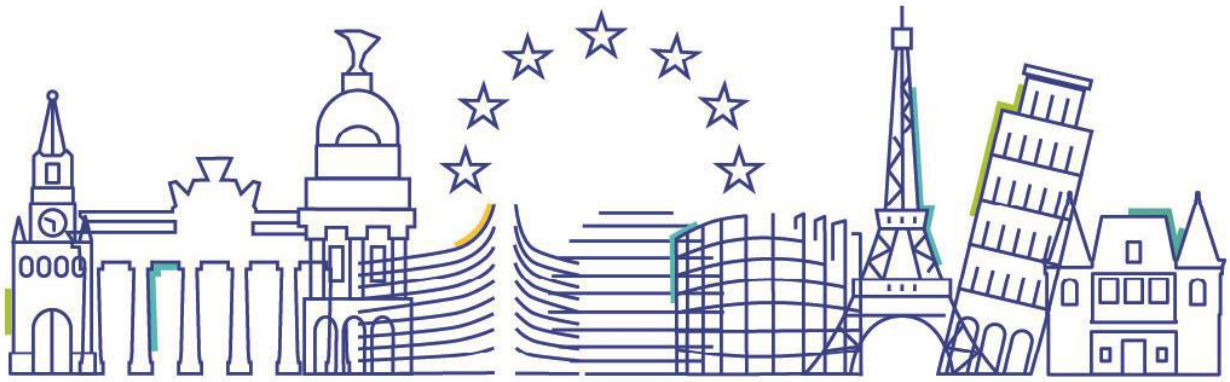
Août 2021



Contribution commune du Groupe La Poste, du Hub France IA et de la Villa Numeris à la consultation de la Commission européenne sur l'Artificial Intelligence (AI) Act

Selon Le Groupe La Poste, le Hub France IA et la Villa Numeris, l'intelligence artificielle (IA) ouvre des possibilités multiples pour l'innovation et la croissance et nous souhaitons saisir tout son potentiel.

Le Groupe La Poste, qui place le numérique et l'IA parmi ses axes prioritaires et stratégiques de développement dans le cadre notamment du plan stratégique de « La Poste 2030, engagée pour vous », **le Hub France IA,** association pour la promotion de l'Intelligence artificielle en France, moteur et fédératrice des initiatives en IA en France et **la Villa Numeris,** association promouvant un modèle européen du digital basé sur l'humain, **ont décidé de mettre en commun leur expertise en vue de s'associer pleinement aux débats européens sur l'IA et l'éthique**.

Nous nous réjouissons par conséquent de pouvoir partager nos positions à l'occasion de la consultation publique de la Commission européenne sur la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle (Artificial Intelligence Act) et modifiant certains actes législatifs de l'Union.

Nous saluons tout d'abord l'ambition et l'initiative de la Commission européenne de positionner **l'Union européenne (UE) comme un leader politique** en matière de technologies et de proposer une **« troisième voie » européenne**. Après avoir influencé le monde en matière de données personnelles avec le RGPD, l'UE cherche en effet aujourd'hui à protéger les

ressortissants européens en s'assurant que **l'intelligence artificielle soit déployée dans le respect de ses valeurs éthiques et de ses droits fondamentaux.**

Nous convenons que l'IA ne répondra à ces attentes que si sa mise en place s'accompagne d'un cadre exigeant qui préserve la confiance des citoyens et s'assure que son utilisation apporte un bénéfice à la société tout entière.

Cependant, nous sommes attentifs à la **compétitivité des entreprises européennes** dans ce domaine absolument clef. Il est important que cette initiative trouve **un juste (et délicat) équilibre entre la promotion de l'innovation et un texte protecteur des droits fondamentaux.**

C'est pourquoi, nous considérons qu'en l'état de la proposition de règlement, cet équilibre n'est pas atteint. Nous identifions **un réel risque pour la compétitivité des entreprises si le texte est publié en l'état**, en particulier pour les raisons suivantes :

- La proposition englobe très largement tout type de solutions IA dont certaines sont déjà largement exploitées et validées ;
- L'approche à haut risque, bien que tout à fait pertinente, considère un périmètre très large de systèmes qui fait porter des exigences sur des systèmes IA dans des secteurs encore peu matures ;
- La mise en conformité est prescriptive pour les systèmes à haut risque et apparaît sur de nombreux points particulièrement complexe et coûteuse à mettre en œuvre ;
- La proposition est floue sur plusieurs points générant de nombreuses incompréhensions à la fois sur le porteur de l'obligation de certification que sur la mise en œuvre des exigences de conformité.

