



Consultation sur le Livre blanc sur l'intelligence artificielle

Une approche européenne

Contribution du
Comité National Pilote d'Éthique du Numérique (CNPEN, France)

Introduction

Le Comité national pilote d'éthique du numérique (CNPEN) a été mis en place en décembre 2019 sous l'égide du Comité consultatif national d'éthique (CCNE) à la demande du Premier ministre de la République Française. Il est constitué de 27 personnes d'horizons différents, issues du monde académique et politique, des entreprises ou de la société civile, pour aborder de manière globale les enjeux éthiques du numérique et donc de l'IA en particulier. Son rôle est à la fois d'élaborer des avis sur les saisines qui lui sont adressées et d'effectuer un travail de veille pour éclairer les prises de décision individuelles et collectives.

Les trois saisines initiales du gouvernement portent sur les agents conversationnels, le véhicule autonome, et le diagnostic médical à l'ère de l'intelligence artificielle. Mais la crise sanitaire de la Covid-19 a entraîné une réflexion, des communiqués et des avis sur les usages massifs du numérique dans un contexte de confinement et sur l'utilisation du numérique dans une stratégie de déconfinement.

Le CNPEN souhaite collaborer étroitement avec d'autres comités éthiques de pays européens pour contribuer à une approche européenne des enjeux éthiques du numérique. Il est donc particulièrement soucieux que l'approche proposée par Le Livre Blanc soit conforme à des valeurs partagées mais aussi à des conditions de vies partagées par le plus grand nombre.

La réponse du CNPEN à cette consultation porte sur les enjeux éthiques de l'IA comprise comme la partie des sciences et technologies du numérique intégrant tout particulièrement l'apprentissage machine (cf. la caractérisation proposée dans le livre blanc).

Section 1 – Un écosystème d'excellence

Afin de construire un écosystème d'excellence capable de soutenir le développement et de favoriser l'adoption de l'IA dans tous les secteurs économiques de l'UE, le Livre blanc propose une série d'actions.

Selon vous, quelle est l'importance des six actions proposées à la section 4 du Livre blanc sur l'IA (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 -Très important	Sans avis
Coopération avec les États membres	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Cibler les efforts de la communauté de la recherche et de l'innovation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Compétences	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Accorder une place de choix aux PME	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Partenariat avec le secteur privé	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Encourager le secteur public à adopter l'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

- A. **Coopération avec les Etats Membres (5)** : Le CNPEN comprend de nombreuses personnes appartenant à la communauté de la recherche et de l'innovation dans le domaine de l'IA en particulier. Elles proviennent principalement d'universités et d'institutions du secteur public mais sont souvent engagées dans des partenariats avec le secteur privé aux niveaux français, européen et international. De ce point de vue le CNPEN considère qu'il est très important de cibler les efforts de la communauté de la recherche et de l'innovation dans le cadre d'une coopération privilégiée entre États membres de l'UE.
- B. **Cibler les efforts (5)** : Voir la réponse précédente.
- C. **Compétences (5)** : La question du développement des compétences en IA est importante. Même si les États membres ont déjà des compétences académiques et des formations de qualité et reconnues internationalement il faut renforcer les compétences académiques et les centres interdisciplinaires pour mieux gérer les applications en IA
- D. **Accorder une place de choix aux PME (5)** : Il est aussi crucial d'accorder une place de choix aux PME pour les aider à maîtriser et adopter les outils de l'IA dans leurs domaines d'activités tout en veillant à ce que l'accès au financement via Invest EU prenne en compte des critères d'usage de l'IA en conformité avec les enjeux éthiques et sociétaux dans le cadre de la transition écologique et solidaire pour l'UE.
- E. **Partenariat avec le secteur privé (5)** : Concernant le partenariat avec le secteur privé, le CNPEN est attentif aux enjeux de souveraineté nationale et européenne (voir aussi le rapport¹ de la CERN) et au risque d'érosion du patrimoine que constituent les données publiques si elles sont accessibles au secteur privé sans garanties suffisantes contre

¹ https://www.allistene.fr/files/2018/10/55708_AvisSouverainete-CERNA-2018.pdf

d'éventuels usages détournés. On pense en particulier aux données de santé, mais cela peut concerner d'autres corpus de données par exemple sur la mobilité des personnes et des biens, l'habitat et plus généralement toutes les ressources vitales. Il est donc indispensable d'assortir ces partenariats public-privé de règles de transparence, de contrôle et de réversibilité, voire de réciprocité d'accès à d'autres données.

- F. **Encourager le secteur public à adopter l'IA (5)** : Enfin le CNPEN considère qu'il est effectivement souhaitable d'encourager le secteur public à adopter l'IA. Il existe plusieurs avantages à cette adoption : tout d'abord, l'acquisition de compétences en IA par l'administration, puis l'acculturation de nos concitoyens grâce à la multiplication des interactions avec l'IA. Enfin, l'adoption de la technologie par l'administration stimulera l'innovation et la commande publique en matière d'IA, qui dynamisera potentiellement le secteur des start-ups. Cependant, l'IA devra être un outil d'amélioration du service et non un remplacement des personnes qui le fournissent, et l'interaction humaine devrait rester la norme en particulier pour les usagers qui en auraient besoin dont les personnes isolées ou vulnérables ou ayant des difficultés d'accès aux interfaces numériques ou de maîtrise des outils numériques.

D'autres actions devraient-elles être envisagées?

Le CNPEN considère que l'Europe a un rôle particulier à jouer dans la coopération internationale externe à l'Union Européenne, en particulier avec les pays ACP (Afrique-Caraïbes-Pacifique), pour le développement d'une IA de confiance et conforme aux valeurs éthiques partagées par les États membres et mentionnées dans le Livre Blanc (section 4 – H aspects internationaux). Pour mieux peser dans les négociations dans les grandes institutions internationales (ONU, G7, G20, OCDE, UNESCO, OMC, UIT etc.) il faudrait que les États membres de l'UE y parlent d'une même voix en se coordonnant au préalable.

