

Septembre 2020

Réponse de TECH IN France à l'Etude d'impact initiale sur l'intelligence artificielle de la Commission européenne

Par la contribution à l'étude d'impact initiale sur l'Intelligence artificielle (IA) ouverte, TECH IN France souhaite poursuivre son implication vis-à-vis des travaux et des réflexions conduits par la Commission européenne dans le cadre de sa stratégie dédiée à l'IA.

Ainsi, le souhait 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 numérique en Europe. De nombreuses entreprises membres de TECH IN France se sont d'ailleurs exprimées publiquement au cours des derniers mois en faveur du principe de l'élaboration d'une régulation.

Dans cette optique, TECH IN France et ses adhérents souhaitent réitérer ici l'attention portée à l'adoption d'une **approche pragmatique et équilibrée dans la définition d'un nouveau cadre réglementaire par la Commission européenne**. Ce principe d'équilibre dans l'élaboration d'une régulation européenne de l'IA apparaît comme essentiel pour **créer les conditions de l'innovation via le développement d'un écosystème de l'excellence, dès le stade de la recherche et de l'innovation**, incitant à une adoption rapide des solutions IA par les entreprises, notamment les TPE et les PME ; et pour être à même 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** par rapport à leurs compétiteurs internationaux, et devra répondre à leurs **besoins de compétitivité dans la bataille mondiale de l'IA et des données**.

Dans le cadre de cette étude d'impact, il est proposé de revenir plus précisément sur les différentes options de régulation de l'IA envisagées par la Commission européenne et présentées au sein du Livre Blanc sur une approche européenne de l'intelligence artificielle en février dernier. Il nous apparaît ainsi important de préciser à nouveau les éléments et points de vigilance, formulés par TECH IN France au sein de sa réponse à la consultation sur le Livre Blanc.

Remarques générales sur le cadre de régulation de l'IA

La Commission européenne propose de **développer et graduer la régulation européenne en matière d'IA selon une approche basée sur le niveau de « risque »**. Elle précise d'ailleurs dans son Livre Blanc de février 2020 que **le principe de proportionnalité** doit guider l'élaboration de ce nouveau cadre réglementaire pour l'IA, qui devrait atteindre ses objectifs avec efficacité **sans être excessivement normatif**, au risque de créer une charge disproportionnée, en particulier pour les PME. Il est en effet indispensable que les législations à venir soient proportionnées et ne soient pas trop complexes à mettre en œuvre par les PME, afin de ne pas les pénaliser. La norme doit pouvoir jouer un rôle porteur de développement économique et non pas contre-productif.

Dans ce cadre, il semble essentiel que le champ d'application, les notions et les critères d'application d'une régulation spécifique soient **définis clairement et de manière pragmatique**, afin de permettre aux entreprises soumises à la régulation de bénéficier de la meilleure visibilité sur les régimes juridiques applicables. Ces éléments sont donc des conditions **indispensables à toute sécurité juridique et à la dynamique d'innovation des entreprises**.

Champ d'application du cadre réglementaire IA : la définition de l'IA

Afin de déterminer le champ d'application de la régulation à définir, la Commission européenne précise dans sa stratégie qu'il s'agit de définir en amont de **manière claire la notion « d'intelligence artificielle »**. Il est intéressant de rappeler qu'il n'existe à ce jour aucune définition arrêtée et acceptée par l'ensemble de l'écosystème, que ce soit par les experts, les académiques ou les entreprises. Pour ce faire, la Commission évoque les éléments principaux composant l'IA : les données et les algorithmes et semble ainsi retenir une **définition vaste de l'IA, qui appelle selon TECH IN France des points de vigilance**.

Il nous apparaît tout d'abord important de préciser ici qu'une **définition claire de l'IA et facilement compréhensible de tous, est une condition de l'efficacité de la régulation**. Définir l'IA en essentialisant les données et les algorithmes implique *de facto* que l'IA couvre un périmètre très large. En ce sens, il conviendrait de **définir plus précisément le périmètre éligible relevant de l'IA par rapport à celui de l'algorithmie en général**. En effet, tout traitement de données, y compris massif, ne relève pas nécessairement du périmètre de l'IA.