Nous avons **quatre principales pistes de recommandations** :

- La première consiste à ce que l'**AI Act prenne davantage en considération les finalités des systèmes d'IA concernés**. En ignorant ces finalités ou les usages prévus de l'IA, le texte impose des obligations générales disproportionnées à un grand nombre de systèmes ;
- La deuxième consiste à réorienter la proposition pour **privilégier une approche *ex post*** en vérifiant *a posteriori* la conformité des systèmes aux obligations décrites dans la proposition de règlement ;
- La troisième consiste à ce que le texte soit moins prescriptif en fonction du niveau de risque considéré. Il convient, par exemple, de s'appuyer sur les bonnes pratiques déjà mises en place par l'industrie ;

  La quatrième consiste à **affiner les définitions du texte**, en particulier celle de l'IA. Il convient que le texte conserve un périmètre proportionné aux objectifs poursuivis.

Nous détaillons ci-dessous nos interrogations, commentaires et recommandations sur l'ensemble du texte.

1. Un texte qui devrait plus insister sur les bonnes pratiques à mettre en place dans le respect des droits fondamentaux et en vue de promouvoir l'innovation et la compétitivité des entreprises

Nous saluons l'ambition de réguler l'intelligence artificielle pour proposer une IA digne de confiance et respectueuse des droits fondamentaux. Cependant, le texte reste très centré sur la sécurité et les garanties apportées par les entreprises pour disposer d'une IA de confiance. **Mais il est important de s'assurer également que ces garanties ne nuisent pas à la compétitivité**

des entreprises européennes et ne constituent pas des freins à l'innovation en Europe : **l'impact de chaque garantie devrait donc être évaluée et proportionnée**.

L'objectif principal, pour la Commission, est donc de développer une intelligence artificielle **digne de confiance**, reposant sur une **technologie éthique** préservant la compétitivité et aidant à la consolidation d'une IA souveraine au sein de l'Union européenne.

- ***Nous soutenons l'ambition de cette régulation des IA fondée sur une approche des risques, néanmoins nous souhaitons souligner que cela ne doit pas se faire au détriment de l'innovation et du business de notre écosystème européen par rapport à la concurrence mondiale. En effet, certains points du règlement, en l'état de leur formulation, laissent craindre des contraintes de mises en œuvre pouvant asphyxier certaines structures, en particulier les startups, mais pas seulement, dans leur démarche d'innovation.***

- ***Nous craignons en effet que le texte, dans son état actuel, renforce les acteurs étrangers qui ne seront pas soumis à cette réglementation.***

- ***Même si ce texte est louable à bien des égards, nous nous inquiétons de sa mise en pratique qui semble complexe, en particulier pour les plus petites structures, en l'état actuel des aspects techniques. C'est pourquoi, nous suggérons d'insister sur les bonnes pratiques à mettre en place dans le respect des droits fondamentaux et en vue de ne pas entraver l'innovation. En effet, il est nécessaire de mieux comprendre et utiliser l'IA notamment :***
  - ***en favorisant une culture de la donnée par de vastes programmes de sensibilisation et de formation ;***
  - ***en promouvant des modèles d'anonymisation profonde permettant de lutter contre les discriminations.***

2. Un texte qui reste encore imprécis sur des concepts fondamentaux

a) Une définition de l'IA trop large et pouvant entraîner de lourdes difficultés de mise en place pour les entreprises

L'AI Act a vocation à s'appliquer à certains « *systèmes d'intelligence artificielle* », expression qui a été préférée à celle d' « *intelligence artificielle* », laquelle renvoie plus à une discipline, une science, qu'à des usages. La technologie est non seulement plurielle, mais elle a vocation à s'appliquer à des domaines et pour des usages très variés.