Une révision du plan coordonné dans le domaine de l'IA (action 1)

En tenant compte des résultats de la consultation publique sur le Livre blanc, la Commission proposera aux États membres une révision du plan coordonné en vue d'une adoption d'ici à la fin 2020

Selon vous, dans quelle mesure est-il important, dans chacun de ces domaines, d'aligner les politiques et de renforcer la coordination, comme décrit à la section 4.A du Livre blanc (de 1 à 5: 1 n'est pas important du tout, 5 est très important) ?

	1 - Pas important du tout	2 – Pas important	3 – Neutre	4 - Important	5 – Très important	Sans avis
Renforcer l'excellence dans la recherche	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Établir des centres d'essai constituant une référence mondiale pour l'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Encourager le secteur public à adopter l'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Accroître le financement des start-ups innovantes dans le domaine de l'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Développer les compétences en matière d'IA et adapter les programmes de formation existants	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Construire l'espace européen des données	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	----------------------------------	-----------------------

En cohérence avec ses réponses aux questions précédentes, le CNPEN considère qu'il est très important de renforcer l'excellence dans la recherche, d'établir des centres d'essai constituant une référence mondiale pour l'IA, d'encourager le secteur public à adopter l'IA et d'accroître le financement des start-ups innovantes dans le domaine de l'IA,

De même le développement des compétences en matière d'IA et l'adaptation des programmes de formation IA sont jugés très important non seulement pour renforcer les compétences académiques, mais aussi pour favoriser l'adoption de l'IA à bon escient par les entreprises, en particulier les PME, et par le secteur public, et surtout pour permettre l'acculturation des populations ayant des difficultés de maîtrise des outils numériques.

Quant à encourager le secteur public à adopter l'IA, le CNPEN émet la même réserve que précédemment, c'est-à-dire que cette adoption soit justifiée et maintienne une relation humaine entre l'administration et les citoyens, en particulier les personnes isolées ou vulnérables et ayant des difficultés d'accès aux interfaces numériques ou de maîtrise des outils numériques.

Enfin la construction d'un espace européen des données est très importante pour i) éviter la fragmentation des systèmes nationaux, ii) élaborer un standard européen pour le format des données, facteur d'interopérabilité et de rayonnement international, et iii) présenter un front commun plus fort dans la capacité de négociation de l'UE avec de grands acteurs privés extra-européens. Cet espace européen des données devra être soumis au contrôle démocratique du Parlement Européen, au contrôle des organes de supervision et aux avis consultatifs d'autres instances européennes telles que le Comité Economique et Social Européen (CESE).

D'autres domaines devraient-ils être envisagés?

Le CNPEN souhaiterait que les pays membres de l'UE se dotent de comités consultatifs nationaux d'éthique du numérique et de l'IA et que ceux-ci se coordonnent au sein d'un comité consultatif européen.

Une communauté de la recherche et de l'innovation unie et renforcée qui vise l'excellence

Il sera essentiel d'unir les forces à tous les niveaux, de la recherche fondamentale jusqu'au déploiement, afin de surmonter la fragmentation et de créer des synergies entre les réseaux d'excellence existants.

Selon vous, quelle est l'importance des trois actions proposées dans les sections 4.B, 4.C et 4.E du Livre blanc sur l'IA (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
Soutenir l'établissement d'un centre «phare» pour la recherche, qui soit de calibre mondial et capable d'attirer les cerveaux les plus brillants	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Créer un réseau des centres d'excellence existants dans le domaine de la recherche en IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Mettre en place un partenariat public-privé pour la recherche industrielle	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
--	-----------------------	-----------------------	-----------------------	-----------------------	----------------------------------	-----------------------

- A. **Soutenir l'établissement d'un centre «phare» (3)** : Le CNPEN est réservé sur la création d'un seul « centre phare » européen sur l'IA qui devrait coordonner les divers centres de compétence actuels. Plusieurs instituts de recherche européens en IA ont déjà une masse critique et pourraient constituer autant de « centres phares » interdisciplinaires européens de calibre mondial sur l'IA.
- B. **Créer un réseau des centres d'excellence (5)** : En revanche il paraît très important, plus opérationnel et efficace de créer un réseau des centres d'excellence existants dans le domaine de la recherche en IA.
- C. **Mettre en place un partenariat public-privé (5)** : La mise en place d'un partenariat public-privé pour la recherche industrielle est jugée importante pourvu que les relations établies avec les grands groupes privés internationaux soient suivies et auditées pour s'assurer que la recherche industrielle menée en Europe soit bien au service d'une souveraineté européenne.

D'autres actions visant à renforcer la communauté de la recherche et de l'innovation devraient-elles se voir accorder une priorité?

Le CNPEN encourage les programmes de recherche collaborative, multidisciplinaires et à long terme, et pas uniquement les projets individuels ou des projets ciblés à court terme.

Une attention particulière pour les petites et moyennes entreprise (PME)

La Commission collaborera avec les États membres pour faire en sorte qu'au moins un pôle d'innovation numérique par État membre ait un niveau élevé de spécialisation en IA.

Selon vous, quelle est l'importance de chacune de ces missions des pôles d'innovation numérique spécialisés mentionnés à la section 4.D du Livre blanc en ce qui concerne les PME (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
Contribuer à sensibiliser les PME aux avantages potentiels de l'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Donner accès aux centres d'essai et de référence	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Promouvoir le transfert de connaissances et soutenir le développement de l'expertise en matière d'IA pour les PME	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Soutenir des partenariats entre les PME, les grandes entreprises et les universités autour de projets d'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Fournir des informations sur le financement en fonds propres pour les start-ups dans le domaine de l'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>	<input type="radio"/>

Le CNPEN souligne l'importance de sensibiliser les PME non seulement aux avantages potentiels de l'IA, mais aussi aux risques liés à l'IA, aux aspects éthiques et juridiques de la conception et de l'usage des outils numériques et des algorithmes d'IA et à leurs impacts sociétaux. L'IA n'est pas toujours la solution la plus appropriée. Ceci implique en particulier de développer et proposer des formations spécifiques.

Une expertise interne aux PME en matière d'IA étant difficile à entretenir et capitaliser le CNPEN considère que l'accès direct des PME aux centres d'essai et de référence leur permettrait d'une part d'expérimenter et d'autre part d'interagir avec les innovations élaborées par d'autres.

