Conseil des barreaux européens
La voix des avocats européens
Rue Joseph II, 40/8 - B-1000 Bruxelles
+32 (0)2 234 65 10 | ccbe@ccbe.eu | www.ccbe.eu

Réponse du CCBE à la consultation sur le Livre blanc de la Commission européenne sur l'intelligence artificielle

05/06/2020

Introduction et résumé

Le Conseil des barreaux européens (CCBE) représente les barreaux de 45 pays, soit plus d'un million d'avocats européens. Le CCBE répond régulièrement au nom de ses membres aux consultations sur les politiques qui concernent les citoyens et les avocats européens.

Le CCBE tient à expliquer plus en détail un certain nombre de ses réponses au questionnaire général concernant la consultation sur le Livre blanc Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance (**tel que repris ci-dessous en annexe**), et à présenter des propositions plus détaillées sur les questions les plus pertinentes du point de vue des avocats. Ce document s'inspire en grande partie des Considérations du CCBE sur les aspects juridiques de l'intelligence artificielle récemment publiées.

Tout d'abord, le CCBE exprime ses préoccupations quant à la manière dont le questionnaire de consultation a été formaté. Le questionnaire n'a pas été adapté à des secteurs et à des cas d'utilisation particuliers et n'offre pas aux répondants la possibilité d'indiquer à chaque question dans quelle perspective la réponse est donnée. En conséquence, il sera très difficile d'interpréter les différentes réponses sans informations complémentaires sur la manière dont les répondants respectifs ont abordé les différentes questions. En outre, de nombreuses questions constituent des questions directives qui n'offrent qu'un ensemble fermé d'options, ce qui rend impossible l'expression d'un avis valable[1].

Dès lors, le CCBE souhaite préciser que la portée de sa réponse à cette consultation est principalement limitée aux aspects liés à l'état de droit, à l'administration de la justice et aux droits fondamentaux. En outre, le CCBE aborde également certaines questions de responsabilité ainsi que les besoins de formation des avocats et des cabinets d'avocats concernant l'utilisation de l'intelligence artificielle dans la pratique juridique.

Les parties ci-dessous sont structurées en fonction des thèmes abordés dans le questionnaire de consultation et traitent des principales questions suivantes :

- Un écosystème d'excellence :

- **Un financement à échelle européenne** doit être mis à la disposition des régulateurs sectoriels (y compris les barreaux) afin de **former les avocats** sur des sujets tels que l'utilisation des nouvelles technologies et l'intelligence artificielle dans le domaine de la justice tout en respectant les principes éthiques et les exigences en matière de protection des données.

[1] Dans ses remarques concernant la consultation de la Commission « Bilan de l'approche de la Commission européenne en matière d'amélioration de la réglementation », le CCBE a demandé à la Commission de réviser sa méthodologie de conception des questionnaires. Voir les paragraphes 3-6 ici.

- **L'interaction entre tous les secteurs**, privés et publics, est essentielle pour garantir que les valeurs éthiques qui guident les différents acteurs soient intégrées dans les systèmes d'intelligence eux-mêmes.
- Les avocats doivent avoir **accès à des installations d'essais** et de référence pour pouvoir exercer pleinement leur rôle et leurs responsabilités en garantissant le déploiement et l'examen appropriés des outils d'intelligence artificielle

- Un écosystème de confiance :

- Intelligence artificielle et droits humains : pratiquement tous les droits humains peuvent être affectés par l'utilisation de systèmes d'intelligence artificielle. Diverses actions sont donc nécessaires, parmi lesquelles : des évaluations approfondies de l'effet des systèmes d'intelligence artificielle ; un examen indépendant et expert ; garantir la disponibilité de recours ; de nouveaux cadres juridiques pour codifier les principes et exigences régissant l'utilisation de l'intelligence artificielle, en conjonction avec des codes éthiques volontaires engageant les développeurs d'intelligence artificielle à agir de manière responsable.

- **En solution de rechange à l'approche fondée sur les risques proposée, le CCBE demande une approche plus ciblée** qui fixe des exigences juridiques adaptées aux besoins des secteurs et des circonstances spécifiques après une évaluation plus détaillée des risques et une évaluation des mesures juridiques ou autres mesures appropriées.
- **L'utilisation de l'intelligence artificielle par les tribunaux et dans les systèmes de justice pénale est un risque élevé** étant donné qu'elle porte atteinte à bon nombre des fondements sur lesquels repose la justice. Tout déploiement de ces outils devrait donc être strictement réglementé et être précédé d'une évaluation et d'analyses d'impact approfondies avec la participation de tous les acteurs et parties prenantes concernés et être strictement réglementé en tenant compte de l'architecture procédurale qui sous-tend les procédures judiciaires. En tout état de cause, **le droit à un juge naturel** doit être garanti à tous les stades de la procédure.
- Une combinaison de **mécanismes de conformité au préalable et de mise en œuvre ultérieure** reposant sur un ensemble de **normes obligatoires** est nécessaire.

