtrdésignée pour réaliser les notifications et la surveillance du marché. Les membres du conseil pourraient avoir une influence sur les utilisations qui seront classées comme "à haut risque" à l'avenir.

* Nous nous interrogeons sur l’autorité (article 59) qui sera chargée d’évaluer la conformité en la matière. Il serait opportun de mieux définir les missions de cette autorité à l’aune des enjeux de compétitivité internationale et de prendre en considération les problématiques relevant de l’innovation, de la recherche et du traitement de données industrielles ou non-personnelles, mais aussi des critères de confidentialité. Afin d’éviter les risques de fragmentations dans l’application du règlement, il est essentiel que les décisions des autorités de contrôle nationales soient harmonisées.
* Hormis la création de ce conseil européen de l’IA, la notion de gouvernance reste encore assez floue.

# **Utilisations de l’IA dans des domaines sectoriels ?**

* Santé (à compléter)
* Industrie (à compléter)
* Autres domaines identifiés ?
1. [Réponse](https://ensemble.syntec-numerique.fr/article/10781) à la consultation sur le livre blanc sur l’IA

[Réponse](https://ensemble.syntec-numerique.fr/article/8942) à l’impact assessment sur la règlementation de l’IA [↑](#footnote-ref-1)