Les partenariats entre PME, grandes entreprises et universités autour de projets d'IA sont fondamentaux pour le transfert de connaissances et le développement d'expertises et de conseils en matière d'IA qui puissent être mis à disposition des PME.

Section 2 – Un écosystème de confiance

Le chapitre 5 du Livre blanc définit des options en vue d'un cadre réglementaire pour l'IA.

Selon vous, quelle est l'importance des préoccupations suivantes concernant l'IA (de 1 à 5 : 1 n'est pas important du tout, 5 est très important)

	1 - Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
L'IA peut compromettre la sécurité	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
L'IA peut porter atteinte aux droits fondamentaux (comme la dignité humaine, le respect de la vie privée, la protection des données, la liberté d'expression, les droits des travailleurs, etc.)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
L'utilisation de l'IA peut entraîner des résultats discriminatoires	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
L'IA peut prendre des mesures dont les motifs ne peuvent pas être expliqués	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>

Il peut être plus difficile pour les personnes ayant subi un préjudice du fait de l'utilisation de l'IA d'obtenir réparation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
L'IA n'est pas toujours exacte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>

- A. **L'IA peut compromettre la sécurité (5) :** La relation entre l'IA et la sécurité est ambivalente.

D'un côté les technologies de l'IA peuvent présenter de nouveaux risques pour la sécurité. Au-delà des exemples bien connus (par ex. un accident lié au dysfonctionnement d'un véhicule autonome) on peut citer aussi le risque que l'IA puisse être utilisée par des pirates pour compromettre la sécurité en repérant, à partir de données, les habitudes des usagers, par exemple les mots de passe qu'ils ont l'habitude d'utiliser, etc. L'IA peut aussi être utilisée pour passer au crible des défenses informatiques et trouver des failles. Une IA digne de confiance nécessite des systèmes et algorithmes suffisamment sûrs, fiables et robustes pour répondre à des exigences de cybersécurité élevées en résistant aux attaques directes et aux tentatives plus subtiles de manipulation des données ou des algorithmes proprement dits. Ils doivent être fondés sur des mécanismes de « safety by design » et adopter les précautions nécessaires contre les risques de mésusages.

De l'autre côté, et de façon plus positive, l'IA peut contribuer à renforcer la sécurité dans un certain nombre de domaines. À titre d'exemple des systèmes d'identité numérique, à condition qu'ils soient fiables et déployés sans biais liés au genre, au handicap, aux caractéristiques physiques ou l'origine ethnique, pourraient grandement améliorer la sécurité d'authentification, de connexion et de transactions. Par ailleurs, l'IA permet d'analyser tous les événements et de distinguer, parmi ceux-ci, les tentatives pour faire une brèche dans la sécurité des systèmes.

- B. **L'IA peut porter atteinte aux droits fondamentaux (5) :** La mauvaise utilisation de l'IA pourrait porter atteinte à plusieurs droits fondamentaux. Le déploiement de certains systèmes de « reconnaissance émotionnelle », sans bases scientifiques solides et à des fins diverses, ou la mise en place de systèmes de surveillance sophistiqués fondés sur des techniques de reconnaissance faciale, illustrent certains risques pour les droits fondamentaux. Le scandale de Cambridge Analytica a par ailleurs montré qu'une mauvaise utilisation des données et de l'IA pourrait déstabiliser les socles démocratiques de nos sociétés européennes et servir à des opérations d'influence. Le CNPEN considère que l'Europe doit prêter la plus grande attention à ces risques.
- C. **L'utilisation de l'IA peut entraîner des résultats discriminatoires (5) :** Il s'agit ici d'une prolongation du point précédent. Les données utilisées par les systèmes d'IA peuvent être biaisées par des partis pris ou par des bases de données incomplètes ou reflétant des discriminations ou des biais humains. Les biais peuvent être présents à tous les stades de la conception et du déploiement (dont l'usage) des systèmes algorithmiques. De manière similaire, la manière dont les systèmes d'IA et les algorithmes sont construits peut également être entachée de biais ou aboutir à des inégalités de traitement, voire les systématiser ou les amplifier. Les systèmes de l'IA doivent être fondés sur le respect de la dignité humaine et de l'égalité de traitement, sans discrimination aucune, tout en prêtant une attention particulière à la sous-représentation de certaines catégories de population (femmes, certains groupes sociaux...) et à la situation des personnes vulnérables ainsi qu'aux questions d'accessibilité. En même temps, et de façon plus optimiste, le CNPEN considère que l'utilisation de l'IA peut aussi contribuer à éliminer les biais humains et à améliorer la situation des personnes handicapées, vulnérables ou à autonomie réduite.
- D. **L'IA peut prendre des mesures dont les motifs ne peuvent pas être expliqués (5) :** L'explicabilité est essentielle, surtout quand l'utilisation de l'IA aboutit à des décisions affectant des personnes et leurs droits. Elle est indispensable, par exemple, pour justifier les décisions

calculées dans les systèmes critiques, les systèmes d'affectation dans l'enseignement, l'aide au recrutement, la justice, etc. L'explicabilité contribuera à construire la confiance des citoyens à l'égard de ces technologies. Actuellement, un champ de recherche émerge afin d'améliorer l'explicabilité et la transparence des systèmes d'apprentissage ainsi que leur adaptation en contexte et l'adéquation de l'apprentissage à ce qu'en attend l'humain. Ainsi, il ne s'agit plus seulement de construire des modèles par apprentissage machine sans comprendre mais bien d'essayer de les expliquer. Voir l'avis de la CERNA, publiée en juin 2017, sur l'Ethique de la recherche en apprentissage machine².