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

- **Certaines modifications importantes doivent être apportées au cadre législatif actuel** compte tenu des différences fondamentales qui existent entre les produits traditionnels et l'intelligence artificielle, notamment en ce qui concerne les notions de produit, de faute et de défaut.
- **Le CCBE privilégie un instrument séparé sur les questions de responsabilité en matière d'intelligence artificielle** plutôt qu'une modification de la directive en matière de responsabilité du fait des produits défectueux. Des aspects tels que l'indemnisation des dommages et l'attribution de la responsabilité, ainsi que les règles relatives à la charge de la preuve, doivent être réglementés au niveau de l'UE.
- Les questions à considérer lors de la modification du cadre législatif actuel comprennent : la **notion de produit**, le **manque de prévisibilité** dans le fonctionnement des systèmes d'intelligence artificielle, le **destinataire de la responsabilité**, les **défenses**, les **types de dommages et victimes**, la **règle de preuve** et le renversement de la charge de la preuve dans certaines situations, ainsi que la question de l'**assurance obligatoire**.

Section 1 - Un écosystème d'excellence

Le développement de l'intelligence artificielle et l'arrivée de la legal tech ont rendu la pratique du droit de plus en plus complexe en raison des nouvelles questions juridiques soulevées par l'intelligence artificielle et du développement d'outils numériques très sophistiqués que les avocats doivent maîtriser et comprendre. Il est également nécessaire que les avocats utilisent ces nouvelles technologies de manière consciente et responsable afin de mener leurs activités de la meilleure manière possible tout en protégeant la relation de confiance entre l'avocat et son client et en respectant leurs obligations professionnelles. De ces points de vue, les principes les plus évidents à respecter dans l'utilisation des outils d'intelligence artificielle concernent : le devoir de compétence, le devoir d'informer le client, le maintien de l'indépendance des avocats en termes de défense et de conseil, le devoir de préserver le secret professionnel et la confidentialité des données des clients. Une formation des avocats est dès lors nécessaire pour améliorer leurs compétences générales en matière de compréhension de l'environnement technologique dans lequel ils risquent de travailler à l'avenir.

Le CCBE soutient dès lors pleinement l'idée que le **financement à échelle européenne soit mis à la disposition des régulateurs sectoriels** (y compris les barreaux) étant donné qu'ils sont les mieux placés pour répondre aux besoins de formation de leur secteur respectif (tels que les avocats), notamment en ce qui concerne la manière dont l'intelligence artificielle peut être utilisée dans le respect de leurs codes de déontologie et de leurs obligations professionnelles. À cet égard, la *Contribution du CCBE à la prochaine politique de l'UE en matière de formation judiciaire*[2] souligne également la nécessité de former les avocats sur des sujets tels que l'utilisation des nouvelles technologies et de l'intelligence artificielle dans le domaine de la justice, tout en respectant les principes éthiques et les exigences en matière de protection des données.

Un autre aspect crucial est l'interaction entre tous les secteurs, privés et publics, pour garantir que les valeurs éthiques soient intégrées dans les systèmes d'intelligence artificielle eux-mêmes. Il ne suffit pas de se fier simplement à l'expertise des spécialistes techniques qui opèrent dans le domaine informatique. De nouveaux liens de confiance doivent être construits en tenant compte de l'expertise et des rôles spécifiques des acteurs et des spécialistes dans les différents secteurs et professions. Le CCBE rappelle à ce sujet que le rôle de l'avocat est important dans la garantie de l'accès à la justice, la défense de l'état de droit et la protection des valeurs démocratiques, il semble avoir un rôle particulier à jouer dans le développement et le déploiement des outils d'intelligence artificielle, en particulier dans les domaines où l'accès à la justice et le respect des procédures sont en jeu.

Les avocats doivent donc également avoir **accès aux installations d'essais et de référence** pour pouvoir exercer pleinement leur rôle et leurs responsabilités en garantissant le déploiement et l'examen appropriés des outils d'intelligence artificielle. Cela est d'autant plus important que les outils d'intelligence artificielle peuvent être contestés dans le cadre d'une procédure judiciaire et doivent alors être examinés par les parties.