Le système visé est défini, à l'article 3.1, comme : « *un logiciel développé à l'aide d'une ou plusieurs des techniques et approches énumérées à l'annexe I de la proposition et capable, pour un ensemble donné d'objectifs définis par l'homme, de générer des résultats tels que des contenus, des prédictions, des recommandations ou des décisions influençant les environnements avec lesquels ils interagissent* ».

Malgré une volonté déclarée par la Commission de neutralité technologique et d'adaptation à l'évolution technologique, que nous comprenons, **la définition retenue de l'IA est très large et peut être amenée à évoluer, ce qui pourrait poser des difficultés d'application dans l'approche par les risques**. L'annexe I énumère par ailleurs trois catégories de techniques algorithmiques, en substance les systèmes (auto-)apprenants, les systèmes logiques et les systèmes statistiques. Cette annexe a vocation à être modifiée et, par conséquent, on peut noter

que **cette définition est amenée à évoluer notamment par des actes délégués ce qui est source d'insécurité juridique**.

- ***Nous considérons qu'avec une définition aussi large de l'IA, il apparaît que de nombreuses applications logicielles risquent d'être incluses dans le périmètre du texte, ce qui pourrait induire des coûts « rétroactifs » pour mettre en conformité des systèmes déjà en production et nuire à l'innovation pour la conception de nouveaux systèmes. Or, dans un contexte de compétitivité internationale, il est essentiel d'encourager le développement technologique.***

- ***Nous recommandons que la définition de l'IA se limite au point a) relatif à l'apprentissage automatique. En effet, si l'idée de cette proposition de règlement vise à faire réguler de nouvelles technologies fondées sur les données et à l'apprentissage automatique, il ne convient pas d'encadrer des solutions déjà éprouvées (les approches symboliques ou les statistiques par exemple qui sont déjà industrialisées) qui ne présentent pas les mêmes défis des systèmes d'IA à apprentissage automatique.***

b) Un périmètre à préciser

La précision des termes est souvent insuffisante. A titre d'exemple : « *natural person* » ou « *personne physique* » : ce terme peut poser des difficultés pratiques, par exemple dans le secteur bancaire, quand une TPE, ne comprenant qu'une seule personne (le créateur) demande un crédit, la distinction entre personne physique et personne morale est ténue.

- ***Nous recommandons que ces termes soient définis avec beaucoup plus de précisions car la rédaction actuelle autorise de multiples interprétations, ce qui constitue un risque juridique.***

3. Un texte qui soulève des commentaires sur l'approche fondée sur l'évaluation du risque et l'alignement d'obligations proportionnées associées

La Commission a privilégié une option déjà pressentie par ses précédents écrits : une approche par graduation des risques.

La démarche de la Commission européenne est la suivante :
- Une pré-qualification des risques inhérents à l'utilisation et au déploiement de l'intelligence artificielle ;
- Un alignement, en miroir de cette pré-qualification, d'obligations graduées et proportionnées.

- ***De manière générale, nous accueillons favorablement une approche par les risques qui met sur un pied d'égalité les entreprises qui opèrent des activités similaires. Il est important d'instaurer un traitement équitable en fonction du risque qu'une activité donnée suscite, afin d'assurer des garanties similaires indépendamment du fait de savoir qui gère cette activité.***

Tous les systèmes d'IA ne sont donc pas concernés par l'encadrement envisagé au regard de la variabilité des obligations en lien avec le niveau de risque. En outre, les usages visés sont les usages professionnels. En effet, l'utilisateur d'un système d'IA à des fins personnelles et non-professionnelles est exclu du champ d'application du texte (voire la définition d'un « utilisateur » à l'article 3. 4).

On peut noter que les fournisseurs, importateurs et les utilisateurs des systèmes d'IA à « risque élevé » sont également directement soumis à une série d'obligations (Articles 16 à 29) et peuvent faire l'objet d'un contrôle par une autorité nationale (articles 30 à 39).

Enfin, il nous semble aussi important de considérer le cas de modèles créés dans le cadre de systèmes qui ne sont pas à haut risque mais qui pourraient être détournés de leurs finalités pour rentrer dans ce cadre.