- E. ***Il peut être plus difficile pour les personnes ayant subi un préjudice du fait de l'utilisation de l'IA d'obtenir réparation (5)*** : Il s'agit d'une préoccupation importante qui appelle en effet un certain nombre de points d'attention s'agissant de la réparation non seulement du préjudice subi à titre *individuel* mais également de la réparation du préjudice *collectif*. Les règles existantes ne permettent pas nécessairement de signaler les discriminations subies par un groupe d'individus visé par un traitement algorithmique, au-delà de la somme des individus. Comme le soulignent certains rapports (voir par exemple le rapport de la CNIL³ ou le rapport de la mission présidée par Cédric Villani⁴), plusieurs algorithmes fonctionnent en effet non à l'échelle de la personne mais à celle du groupe et les données ne sont pas tant granulaires que réticulaires, c'est-à-dire organisées en réseau. Ils peuvent dès lors être exploités afin de produire des corrélations concernant des segments ou groupes d'individus, potentiellement exposés à certains risques de discrimination. Cela appelle par conséquent une réflexion sur ces enjeux éthiques s'agissant de cette dimension collective et les solutions possibles.
- F. ***L'IA n'est pas toujours exacte (5)*** : Les techniques d'apprentissage machines ne sont en général pas exactes au sens propre, mais peuvent fournir des approximations qui peuvent être intéressantes. Par ailleurs, il va de soi qu'un système qui est systématiquement faux ou approximatif est problématique. Il faudrait donc prévoir des méthodes et des critères de validation de l'apprentissage machine ainsi que des procédures de maintenance et s'intéresser aussi à la question importante de la reproductibilité des résultats.

Avez-vous d'autres préoccupations concernant l'IA qui ne sont pas mentionnées ci-dessus? Veuillez préciser:

D'autres enjeux éthiques importants sont soulignés dans l'avis de 2017 la CERNA sur [l'Ethique de la recherche en apprentissage machine](#).

Trois problèmes de premier plan provoquent surtout des tensions éthiques : a) la spécification d'un système d'IA qui ne peut saisir complètement et correctement la définition d'un concept en langue naturelle, d'où l'inexactitude inhérente qui induit des erreurs d'interprétation ; b) l'instabilité de l'apprentissage d'un système d'IA qui ne classifiera pas « humainement » ou « correctement » une donnée qui ne faisait pas partie de son corpus d'apprentissage, provoquant de multiples problèmes de sécurité; c) la vérification d'un système d'IA dont on ne peut prouver que l'apprentissage respectera un cadre prédéfini en toutes circonstances, ce qui pose des question de responsabilité).

Plus largement, et en continuation de la discussion sur l'explicabilité, se pose la question des actions « inhumaines » de la part des systèmes d'IA, des interprétations données à ces actions par les utilisateurs et des changements de comportement des utilisateurs humains qui interagissent avec de tels systèmes.

Pensez-vous que les préoccupations exprimées ci-dessus peuvent être résolues par la législation européenne applicable? Dans la négative, estimez- vous qu'il devrait y avoir de nouvelles règles spécifiques pour les systèmes d'IA?

² http://cerna-ethics-allistene.org/digitalAssets/53/53991_cerna___thique_apprentissage.pdf

³ https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

⁴ https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf

- La législation actuelle est amplement suffisante
- **La législation actuelle peut présenter quelques lacunes**
- Une nouvelle législation s'impose
- Autre Sans avis

Nous avons aujourd'hui un corpus de règles très important découlant d'instruments divers adoptés au fil du temps au sein de l'Union Européenne (sans parler d'autres règles et standards internationaux). Ces règles (telles que celles contenues, par exemple, dans le RGPD) sont « technologiquement neutres » (c'est à dire qu'elles ne sont pas spécifiques de technologies particulières) et restent pleinement applicables en matière d'IA. Elles constituent une bonne base de départ pour la régulation de l'IA et pour répondre aux risques susmentionnés.

Néanmoins, le CNPEN considère que le cadre législatif pourrait être amélioré et ceci pour plusieurs raisons.

- Premièrement, en l'état actuel il existe un risque de fragmentation du fait de divergences nationales dans l'application des règles existantes. Il serait donc utile d'assurer progressivement une interprétation uniforme des règles existantes par les organes de contrôle, les régulateurs, voire le législateur européen. À titre d'exemple, le Comité Européen de Protection des Données a un rôle important à jouer en ce qui concerne l'application du RGPD en matière d'IA.
- Deuxièmement, il est clair que, dans certains domaines, les règles existantes pourraient ne pas suffire et que l'on pourrait avoir besoin d'adapter le cadre législatif existant, voire d'adopter des nouvelles règles, pour faire face à un certain nombre de situations et de risques (voir, par exemple, nos commentaires sur la responsabilité dans la Section 3). Ceci pourrait être particulièrement utile pour mieux protéger les droits fondamentaux ou pour améliorer le régime juridique de responsabilité afin de garantir un système plus efficace et équitable d'indemnisation pour les dommages causés par l'utilisation d'IA.
- Enfin, le CNPEN considère qu'il est nécessaire de s'assurer que le cadre réglementaire existant tient suffisamment compte d'une série de principes éthiques nécessaires pour bâtir une IA de confiance.

Si vous pensez que de nouvelles règles sont nécessaires pour les systèmes d'IA, êtes-vous d'accord avec le fait que l'introduction d'exigences obligatoires nouvelles devrait être limitée aux applications à haut risque (dans lesquelles le préjudice éventuel causé par le système d'IA est particulièrement élevé)?

- Oui
- Non
- Sans Avis
- **Autre (veuillez préciser):**

Une approche réglementaire fondée sur une analyse de risques semble justifiée, tout comme la préoccupation de la Commission de ne pas s'engager dans une sur-réglementation européenne qui pourrait freiner l'innovation et le déploiement des effets bénéfiques multiples attendus par l'IA.

Il est important néanmoins d'évaluer les besoins en matière de régulation au cas par cas. Le critère pour l'adoption de règles pourrait ne pas être exclusivement le risque d'un préjudice « particulièrement élevé » mais aussi d'autres critères, y compris un risque important de violation des principes éthiques. Comme expliqué en introduction, les saisines initiales du CNPEN concernent trois domaines dont deux seulement (santé et véhicules connectés) semblent répondre à la définition de « haut risque » de la Commission. Les agents conversationnels présentent pourtant de « haut risques » dans certains domaines, par exemple lorsqu'ils sont utilisés avec reconnaissance faciale (et/ou audio) des émotions dans le cadre du recrutement avec des risques élevés de discrimination.