Section 2 - Un écosystème de confiance

I. Intelligence artificielle et droits humains

En général, le recours à l'intelligence artificielle dans les processus décisionnels automatisés peut remodeler l'interaction entre les citoyens et les décideurs publics ou privés, ce qui peut nuire à la

[2] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/TRAINING/TR_Position_papers/FR_TR_20200427_CCBE-contribution-for-the-next-EU-policy-on-judicial-training.pdf

capacité des citoyens à demander des conseils, à contester ou à tenter de renverser des décisions. Il convient donc de garantir des mécanismes de recours solides ainsi qu'une implication étroite des acteurs qui ont une fonction de protection des droits des citoyens (les avocats et les juges par exemple).

En outre, pratiquement tous les droits humains peuvent être affectés par l'utilisation de systèmes d'intelligence artificielle. Le CCBE attire en particulier l'attention sur les points suivants :

Du point de vue du CCBE, le **droit à un procès équitable** est un point de préoccupation essentiel. Bien que les questions relatives à l'utilisation de l'intelligence artificielle au sein des tribunaux et dans les procédures pénales soient identifiées ci-dessous, le **droit à un juge naturel** fait également partie du droit à un procès équitable.

En outre, le **préjugé** potentiel des ensembles de données que l'intelligence artificielle utilise pour apprendre est également un exemple clair de problème affectant l'équité d'un procès. Les systèmes d'intelligence artificielle ne comprennent pas l'ensemble du contexte de nos sociétés complexes. Leurs données d'entrée constituent leur seul contexte et si les données fournies pour former l'intelligence artificielle sont incomplètes ou comportent un préjugé (même non intentionnel), les résultats de l'intelligence artificielle seront probablement dès lors également incomplets et biaisés. En outre, au stade actuel de développement, les systèmes d'intelligence artificielle manquent souvent de transparence dans leurs conclusions. Ils manquent d'explicabilité, c'est-à-dire la capacité d'expliquer à la fois les processus techniques d'un système d'intelligence artificielle et les décisions humaines qui s'y rapportent (par exemple, les domaines d'application d'un système). Par conséquent, les humains ne comprennent pas ou ont des doutes sur la manière dont les systèmes d'intelligence artificielle parviennent à leurs conclusions. Ces conclusions peuvent être inoffensives dans le cadre d'un usage ordinaire, mais elles peuvent porter atteinte à l'équité de la procédure lorsqu'elles sont utilisées devant un tribunal.

Dans un souci de **transparence** et afin de permettre aux personnes de défendre leurs droits, il semble approprié que les personnes concernées par l'utilisation d'un système d'intelligence artificielle soient dûment informées que l'intelligence artificielle est utilisée et que les données les concernant peuvent être examinées par un système automatisé. Cela correspond aux principes actuels de protection des données, qui doivent en général être respectés lors de l'utilisation de l'intelligence artificielle, tout comme toute autre norme juridique applicable. Comme c'est souvent le cas ailleurs, garantir la disponibilité de recours sera probablement la mesure appropriée pour traiter les cas d'utilisation abusive des systèmes d'intelligence artificielle ou les dommages causés par ceux-ci.

Le **droit à la liberté d'expression et d'information** peut également être affecté : l'intelligence artificielle permettra de surveiller et de contrôler davantage la manière dont les gens peuvent s'exprimer en ligne et hors ligne. Si des utilisations positives peuvent être constatées dans la lutte contre les discours de haine et les fausses informations (fake news), la ligne de démarcation entre l'utilisation bénéfique de l'intelligence artificielle et son utilisation abusive semble peu convaincante.

De même, le **droit à la liberté de réunion et d'association** est à prendre en compte lorsque l'intelligence artificielle sert à identifier les participants à des assemblées, des manifestations ou tout autre grand rassemblement. Bien qu'utiles dans certaines situations pour protéger l'ordre public, ces outils peuvent facilement être utilisés à mauvais escient contre des opposants politiques. Des systèmes capables de reconnaître automatiquement les individus (reconnaissance faciale ou des mouvements) et d'analyser leur comportement sont déjà disponibles. Ces outils pourraient très bien influencer la participation des personnes aux assemblées, restreignant ainsi le droit à la liberté de réunion et d'association.

Le **droit à une vie protégée** dans le contexte des armes intelligentes et des drones à fonctionnement algorithmique sera également affecté par l'intelligence artificielle.