- ***Concernant les usages visés, la proposition de règlement devrait se limiter explicitement aux usages concernant les personnes physiques.***

a) Sur les systèmes à haut risque (Titre III – Article 6 à 51)

- *Sur la définition des systèmes IA à haut risque (article 6)*

Nous sommes convaincus que les applications IA considérées comme à haut risque doivent répondre à des critères définis s'il existe des menaces avérées pour la santé, la vie ou les droits fondamentaux.

La définition très large des systèmes IA à haut risque prévue au titre III 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 en Europe.

Par ailleurs, il est à noter que les dispositions de l'article 7 prévoient une évolution de l'Annexe III établissant une liste de systèmes IA considérés à haut risque par l'adoption d'actes délégués.

- ***Nous sommes conscients des évolutions rapides en matière d'IA et donc des définitions concernées toutefois, le recours aux actes délégués ne semble pas assurer la sécurité juridique nécessaire.***

- ***Nous estimons que cette définition demeure trop large ce qui pourra faire peser d'importantes obligations. Nous recommandons de mettre en place une balance bénéfice/risque des évolutions technologiques 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, notamment liées aux obligations de mises en conformité (cf. § Sur l'obligation de mener des analyses de risque et de conformité (articles 9, 19 et 43).***

- ***Il pourrait être pertinent de déterminer plusieurs niveaux de système à haut risque et n'imposer des dispositions strictes pour le plus haut niveau.***

- *Sur l'obligation d'utiliser des ensembles de données sans erreur (article 10)*

Afin d'utiliser l'IA de façon éthique, il faut la maîtriser et qu'elle soit d'un haut niveau de qualité.

Concernant les obligations, l'article 10 impose en particulier une obligation d'utiliser des **ensembles de données sans erreur, ce qui est n'est absolument pas réalisable en pratique.**

- ***Il serait préférable de retirer cette obligation. Le concept de zéro erreur dans les données est contraire avec la notion d'IA qui intègre conceptuellement cette capacité de reproduire une analyse humaine.***

- ***De la même manière, si la constitution de jeux de données sans biais est souvent considérée comme un enjeu important de l'IA, ils restent inévitables. Il est important de mettre en place des procédures pour les mesurer. Les fournisseurs d'IA devront fournir leur meilleur effort pour se prémunir des discriminations pouvant résulter de l'existence de biais.***

Par ailleurs, le texte ne semble pas assez prendre en compte les données nécessaires (plus particulièrement leur qualité) à l'IA.

- *Sur l'obligation de mener des analyses de risque et de conformité (articles 9, 19 et 43)*

Il est fait référence aux articles 9, 19 et 43 à l'obligation, pour les opérateurs de mener des analyses de risque et de conformité à l'ensemble des législations applicables. Or, du fait des similitudes que ce texte 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.

- ***Nous nous demandons 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 ? Par ailleurs, ces analyses nécessitent d'importants moyens techniques et financiers pour chaque entreprise en vue de répondre à ces mesures de façon optimale. Les entreprises devront faire face à des coûts supplémentaires qui pourraient avoir un impact négatif sur l'innovation.***

- ***En pratique, l'exigence que la conformité soit vérifiée dès qu'une mise à jour est réalisée demeure très coûteuse, impossible en temps réel voire peu pertinente s'agissant de certaines mises à jour. Les exigences de traçabilité sur toute la durée de vie du système ne sont pas tenables en matière de coûts et capacités de stockage, et même incompatibles avec d'autres réglementations comme le RGPD.***

- ***Nous craignons qu'in fine cette obligation ait des effets de bord négatifs et découragent les fournisseurs de mettre à jour leurs modèles pour qu'ils restent efficaces dans le temps compte tenu des démarches de remise en conformité nécessaire à ces mises à jour.***

- *Sur les « logs » (ou « journaux ») générés automatiquement (article 12)*

Selon l'article 12, les fournisseurs d'IA à haut risque devront conserver les « logs » (ou « journaux ») générés automatiquement.

- ***Cette obligation nous semble contraignante compte tenu de la volumétrie importante des logs qui seraient à conserver : conserver les logs de toutes les expérimentations ayant conduit au système final serait beaucoup trop coûteux. Il suffit, selon nous, de conserver les logs de l'expérimentation (avec les jeux de données correspondants) qui a produit le système final.***

- *Sur le « contrôle humain » (article 14)*

L'article 14 prévoit « **un contrôle et une surveillance de l'IA humains** ».