Ces situations mériteraient considération dans une approche réglementaire. Il serait peu satisfaisant, d'un point de vue éthique, que des dommages subis par des individus ne soient pas indemnisés ou pris en considération car d'une part ils se situent dans la « zone grise » de l'arsenal réglementaire existant et, d'autre part, les institutions européennes n'auraient pas souhaité combler les lacunes existantes considérant qu'il ne s'agit pas là de domaines « à haut risque ».

Êtes-vous d'accord avec l'approche proposée à la section 5.B du Livre blanc afin de déterminer si une application de l'IA est «à haut risque» ?

- Oui
- Non
- Sans Avis
- **Autre (veuillez préciser):**

L'approche proposée constitue un bon point de départ mais devrait être affinée afin de mieux parvenir à une définition satisfaisante de la notion de « haut risque ». Comme la Commission elle-même le reconnaît, il peut exister des situations (des cas exceptionnels ?) dans lesquelles, « compte tenu des risques, l'utilisation d'applications d'IA à certaines fins devrait être considérée comme étant à haut risque en soi, c'est-à-dire indépendamment du secteur concerné ». Il en résulte une double incertitude : quant aux situations précises où le secteur n'est plus un critère déterminant ; et quant à la personne qui va procéder à cette évaluation et aux méthodes utilisées. On pourrait craindre que, compte tenu de ces incertitudes, les développeurs et opérateurs de systèmes IA puissent revendiquer ce pouvoir d'appréciation. Le fait de décider si un système d'IA (et les technologies connexes) doit être considéré comme étant « à haut risque » devrait toujours découler d'une évaluation impartiale, réglementée et externe prenant en compte non seulement l'application elle-même, mais aussi son intégration dans un système d'information plus global. L'évaluation du risque doit être fondée non seulement sur la gravité du dommage potentiel mais aussi sur la gravité de la violation des principes éthiques sous-jacents.

Si vous le souhaitez, veuillez indiquer quelle est, de votre point de vue, l'application ou l'utilisation de l'IA la plus préoccupante («à haut risque»):

Si les systèmes d'armes létaux autonomes viennent immédiatement à l'esprit, d'autres applications pourraient aussi susciter des préoccupations éthiques tout aussi fondamentales. À titre d'exemple les applications suivantes pourraient être très préoccupantes : les systèmes de « notation sociale » des citoyens d'un pays fondés sur une évaluation de leur comportement et de leur « intégrité éthique » ; les systèmes de surveillance de masse fondés sur la reconnaissance biométrique ; ou encore certains systèmes décisionnels fondés sur les réactions émotionnelles comme par exemple la reconnaissance d'émotions faciales ou audio pour le recrutement, la détection du mensonge aux frontières, la détection de l'attention des élèves à l'école, etc.

Selon vous, quelle est l'importance des exigences obligatoires suivantes énoncées dans un éventuel futur cadre réglementaire pour l'IA (section 5.D du Livre blanc) (de 1 à 5: 1 n'est pas important du tout, 5 est très important)?

	1 — Pas important du tout	2 - Pas important	3 - Neutre	4 - Important	5 - Très important	Sans avis
Qualité des ensembles de données d'entraînement	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Conservation des dossiers et des données	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>	<input type="radio"/>
Informations sur la finalité et la nature des systèmes d'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Robustesse et précision des systèmes d'IA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Contrôle humain	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>
Règles claires en matière de sécurité et de responsabilité	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	X	<input type="radio"/>

A. **Qualité des ensembles de données d'entraînement (5)** : La qualité et l'intégrité des données sont essentielles au bon fonctionnement des systèmes IA.

B. **Conservation des dossiers et des données (4)** : Il convient ici de distinguer deux situations. D'une part, il est très important d'établir des exigences relatives à la conservation des dossiers de programmation de l'algorithme et des données utilisées pour entraîner les systèmes d'IA. La traçabilité des systèmes d'IA doit en effet être assurée. Il est donc important de pouvoir tracer l'ensemble du processus qui a abouti à la prise d'une décision et d'enregistrer l'ensemble des décisions prises par les systèmes.

En revanche, la conservation des données elles-mêmes pourrait s'avérer problématique à trois titres :

- Premièrement la conservation de grandes masses de données pourrait augmenter les risques d'atteinte à la vie privée et d'exploitation malveillante.
- Deuxièmement la conservation systématique de grandes masses de données a un impact énergétique et environnemental non négligeable. Le CNPEN considère que l'IA doit être développée et utilisée de manière à garantir un respect optimal de l'environnement et à réduire autant que possible son empreinte écologique, afin de soutenir la réalisation des objectifs fixés en matière de neutralité climatique et d'économie circulaire.
- Troisièmement la conservation des données personnelles doit être conforme aux règles en matière de protection des données et de la vie privée qui imposent souvent aux acteurs privés et publics des délais de rétention courts et/ou des limitations dans le temps liées à la durée du consentement et au principe de minimisation des données.

C. **Informations sur la finalité et la nature des systèmes d'IA (5)** : L'information sur la finalité d'un système d'IA (les objectifs poursuivis), ses capacités et ses limites et les conditions dans lesquelles il devrait fonctionner sont importantes non seulement pour les opérateurs et les utilisateurs mais aussi, éventuellement, pour les autorités compétentes. Il est important, de façon générale, de respecter le principe de transparence et d'information. Par ailleurs la Commission souligne avec raison que des informations devraient être clairement fournies aux citoyens lorsqu'ils interagissent avec un système d'IA et non avec un être humain.

D. **Robustesse et précision des systèmes d'IA (5)** : Comme déjà mentionné, la robustesse et la fiabilité des systèmes IA ainsi que leur cybersécurité sont des conditions essentielles pour parvenir à une IA de confiance. Les systèmes d'IA devraient être fiables et intégrer des mécanismes de sécurité par conception (« safety by design ») et

de sûreté. Voir aussi *supra* nos développements sur « l'exactitude » et le rapport qui y est mentionné.

- E. **Contrôle humain (5)** : Le Livre Blanc intègre, à juste raison, la notion d'une Garantie Humaine de l'intelligence artificielle (*Human Oversight* ou *Human Warranty*). Ce principe a d'ores et déjà fait l'objet de travaux abondants dans le cadre du processus en cours de révision de la loi de bioéthique française sous l'égide du CCNE et des démarches initiées par le CNPEN.