Le **droit à la protection contre les discriminations** peut être affecté lorsque les employeurs utilisent l'intelligence artificielle pour automatiser certaines parties des processus de recrutement des employés. Aujourd'hui encore, des systèmes capables de présélectionner les candidats à un lieu de travail sont disponibles.

À cette époque numérique, la quantité de données que les personnes fournissent sur elles-mêmes est énorme. Qu'il s'agisse de métadonnées ou de données de contenu, elles fournissent de nombreux détails sur leur vie personnelle ou des détails qui sont simplement privés. L'intelligence artificielle vit des données et sa capacité à travailler avec les données et à les combiner est immense. Le **droit à la vie privée et à la protection des données** est donc clairement en jeu.

Les principes démocratiques et l'état de droit sont étroitement liés aux droits humains du fait qu'ils se complètent. Compte tenu du droit à la vie privée, la collecte d'informations à partir des profils des réseaux sociaux des personnes sur leurs opinions politiques et leur utilisation (à mauvais escient) pour influencer les scrutins et les élections non seulement porte atteinte au droit à la vie privée mais peut également être considérée comme une ingérence dans l'un des principes de la société démocratique ayant une incidence directe sur l'ordre public.

Compte tenu de ces considérations, le CCBE recommande de prendre les mesures suivantes :

- En général, selon les recommandations actuellement disponibles dans ce domaine[3], il convient de noter que **des évaluations approfondies de l'effet des systèmes d'intelligence artificielle sur divers droits humains, principes démocratiques et l'état de droit** semblent être l'une des mesures pouvant être utilisées pour prévenir des conflits indésirables avec ces droits, principes et règles. Ces évaluations doivent être réalisées dès que possible, même au stade initial de développement, en évaluant les effets potentiels que les systèmes d'intelligence artificielle peuvent avoir sur les droits humains tout au long de leur cycle de vie.
- Il est également nécessaire de soumettre les systèmes d'intelligence artificielle à un **examen indépendant et expert**, en particulier lorsqu'ils sont destinés à un usage public. La publication des résultats d'un tel examen diminuera la probabilité de préjugés intentionnels et non intentionnels et augmentera probablement la fiabilité des systèmes d'intelligence artificielle. Ouvrir les systèmes d'intelligence artificielle à l'examen de n'importe quelle partie prenante peut accroître encore leur fiabilité mais entraînera forcément des ingérences proportionnées dans les secrets commerciaux et aux droits de propriété intellectuelle des développeurs d'intelligence artificielle.
- Dans un souci de **transparence** et afin de permettre aux personnes de défendre leurs droits, les personnes concernées par l'utilisation d'un système d'intelligence artificielle doivent être **dûment informées que l'intelligence artificielle est utilisée** et que les données les concernant peuvent être examinées par un système automatisé. Cela correspond aux principes actuels de protection des données, qui doivent en général être respectés lors de l'utilisation de l'intelligence artificielle, tout comme toute autre norme juridique applicable.
- Comme c'est souvent le cas ailleurs, **garantir la disponibilité de recours** sera probablement la mesure appropriée pour traiter les cas d'utilisation abusive des systèmes d'intelligence artificielle ou les dommages causés par ceux-ci.
- Il est nécessaire d'examiner si les **cadres juridiques** actuellement disponibles sont adéquats ou doivent être adaptés afin de garantir que les systèmes d'intelligence artificielle soient

[3] Conseil de l'Europe, Commissaire aux droits de l'homme : Désenclavement de l'intelligence artificielle : 10 mesures pour protéger les droits de l'homme (https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64)

utilisés dans le respect des droits humains. Il est possible que de nouveaux cadres juridiques doivent être établis pour codifier certains principes et exigences en conjonction avec des codes éthiques volontaires engageant les développeurs d'intelligence artificielle à agir de manière responsable. Étant donné que les technologies (y compris l'intelligence artificielle) sont extranationales, il serait souhaitable de mettre en place un cadre juridique qui ne se limite pas à une seule juridiction, ce qui semblerait conforme à l'évolution actuelle.[4]

Parallèlement à ces actions générales, certaines règles et certains principes doivent être établis dans des domaines spécifiques, notamment en ce qui concerne l'utilisation de l'intelligence artificielle par les tribunaux et dans les systèmes de justice pénale, tel qu'indiqué ci-après.