Par ailleurs, certaines définitions existantes de l'IA (dont une réalisée par la Commission européenne en 2018 dans sa communication « L'IA pour l'Europe »), certaines opèrent une distinction entre les systèmes d'IA « apprenants », qui font « *preuve d'un comportement intelligent en analysant leur environnement et en prenant des mesures, avec un certain degré d'autonomie, pour atteindre des objectifs spécifiques* » et les systèmes d'IA classiques, « *qui peuvent être purement logiciels, agissant dans le monde virtuel mais aussi dans des dispositifs matériels* ». Suivre une telle logique dans une définition de l'IA permettrait de réaliser des distinctions de régulation selon les catégories d'IA, en réalisant un focus sur les systèmes « apprenants », réduisant ainsi le champ d'application de l'intervention réglementaire à définir et conduisant à ne pas créer une réglementation excessive.

3

Créer un écosystème de la confiance : les options de régulation de l'IA

Sur l'option « 0 » et l'importance du principe de cohérence (« consistency »)

La Commission européenne dans son option « 0 » envisage la possibilité de ne pas créer une réglementation propre aux applications et systèmes d'IA, avec des règles et des exigences spécifiques, dans la mesure où des législations existantes sont déjà applicables à l'IA.

Il apparaît en effet utile qu'une évaluation des législations existantes et de leur capacité à s'appliquer de manière pertinente aux technologies d'IA, soit réalisée au préalable ; cela avant d'envisager toute réglementation dédiée.

Surtout, il semble important de rappeler qu'en cas de nouvelle réglementation, le principe de cohérence (« consistency ») est essentiel. En effet, **la cohérence est nécessaire entre une nouvelle**

régulation de l'IA et les nombreux textes européens ou nationaux existants, qui s'appliquent pleinement comme l'a d'ailleurs relevé la Commission européenne, tels que le RGPD, la directive relative à la sécurité générale de produits, la directive sur l'égalité de traitement entre les personnes sans distinction de race ou d'origine ethnique, la directive sur l'égalité de traitement en matière d'emploi et de travail ou encore la directive relative aux droits des consommateurs.

Il s'agit donc de veiller à ce que l'élaboration de **toute autre forme de nouvelle réglementation soit cohérente avec les textes existants.**

En pratique, les entreprises ont acquis une **expérience conséquente en matière de conformité** (process, outils, documentation, autorégulation...), notamment dans le cadre de la mise en œuvre du règlement général sur la protection des données (RGPD).

Ainsi, en ce qui concerne les décisions automatisées, le RGPD impose des restrictions, mais aussi le droit des individus d'être informés quant à la logique sous-tendant ces décisions. De même, le règlement prévoit, notamment en son article 22, un cadre précis en matière de traitement des données personnelles. **Il sera donc nécessaire pour toute nouvelle régulation en matière d'IA de ne pas se « chevaucher » avec les dispositions déjà prévues par le RGPD.** Surtout, ce principe de cohérence, garantie d'une harmonisation des législations, permettra également aux entreprises de **conserver le cadre juridique auxquelles elles se sont adaptées depuis maintenant plusieurs mois ;** élément nécessaire à la sécurité juridique et donc à la création d'un environnement favorable à la confiance et à l'innovation.

Sur l'option 1, une approche de *soft law*

La Commission européenne dans son option 1 propose de ne pas édicter d'instrument législatif ou réglementaire mais de faciliter, privilégier et promouvoir l'intervention et les initiatives de l'industrie en matière d'IA. Des approches volontaires seraient ainsi privilégiées, reposant sur de bonnes pratiques, le développement de standards et principes... Tout soutien à l'industrie et l'encouragement à la définition et au partage de bonnes pratiques doit être selon nous encouragé.

4

Sur l'option 2 et le principe de labélisation volontaire

Le schéma de labélisation volontaire défini par un instrument législatif, envisagé dans l'option 2 pourrait être un élément contribuant à renforcer la confiance des utilisateurs dans les systèmes d'IA, en facilitant ainsi l'adoption. **Ce système de compliance** devrait néanmoins selon nous laisser aux entreprises **la flexibilité de choisir les outils les plus pertinents pour attester de leur *compliance*.** Des outils concrets tels que les codes de conduite, les certifications, le concept *de privacy by design/ by default*, permettraient aux entreprises de bénéficier de cette flexibilité. L'adoption par les entreprises, notamment les start-ups et les PME, de ce système de labélisation dépendra de cette flexibilité.