Cette idée d'une Garantie Humaine de l'IA est issue d'un mouvement de propositions académiques, citoyennes mais aussi de professionnels de santé. Ce principe a été reconnu dans les avis 129 et 130 du CCNE et dans l'article 11 du projet de loi bioéthique en cours d'examen devant le Parlement français. Cette notion a également été portée dans le cadre des travaux en cours de la task-force sur la régulation de l'IA dans le cadre de l'Organisation Mondiale de la Santé.

Le concept de « Garantie Humaine » peut paraître abstrait mais il est, en réalité, très opérationnel. Dans le cas de l'IA, l'idée est d'appliquer les principes de régulation de l'intelligence artificielle en amont et en aval de l'algorithme lui-même en établissant des points de supervision humaine. Non pas à chaque étape, sinon l'innovation serait bloquée. Mais sur des points critiques identifiés dans un dialogue partagé entre les professionnels, les patients et les concepteurs d'innovation.

Dans le domaine de la santé, le CCNE a proposé que cette supervision puisse s'exercer avec le déploiement de « **collèges de garantie humaine** » associant médecins, professionnels paramédicaux et représentants des usagers. Leur vocation serait d'assurer *a posteriori* une révision de dossiers médicaux pour porter un regard humain sur les options thérapeutiques conseillées ou prises par l'algorithme. L'objectif consiste à s'assurer « au fil de l'eau » que l'algorithme reste sur un développement de *Machine Learning* à la fois efficace médicalement et responsable éthiquement. Les dossiers à auditer pourraient être définis à partir d'événements indésirables constatés, de critères prédéterminés ou d'une sélection aléatoire. Un premier cas pilote de collège de garantie humaine est en phase de déploiement sous l'égide de l'Union française pour la santé bucco-dentaire (UFSBD) : il mettra en œuvre, dans le cadre d'un programme de financements innovants de la Sécurité sociale, une supervision pour un programme d'IA applicable aux soins dentaires pour 48 EHPAD et mis en œuvre par la start-up française *Dental Monitoring*. Cette méthodologie est, en outre, mobilisée dans le cadre des travaux de DRIM France IA, démarche de rassemblement des acteurs de la radiologie française pour le développement responsable de l'IA dans cette discipline.

Cette méthode de supervision humaine au fil de l'eau associant innovateurs en IA, experts techniques et représentants des bénéficiaires finaux est transposable dans d'autres domaines économiques et sociaux que la santé.

- F. **Règles claires en matière de sécurité et de responsabilité (5)** : Nous n'avons aucun doute sur le fait que l'existence de règles claires en matière de sécurité et de responsabilité est indispensable pour assurer la nécessaire sécurité et visibilité juridiques et garantir la protection des consommateurs, la sécurité juridique pour les entreprises et un rôle et des limites clairs pour les régulateurs et les pouvoirs publics.

En plus de la législation existante de l'UE, en particulier le cadre relatif à la protection des données, et notamment le règlement général sur la protection des données et la directive en matière de protection des données dans le domaine répressif, ou, le cas échéant, les nouvelles exigences obligatoires éventuellement prévues plus haut (voir la question ci-dessus), estimez-vous que l'utilisation de systèmes d'identification biométrique à distance (par exemple, la reconnaissance faciale) et d'autres technologies susceptibles d'être utilisées dans les espaces publics doit

faire l'objet d'orientations ou de réglementations supplémentaires au niveau de l'UE?

- Aucune orientation ou réglementation supplémentaire ne s'impose
- Les systèmes d'identification biométrique ne devraient être autorisés dans les espaces accessibles au public que dans certains cas ou si certaines conditions sont remplies (veuillez préciser)
- **Il faudrait imposer d'autres exigences particulières, en plus de celles mentionnées dans la question ci-dessus (veuillez préciser)**
- L'utilisation de systèmes d'identification biométrique dans les espaces accessibles au public, à titre d'exception à l'interdiction générale actuelle, ne devrait être possible qu'après la mise en place d'une orientation ou d'une législation spécifique au niveau de l'UE
- Les systèmes d'identification biométrique ne devraient jamais être autorisés dans les espaces accessibles au public
- Sans avis

Veuillez préciser votre réponse:

Il est très satisfaisant qu'en Europe, contrairement à d'autres parties du monde, nous disposions déjà de règles importantes en matière de cadrage de la reconnaissance faciale. Des instruments comme la Charte des droits fondamentaux de l'UE, la Convention européenne des droits de l'homme, le RGPD ou la directive police-justice posent déjà un cadre réglementaire important pour l'utilisation de techniques de reconnaissance faciale (TRF) par le secteur privé ou le secteur public.

Nous considérons, néanmoins, que, compte tenu des risques particulièrement importants existant dans ce domaine, les règles devraient être précisées et complétées. Premièrement, il y a un risque important d'interprétation divergente des règles existantes par les autorités de régulation et de contrôle dans les pays européens. Deuxièmement, la transparence en Europe sur les projets d'utilisation des TRF par le privé et le public devrait être assurée. Troisièmement, plutôt que d'entrer de façon aveugle dans une « course » aux TRF avec les États-Unis ou la Chine, l'Europe devrait donner l'exemple en se focalisant sur les problèmes que la reconnaissance faciale pourrait résoudre et en insistant sur les principes de nécessité et de proportionnalité. Quatrièmement, une réglementation claire et homogène au sein de l'EU favoriserait la dynamique de l'innovation et l'acceptabilité des citoyens, en prévenant d'éventuelles dérives. Des interventions législatives ou réglementaires pourraient s'avérer nécessaires pour fixer les « lignes rouges », aider à établir des lignes directrices là où l'utilisation des TRF se justifie et prévoir des garanties, contrôles et voies de recours appropriés. De façon plus générale, les TRF dans l'espace public posent des dilemmes éthiques particulièrement importants qui devraient d'abord être analysés au niveau politique après un débat démocratique. Le CNPEN espère pouvoir contribuer dans l'avenir à ce débat tant sur le plan national que sur le plan européen.

Estimez-vous qu'un système de label non obligatoire (section 5.G du Livre blanc) serait utile pour les systèmes d'IA qui ne sont pas considérés comme étant à haut risque, en plus de la législation existante?