II. Adaptations possibles du cadre législatif communautaire existant en matière d'intelligence artificielle

A. Une approche fondée sur les risques

Le CCBE craint qu'un exercice de catégorisation des risques comme « élevés » ou « faibles » selon des critères abstraits soit trop simpliste et conduise à une réglementation structurellement défectueuse. Une approche plus ciblée est nécessaire.

Les facteurs à prendre en considération pour déterminer les risques sont nombreux et complexes, en fonction des cas d'utilisation spécifiques, des circonstances d'utilisation, de la complexité de la tâche, des risques posés par un éventuel dysfonctionnement de l'intelligence artificielle et de sa nature technique. Par exemple, l'intelligence artificielle d'un système de gestion des affaires utilisé par les tribunaux présente moins de risques que l'intelligence artificielle pour l'évaluation de la probabilité de récidive d'un défendeur.

Dans ces circonstances, il n'est pas approprié, tout d'abord, d'accorder le même traitement juridique à des choses qui sont techniquement différentes, par exemple l'intelligence artificielle, l'internet des objets et d'autres technologies numériques, même si elles partagent parfois des caractéristiques communes. En réalité, une approche plus nuancée prenant en considération les nouveaux défis complexes que crée l'intelligence artificielle est nécessaire.

Deuxièmement, le Livre blanc reconnaît que le niveau de risque peut être très différent, même au sein d'un même « secteur », comme les soins de santé par exemple. Une réglementation visant à neutraliser les risques ne peut donc être efficace que si elle cible des risques très spécifiques dans des circonstances particulières, tels qu'un risque de discrimination dans les systèmes de surveillance des services répressifs, ou un risque de procès inéquitable si les parties à une affaire n'ont pas la possibilité d'évaluer, de discuter et de soulever des objections contre un outil d'intelligence artificielle utilisé dans le processus de prise de décisions judiciaires.

Le CCBE demande donc une approche plus ciblée reposant sur les actions suivantes :

- **Évaluation des risques et dommages spécifiques** que l'utilisation d'outils d'intelligence artificielle peut entraîner dans des secteurs et circonstances spécifiques.
- **Évaluation du type de mesures juridiques ou autres mesures appropriées** qui pourraient être prises pour faire face aux risques et dommages identifiés dans des secteurs et circonstances spécifiques, en gardant à l'esprit que, dans un secteur donné, des niveaux de risque très

[4] Voir les activités du Conseil de l'Europe dans ce domaine et son comité ad hoc sur l'intelligence artificielle créé le 11 septembre 2019 pour évaluer la nécessité d'un tel cadre juridique : https://www.coe.int/fr/web/artificial-intelligence/-/the-council-of-europe-established-an-ad-hoc-committee-on-artificial-intelligence-cahai.

différents peuvent exister selon l'utilisation précise à laquelle l'intelligence artificielle est soumise. Dans ce contexte, il convient également d'évaluer dans quelle mesure la réglementation de l'UE existante doit être adaptée ou ajustée.

- **Définition d'exigences juridiques adaptées aux besoins des secteurs et des circonstances spécifiques.** Dans ce contexte, il est important d'examiner comment les principes généraux, tels que la non-discrimination et le droit à un procès équitable, s'appliquent et doivent être respectés.

B. Application de l'intelligence artificielle à haut risque : l'utilisation de l'intelligence artificielle par les tribunaux

En examinant les différentes utilisations possibles de l'intelligence artificielle dans le processus judiciaire, le constat est immédiat : son introduction dans les systèmes judiciaires pourrait porter atteinte à bon nombre des fondements sur lesquels repose la justice (voir le tableau).

Dans le domaine de la justice, de fortes incitations à avoir recours à l'intelligence artificielle peuvent exister. Les autorités publiques ont déjà identifié les avantages budgétaires supposés en remplaçant une partie du personnel judiciaire par des systèmes automatisés. L'utilisation potentielle de l'intelligence artificielle pourrait également être perçue comme un moyen permettant aux juges de rendre des décisions plus cohérentes et de meilleure qualité, plus rapidement, plus rationnellement et plus efficacement. Il ne fait donc aucun doute qu'il existera des tentatives de déploiement de l'intelligence artificielle dans le domaine de la justice, ce qui pose dès lors la question des conditions de cette utilisation.

La nécessité d'un cadre éthique pour l'utilisation de l'intelligence artificielle par les tribunaux est donc clairement apparue et, par conséquent, le CCBE soutient l'initiative de la Commission européenne pour l'efficacité de la justice du Conseil de l'Europe (CEPEJ) qui a adopté une *Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement*[5].