- ***Il convient de noter que toute conception d'un algorithme ne peut se faire sans intervention humaine. La supervision du système d'IA nous paraît également importante pour détecter les dérives par rapport à l'usage initialement prévu de l'IA.***

- *Sur les composants IA (article 26)*

Il est fait référence aux composants IA dans la définition des systèmes IA à haut risque. Les responsabilités de chaque opérateur doivent correctement s'articuler.

- ***Sous l'angle de la responsabilité et de la conformité, comment traiter des briques d'IA proposées par des fournisseurs, mais assemblées par l'utilisateur ? Aux termes de l'article 26, l'importateur de ces composants devra-t-il de la même manière s'assurer que les analyses de conformité ont été effectuées par le fournisseur ? Nous comprenons et soutenons qu'il est nécessaire de disposer d'une chaîne de confiance en la matière mais il sera impossible de procéder à une évaluation complète de ce champ.***

- ***Nous nous interrogeons en effet, sur la responsabilité de chaque acteur notamment dans le cas de figure où l'application élaborée par un fournisseur devrait être modifiée par l'utilisateur. Quelle sera également la responsabilité engagée dans le cadre d'une relation entre un fournisseur de brique technologique et un producteur de solution ?***

b) Sur le « marquage CE de conformité » (marquage CE) (articles 3.24 et 49)

Le « marquage CE de conformité » (marquage CE), un marquage par lequel un fournisseur indique qu'un système d'IA est conforme aux exigences énoncées au titre III, chapitre 2, de la proposition de règlement et à d'autres textes législatifs applicables de l'Union harmonisant les conditions de commercialisation des produits prévoyant son apposition.

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

- ***Concernant la certification, nous pouvons nous interroger sur l'articulation de ces nouvelles exigences en matière de certification avec les instances de normalisation déjà en place (normes ISO, marquage CE, directive Machines, etc.).***

- ***De la même façon, les systèmes IA déjà en exploitation devront-ils être certifiés a posteriori ? Si oui selon quelles modalités ? En effet, la mise en conformité se faisant avant la mise sur le marché, qu'adviendra-t-il des solutions déjà éprouvées, qui même à haut risque n'aurait jamais posé de problème particulier depuis leur mise sur le marché ? Les coûts n'ayant pas été anticipés, ainsi que les contraintes et exigences de réglementation, il semble complexe d'appliquer ces exigences de façon rétroactive.***

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.

- ***Quelle autorité sera chargée d'évaluer la conformité en la matière ?***

4. Une réglementation par l'expérimentation

L'Artificial Intelligence Act encourage les autorités nationales compétentes à mettre en place des « Sandboxes » (bacs à sable) réglementaires de l'IA afin de tester des technologies innovantes pendant une durée limitée, sur la base d'un plan d'essai convenu avec les autorités compétentes (Articles 53, 54 et 55).

Cette approche est nécessaire afin d'éviter de brider l'innovation par une réglementation inadaptée. Il semble toutefois nécessaire de conserver une approche pragmatique au cours de la construction de l'encadrement juridique de l'IA, pour ne pas faire peser trop de contraintes sur les initiatives technologiques européennes.

- ***Ce droit à l'expérimentation apparaît un outil intéressant pour appréhender un domaine d'innovation forte telle que l'IA. Toutefois nous souhaiterions obtenir des précisions concernant :***
  - ***les critères d'éligibilité à respecter pour les entreprises qui veulent avoir recours à ces sandboxes. En particulier, comment les « jeunes entreprises » seront identifiées (article 55) ?***
  - ***les données utilisées dans ces bacs à sable.***

- ***Pour une efficacité renforcée, ces sandboxes devraient impliquer les régulateurs de bout en bout.***

- ***Par ailleurs, nous recommandons, en parallèle des sandboxes, de permettre aux entreprises de bénéficier d'un cadre réglementaire assoupli pendant les phases de pré-production ou pilotes de leurs projets. Les deux mécanismes pourraient coexister pour permettre aux plus petites structures d'innover dans un contexte plus flexible.***

5. L'autorité nationale compétente sur l'IA (article 59) et le risque de gouvernance européenne éclatée

L'article 59 prévoit la désignation d'une autorité nationale compétente sur l'IA pour vérifier et mettre en place des procédures pour les analyses, la désignation et la notification des organismes d'évaluation de conformité.