- Extrêmement utile
- **Très utile**
- Plutôt inutile
- Tout à fait inutile
- Sans avis

Avez-vous d'autres suggestions sur un système de label non obligatoire?

Un système de label non obligatoire peut être utile pour des systèmes d'IA qui ne sont pas considérés à haut risque. Mais il faut veiller à ce que ces labels ne soient pas l'apanage de groupes industriels qui s'auto-labelliseront. En complément, cela nécessite donc la mise en place d'organismes de certification et d'éducation de la population et l'on préconise plutôt le respect de normes et de standards internationaux précis et auditable.

Quel est le moyen de garantir une IA digne de confiance, sûre et respectueuse des règles et valeurs européennes?

- Évaluation préalable de la conformité des applications à haut risque avec les exigences identifiées (avant de mettre le système sur le marché)
- Évaluation a posteriori de la conformité des applications à haut risque au moyen d'une procédure d'évaluation externe de la conformité
- Surveillance a posteriori du marché après la mise sur le marché du produit ou du service à haut risque reposant sur l'IA et, le cas échéant, contrôle du respect assuré par les autorités compétentes concernées
- **Combinaison de mécanismes d'évaluation préalable de la conformité et de contrôle a posteriori du respect**
- Autre système de contrôle du respect
- Sans avis

Veillez préciser tout autre système de contrôle du respect

Tout système d'IA considéré « à haut risque » devra être soumis une homologation et une certification de conformité a priori. De plus, dans la mesure où la réponse d'un algorithme d'IA est susceptible d'évoluer quand il s'agit d'un apprentissage supervisé ou non supervisé ou par renforcement, en particulier si l'apprentissage est réalisé en continu et si le domaine d'application est ouvert, il est indispensable de soumettre le système à des tests réguliers et normés pour vérifier que la réponse ne s'écarte pas du cadre de l'homologation. Cela peut passer a minima par des contrôles techniques réguliers, comme ceux déjà pratiqués pour les automobiles, mais aussi nécessiter des étapes de re-homologation et re-certification des logiciels d'IA.

Section 3 – Implications de l'intelligence artificielle, de l'internet des objets et de la robotique en matière de sécurité et de responsabilité

L'objectif général des cadres juridiques en matière de sécurité et de responsabilité est de garantir que tous les produits et services, y compris ceux qui intègrent des technologies numériques émergentes, fonctionnent de manière sûre, fiable et cohérente et que les dommages qui se sont produits soient réparés efficacement.

La législation actuelle sur la sécurité des produits offre déjà une interprétation étendue de la notion de sécurité qui permet de protéger contre tous types de risques liés aux produits en fonction de leur utilisation. Toutefois, quels risques particuliers découlant de l'utilisation de l'IA conviendrait-il, selon vous, de préciser davantage afin d'assurer une plus grande sécurité juridique?

- **Les risques liés à la cybersécurité**
- **Les risques pour la sécurité des personnes**
- Les risques liés à la perte de connectivité
- **Les risques pour la santé mentale**

Les risques liés à la cybersécurité sont de loin les plus importants car les cyberattaques peuvent avoir des conséquences multiples et néfastes. Il est néanmoins rassurant que toutes les parties prenantes ont conscience de ces risques ce qui devrait permettre une prise en compte adéquate de ce risque dans le cadre de futures évolutions normatives. D'autres risques, néanmoins, tels que ceux relatifs à la santé mentale décrits dans le Livre Blanc, sont très peu pris en considération par les règles existantes. Il serait dès lors utile que les risques pour la santé mentale soient explicitement couverts par le concept de sécurité des produits dans le cadre législatif.

Selon vous, faut-il élargir à d'autres risques afin d'assurer une plus grande sécurité juridique ?

N/A

Pensez-vous que le cadre législatif relatif à la sécurité devrait envisager de nouvelles procédures d'évaluation des risques pour les produits faisant l'objet de changements importants au cours de leur durée de vie?

- **Oui**
- Non
- Sans avis

Le développement des outils numériques et des algorithmes d'IA permettant de rejouer des séquences préalablement enregistrées, ainsi que la simulation numérique de mises en scène réalistes de cas d'usage comportant des risques offrent de grandes possibilités de faire évoluer les procédures d'évaluation des risques pour les produits faisant l'objet de changements importants au cours de leur durée de vie. Cela offre de nouvelles possibilités de virtualisation des tests d'homologation et de certification par des « jumeaux numériques ». De plus, en développant des scénarios (*serious games*) les outils de simulation peuvent constituer des outils d'aide à la décision pour des comités d'évaluation impliquant des représentants des diverses parties prenantes d'un domaine d'application et d'un écosystème spécifique (mobilité, énergie, santé, défense etc.).

Avez-vous d'autres considérations concernant les procédures d'évaluation des risques?

N/A

Pensez-vous que le cadre législatif actuel de l'UE en matière de responsabilité (directive sur la responsabilité du fait des produits) devrait être modifié afin de mieux couvrir les risques engendrés par certaines applications de l'IA?

- **Oui**
- Non
- Sans avis

Avez-vous d'autres considérations concernant la question ci-dessus?

Comme en matière de régulation en général (*supra*), le CNPEN n'est pas favorable à une refonte complète des régimes de responsabilité existants – et de la directive sur la responsabilité du fait des produits (directive 85/374/CEE) – qui fonctionnent plutôt bien. Il considère que la mise en place de règles de responsabilité très lourdes pourrait freiner l'innovation et s'avérer préjudiciable pour le développement de l'IA en Europe.