Sur les options 3b) et 4, une approche fondée sur le risque

L'approche européenne retenue dans les options 3b) et 4 de l'étude d'impact initiale se fonde sur la notion de « risque », qui doit permettre de graduer la réponse réglementaire. **Cette approche semble pertinente, notamment car elle permet *a priori* de ne pas décourager le développement et l'utilisation de l'IA,** en appliquant une logique réglementaire s'ajustant à la diversité des applications IA ; et semble adaptée à des technologies en évolution comme l'IA et le *machine learning*. Elle

permettrait également de **ne pas réguler de manière excessive les applications IA présentant peu de risques** pour l'intégrité physique ou les droits fondamentaux des individus par exemple, ce qui est le cas pour la plupart des applications IA.

L'approche cumulative pour déterminer le degré de risque : une approche pragmatique

Pour déterminer le niveau de risque de l'application IA, **les critères pris en considération doivent être clairs et intelligibles**, comme le précisait déjà le Livre Blanc de la Commission européenne, « *les éléments permettant d'établir qu'une application d'IA est à haut risque devraient être clairs, faciles à comprendre et applicables à toutes les parties concernées* ». Ainsi, **l'approche cumulative consistant à prendre en compte le secteur dans lequel l'IA est utilisée, mais aussi l'utilisation qui en est faite au sein de ce même secteur, apparaît raisonnable et pragmatique**. Cette combinaison de critères permettant de déterminer si une application IA est à haut risque ou à faible risque, **permet de ne pas stigmatiser certains secteurs**, qui par nature seraient considérés comme à haut risque, alors que l'utilisation en question faite de l'application comporterait en réalité un faible risque, voire dans certains cas contribuerait à diminuer le risque.

Il semble néanmoins important en pratique que la distinction entre les deux types de risques envisagée par la Commission européenne soit clarifiée pour garantir la sécurité juridique des entreprises, et notamment éviter de placer les petits acteurs économiques dans des situations juridiques complexes.

En effet, les critères peuvent être vus comme encore assez flous, ce qui pourrait laisser craindre que la notion de « risque » soit **interprétée de manière extensive**. Des éléments complémentaires pourraient ainsi être pris en compte lors de l'évaluation du risque (permettant aux entreprises de la réaliser plus facilement), comme le fait d'envisager les dommages potentiels, **mais aussi les opportunités pour la société et les citoyens**, et donc de « mesurer » le coût de ne pas utiliser en pratique l'IA. Une telle **mise en balance** apparaîtrait utile pour ne pas décourager l'utilisation de l'IA dès lors qu'elle présenterait des risques, qui peuvent, dans de nombreux cas, être atténués en pratique. De même, la détermination du niveau de risque pourrait prendre en compte, **au-delà de la gravité potentielle d'un dommage, sa probabilité**. Par ailleurs, **les cas exceptionnels** mentionnés par la Commission européenne dans son Livre Blanc, qui seraient considérés par nature comme à haut-risque, et ce, quel que soit l'évaluation des risques selon les critères cumulatifs réalisée, peut être perçue comme créant un véritable flou dans la détermination du risque et l'application de la réglementation spécifique, et donc comme un **facteur important d'insécurité juridique**.

Il conviendrait également de relativiser les attentes de performance en matière d'IA, car bien que tout puisse être fait pour minimiser les risques et les erreurs, les algorithmes servant au système d'IA peuvent être biaisés ou comporter des erreurs, cela relevant du caractère inhérent de l'algorithme, consistant à fournir des résultats statistiques et des probabilités basés sur des données. La Commission européenne rappelle d'ailleurs que les biais et discriminations ne sont pas propres à la machine et sont inhérents à toute société et activité économique.

Enfin, il semble qu'une nomenclature plus précise de la donnée permettrait également aux entreprises d'apprécier plus finement la notion de risque et d'élaborer des stratégies de normalisation adaptées.

Exigences obligatoires pour les applications d'IA à haut risque

La Commission européenne dans son option 3b) évoque des exigences et obligations légales imposées aux développeurs et aux utilisateurs professionnels de l'IA, qui ne s'appliqueraient que dans les cas d'applications IA considérées comme à haut risque.