Cette nouvelle réglementation s'accompagne d'une gouvernance européenne de l'IA, dont la politique sera dirigée par un Conseil Européen de l'Intelligence Artificielle, composé de représentants des États membres et de la Commission. Ce conseil assurera la coopération des autorités nationales de contrôle et coordonnera l'analyse de la Commission par le partage d'expertise, des recommandations ou des avis Articles 56 à 59). Toutefois, malgré la création de ce Conseil, **la notion de gouvernance semble encore assez floue. Un cadre d'application aussi complexe avec de nombreuses autorités différentes pourrait engendrer un chevauchement des compétences entre les autorités.**

- ***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.***

- ***Il est essentiel que les décisions et doctrines des autorités de contrôle nationales soient harmonisées afin d'éviter les risques de fragmentations dans l'application du texte. Il existe en effet un risque de non-alignement, de différences d'interprétation, qui, de facto entraîneront l'émergence de services qui ne seront pas « égaux » entre services développés dans certains Etats membres.***

- ***Notamment pour des questions de secret bancaire, nous souhaitons demander que pour les banques et assureurs les autorités compétentes en matière de supervision bancaire et assurantielle (BCE, EBA, ACPR) soient nommément désignées***.

6. La surveillance du marché des systèmes IA à haut risque (Titre VIII – article 64)

L'article 64 prévoit la possibilité pour les autorités de surveillance du marché **d'exiger l'accès aux données, à la documentation et au code source des systèmes IA pour le contrôle de conformité des IA à haut risque.**

Nous nous demandons comment l'accès au code source doit être donné. Il semble difficile de donner accès à un code source à distance 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 paraissent disproportionnées par rapport à l'utilité de cette démarche.

- ***L'accès au code source à distance nous semble difficile à mettre en place et entraver la sécurité du système, en particulier si ce système est à haut risque.***

- ***Aussi, l'accès aux données et à la documentation n'est pas réalisable sous forme d'API comme précisé dans l'article 64.1 pour les mêmes raisons de sécurité.***

7. Des sanctions particulièrement lourdes (Articles 71 à 72)

La Commission s'inspire encore du RGPD étant largement fondé sur le risque encouru en cas de non-respect, en proposant des sanctions particulièrement lourdes en cas de non-respect des règles édictées (Articles 71 à 72).

Les sanctions mises en place par le RGPD sont déjà assez importantes, cumulées avec celles-ci, il est probable que **les entreprises ne prennent pas le risque d'innover** surtout au regard d'obligations qui ne pourraient être respectées en l'état (cf code source, données exemptes d'erreur, etc).

- ***Il serait préférable de réduire ces sanctions et de mettre en place une autorité de conseil en IA en vue d'aider les entreprises à mettre en place leurs projets (boîtes à outils, analyse des projets, etc.).***

8. La responsabilité et l'IA

Nous nous demandons quelles seront au total les dispositions qui seront prévues par la proposition qui devrait être élaborée en fin d'année par la Commission européenne et comment elle s'articulera avec cette proposition de règlement.

***

Août 2021

Nous contacter

Pour le Groupe La Poste :

- **Christelle DEFAYE-GENESTE**, Directrice des Affaires Européennes et Douanières, Représentation de La Poste à Bruxelles

  Tel : +33 (0)6 71 70 37 32 ou +32 (0)2 231 56 27 – christelle.geneste@laposte.fr
- **Gaëlle KULIG**, Responsable des Affaires Européennes Numériques

  Tel : +33 (0)6 22 69 98 82 – gaelle.kulig@laposte.fr

Pour le Hub France IA :

- **Françoise SOULIE**, Conseiller Scientifique

  francoise.soulie@hub-franceia.fr
- **Caroline CHOPINAUD**, Directrice Associée

  Tel : + 33 (0)6 07 51 74 80 – caroline.chopinaud@hub-franceia.fr

Pour la Villa Numeris :

- **David LACOMBLED**, Président

  david@lacombled.com