Le CNPEN note, néanmoins, que la directive sur la responsabilité du fait des produits a été adoptée en 1985, une époque antérieure à la prise en considération des risques associés à l'émergence des nouvelles technologies numériques et, surtout, de l'IA. Certes, les règles de la directive ne sont pas spécifiques à des technologies particulières et s'appliquent donc quelle que soit la technologie

utilisée. Mais elles ne sont pas toujours en mesure de saisir les difficultés qui résultent de la complexité, la connectivité, l'opacité, la vulnérabilité et l'autonomie des systèmes d'IA. L'impact social d'une incapacité des systèmes juridiques d'apporter des réponses satisfaisantes aux défis posés par les technologies de l'information, y compris et surtout en matière d'indemnisation équitable pour les dommages subis, pourrait rompre la confiance dans l'IA et compromettre les effets bénéfiques attendus. Le CNPEN considère donc que des ajustements spécifiques du cadre législatif actuel pourraient être nécessaires pour éviter que des personnes victimes de préjudices ou dont les biens sont endommagés se trouvent sans réparation. L'attention du législateur pourrait être portée sur des sujets tels que les suivants :

- Le fait que la directive repose sur le concept de « produit » (et de ses défauts), perçu essentiellement comme un objet alors que dans les systèmes d'IA les « produits » et les « services » interagissent de façon permanente (comme en témoigne l'exemple de la voiture connectée) ;
- Le fait que le concept de « défaut » d'un produit mériterait d'être précisé dans le cadre des caractéristiques très spécifiques des systèmes d'IA, voire des logiciels en général.

Pensez-vous que les règles nationales actuelles en matière de responsabilité devraient être adaptées en tenant compte du fonctionnement de l'IA afin de mieux garantir une réparation adéquate des dommages et une répartition équitable des responsabilités?

- Oui, pour toutes les applications de l'IA
- **Oui, pour des applications de l'IA spécifiques**
- Non
- Sans avis

Veuillez préciser les applications de l'IA:

Les droits nationaux en matière de responsabilité souffrent de fragmentation et ne comportent souvent pas de règles spécifiques en matière de responsabilité pour dommages causés par des systèmes d'IA. Sans énumérer ici les applications de l'IA spécifiques, il nous semble qu'il est nécessaire de procéder à une étude approfondie et secteur par secteur afin de tenir compte des éléments suivants :

- Les difficultés liées à la définition du dommage et des types de dommages indemnisés par les droits nationaux.
- Les difficultés liées à la nécessité pour la victime d'apporter la preuve de l'existence d'un lien de causalité qui pourrait s'avérer une véritable *probatio diabolica* quand le dommage résulte du dysfonctionnement d'un système d'IA. Apporter la preuve d'une discrimination résultant d'un traitement algorithmique constitue, par exemple, une difficulté essentielle au regard de l'opacité du système informatique.
- Ces difficultés probatoires ne se limitent pas d'ailleurs à l'établissement du seul lien de causalité. Elles portent également sur l'existence de la discrimination per se. En effet, comment le demandeur peut-il être à même d'établir l'effet discriminatoire d'une pratique, notamment lorsque les critères fondant la décision prise à l'issue d'un traitement algorithmique ainsi que leur pondération ne sont pas connus ? A défaut d'information sur ces critères, seule une analyse statistique des résultats produits par l'algorithme permettrait d'établir de tels faits. Mais une telle analyse ne saurait certainement être menée par le demandeur seul, s'il s'agit d'un individu contestant une décision prise à son encontre. Il convient alors de mener une réflexion sur le point de savoir comment remédier à de telles difficultés.
- La nécessité de repenser, en fonction de la situation, la répartition de la responsabilité entre le producteur, le fabricant, le développeur, l'opérateur, et l'utilisateur.

- La possibilité de prévoir différentes règles de responsabilité pour différents risques et, surtout, un système de facilitation de la preuve ou un régime de responsabilité stricte pour des systèmes d'IA « à haut risque ».
- La nécessité de définir si les systèmes d'IA identifiés comme « à haut risque » à des fins de responsabilité stricte devraient être les mêmes (ou plutôt plus restreints) que les systèmes « à haut risque » à des fins de régulation discutés dans la Section II de ce questionnaire et sur la base de quels critères distinguer les deux catégories.
- L'utilité ou non d'envisager un devoir de diligence accrue des développeurs, opérateurs et autres parties prenantes d'un système d'IA leur imposant de sélectionner, d'exploiter, de surveiller et d'entretenir correctement la technologie utilisée.
- Le principe d'équivalence fonctionnelle qui devrait garantir que les personnes qui ont subi un dommage du fait de l'utilisation d'un système d'IA ne devraient pas être moins indemnisées que si le dommage provenait d'un système analogue déjà couvert par le droit européen ou les droits nationaux.

Avez-vous d'autres considérations concernant la question ci-dessus?

Le CNPEN souhaite rappeler la polémique suscitée début 2017 quand [le Parlement Européen a proposé](#) à la Commission Européenne, « la création d'une personnalité juridique spécifique aux robots » qui impliquerait que les robots pourraient être tenus pour civilement responsables des dommages qu'ils causeraient, ce qui obligerait leurs fabricants ou propriétaires à contracter des polices d'assurance couvrant les dommages potentiels causés par leurs robots.

Le [Comité Economique et Social Européen \(CESE\) s'est opposé](#) formellement à cette proposition pour deux raisons principales : i) « le risque moral inacceptable » que le fabricant n'assume plus sa responsabilité, transférée au robot (ou au système d'IA), au détriment d'une éthique de conception, et ii) « le risque d'utilisation impropre et d'abus d'une telle forme juridique » si les incidents consécutifs à une mauvaise utilisation peuvent être imputés à l'IA ou au robot intelligent par son propriétaire.

Le CNPEN considère que ce débat juridique et éthique est de première importance.

Merci pour votre contribution à ce questionnaire.

Les membres du Comité national pilote d'éthique du numérique

Gilles Adda	Christine Froidevaux	Christophe Lazaro
Raja Chatila	Jean-Gabriel Ganascia	Gwendal Le Grand
Theodore Christakis*	Eric Germain	Claire Levallois-Barth
Laure Coulombel	Alexei Grinbaum	Caroline Martin
Jean-François Delfraissy	David Gruson	Tristan Nitot
Karine Lefeuvre	Emmanuel Hirsch	Jérôme Perrin*
Laurence Devillers	Jeany Jean-Baptiste	Catherine Tessier
Karine Dognin-Sauze	Claude Kirchner - directeur	Serena Villata
Gilles Dowek	Augustin Landler	Célia Zolynski
Valeria Faure-Muntian		

*co-rapporteurs de cette contribution

Contact : camille.darche@ccne.fr