Au vu des obligations envisagées dans le Livre Blanc, **il convient d'être vigilant quant à l'élaboration de ces règles et quant à leur interprétation pratique** : il est important que cela soit réalisé avec **pragmatisme et que les exigences soient applicables en pratique par les entreprises, au risque de freiner drastiquement l'innovation.**

Conformité et mise en application

La Commission européenne envisage que les applications d'IA fassent l'objet d'une évaluation de conformité préalable visant à s'assurer que les exigences obligatoires, dans le cas d'application à « haut risque » sont bien respectées. Ce « *prior assessment* » pourrait inclure des procédures de test, d'inspection ou de certification, voire des vérifications des algorithmes et des datasets utilisés dans la phase de développement.

Les entreprises peuvent s'inquiéter de la mise en place d'une telle procédure de conformité *ex ante*. En effet, de nombreuses questions concrètes émergent, auxquelles il sera important d'apporter des précisions. Par exemple, *quid* de l'application rétroactive d'une telle procédure à des produits déjà mis sur le marché ?

Des alternatives efficaces à cette évaluation de conformité préalable, et pouvant être mises en œuvre plus facilement par les entreprises, pourraient être envisagées, sur la base par exemple de ce qui existe dans le cadre du RGPD en matière d'évaluation des impacts sur la protection des données (« *impact assessment* »). De même, **la combinaison d'évaluations par les entreprises des risques *ex ante* et *ex post***, pourrait permettre d'évaluer la conformité aux exigences obligatoires, sans imposer de charges supplémentaires trop lourdes aux entreprises, s'appuyant par exemple sur des pratiques juridiques ou éthiques.

Par ailleurs, **une démarche de certification devrait davantage viser les processus mis en œuvre dans la phase de développement**, comme c'est le cas par exemple dans les industries sensibles, que les produits finis.

En ce qui concerne les évaluations de risques liées à la sécurité des produits, la législation actuelle apparaît suffisamment souple pour prendre en considération la majorité des risques existants liés à l'utilisation de ces technologies émergentes. C'est pourquoi la notion de « risque » liée à l'IA ne doit pas être envisagée sous un angle plus large, ce qui pourrait avoir pour conséquence de **créer des contraintes trop importantes et donc de freiner l'innovation**. Il est à noter que les développeurs de solutions IA font régulièrement des mises à jour de leurs produits. **Une autorégulation en la matière existe donc et mérite d'être soulignée**. Elle est d'ailleurs fondamentale pour les entreprises dont les clients sont de plus en plus exigeants en matière de sécurité, et cette confiance que le client peut accorder dans le produit encourage les bonnes pratiques dans le métier.

Par ailleurs, dans le cadre des réflexions sur la mise en place de nouvelles procédures d'évaluation des risques pour les produits, **la réflexion devrait s'engager selon deux axes, qui sont fonction du type**

d'IA en question. En effet, pour les systèmes d'IA apprenant sur des jeux dits « statiques », le produit final en résultant n'a pas vocation à évoluer davantage après sa mise sur le marché. En revanche, pour les systèmes d'IA qui continuent d'apprendre sur des jeux d'essais, ils peuvent parfois évoluer au point de parvenir à des ruptures si fortes dans le comportement du système que le produit final peut en être modifié. Ainsi, dans le premier cas, il ne serait pas nécessaire de mettre en place de nouvelles procédures d'évaluation des risques, puisque le produit fini n'aura pas vocation à être modifié ou altéré. Mettre en place cette procédure **pourrait même constituer un frein à l'innovation**. Il convient en effet de **relativiser l'évolutivité des algorithmes d'IA dans ce cas puisque les technologies sont stabilisées**.

[A propos de TECH IN France]

Créée en 2005, TECH IN France est une association professionnelle de loi 1901 qui a pour but de rassembler et de représenter les éditeurs de logiciels, de services internet et de plateformes en France. Porte-parole de l'industrie numérique, TECH IN France compte 400 entreprises adhérentes : de la startup à la multinationale en passant par la PME et les grands groupes français ; soit 8 milliards d'euros et 90 000 emplois. TECH IN France s'est donnée pour mission de mener une réflexion permanente sur l'évolution de l'industrie numérique et promouvoir l'attractivité du secteur.

www.techinfrance.fr