Cependant, la réflexion éthique ne suffira pas à elle seule, et il est également nécessaire d'identifier les principes opérationnels effectifs et contraignants qui peuvent régir, en pratique, l'utilisation des outils d'intelligence artificielle par les tribunaux. En particulier, l'utilisation des outils d'intelligence artificielle doit être conciliée avec les principes fondamentaux qui régissent les procédures judiciaires et garantissent un procès équitable : égalité des armes, impartialité, procédures contradictoires, etc. Même si la tentation de tout sacrifier à l'efficacité peut être présente, ces droits fondamentaux doivent rester garantis à tous les justiciables.

Tableau : Identification des utilisations possibles de l'intelligence artificielle dans les systèmes judiciaires et dangers imminents pour les droits fondamentaux et l'état de droit

[5] Voir la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement, adoptée par la CEPEJ lors de sa réunion plénière des 3 et 4 décembre 2018, et disponible en ligne à l'adresse suivante : https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b

Use of AI by Courts					
Stages	**Management of cases**	**Pre-trial**	**Trial**	**Judges' deliberation/ decision-making**	**Post sentencing**
(Potential) AI applications	- Case management system - Electronic communications - Digital platforms accessible for lawyers/clients - Automatic monitoring of procedures - Automatic system for monitoring procedural delays - Automatic system for completing procedural formalities - Automatic decisions on the progress of the case - Queue management - Automatic sorting of appeals	- Plea-bargaining: Prosecutor's databases	- Use of videoconference - Automated transcription / automated translation - Automated presentation of file's document on screens during hearings - Case management (in a situation of complex cases) - Use of emotional AI (detection of emotions, etc....)	- Case law tools - Prediction technology - Legal researches and analysis / autonomous researches - Scoring of risks / assessment of the suspect (probability of recidivism) - Automated judgments (decision trees) - Writing assistance tools and drafting judgments - Decision making systems - Intelligence assistant systems (identification of patterns, analysis of data...)	- Scoring of risks / probability of recidivism / parole opportunities
Main principles and issues to be taken into account					
Principles	- Adversarial proceedings - Rule of law, due process, security - No restriction of access to justice - Equality of arms - Transparency of decision-making - Access to data by lawyers	- Adversarial proceedings - Equality of arms - Access to data by lawyers - Data protection and compatibility with fundamental rights	- Adversarial proceedings - Fair trial - Transparency - Neutrality (in profiling) - No use of emotional AI when videos are used during a trial	- Adversarial proceedings - Fair trial - Transparency about use of AI by judge - Transparency of decision-making process - Algorithms and accountability - Liability if errors occur - Access to evidence - Right to request for a human intervention (judge)	- Adversarial proceedings - Fair trial - Transparency of decision-making process - Algorithms and accountability - Right to appeal

Principales préoccupations

Le tableau ci-dessus montre que l'on peut imaginer l'utilisation d'outils d'intelligence artificielle dans la gestion du suivi des dossiers, pendant les audiences (en cours de procès ou pendant l'instruction), pour faciliter la prise de décision du juge (la phase de délibération) et dans le suivi de l'exécution des décisions.

Il indique également les principes qui pourraient être affectés par l'utilisation des outils d'intelligence artificielle en raison d'une multitude de réalités négatives qui pourraient se produire, par exemple :

- l'utilisation de données et d'éléments qui n'ont pas fait l'objet d'un débat contradictoire ;
- l'exploitation de conclusions (même partielles) qui n'ont pas été obtenues par le raisonnement du juge ;
- le manque de transparence du processus, puisqu'il devient impossible de savoir ce qui doit être attribué au juge et ce qui provient d'une machine ;
- le manque de conditions équitables (égalité des armes) ;
- l'affaiblissement du principe d'impartialité en raison de l'impossibilité de neutraliser et de connaître les préjugés des concepteurs du système ;
- la violation du principe d'explicabilité, en raison de l'existence de résultats qui dépassent le raisonnement humain et ne peuvent pas être retracés.

L'utilisation d'outils d'intelligence artificielle par les tribunaux pourrait donc gravement compromettre l'architecture procédurale actuelle qui sous-tend les procédures judiciaires, d'autant plus s'il est accepté que le juge y accède seul pendant le processus de délibération.

L'architecture générale actuelle d'un procès s'explique par la nécessité de garantir le respect d'un certain nombre de principes et de produire des décisions prises par le juge lui-même, à la lumière des arguments et des preuves fournis par les parties. Le juge est impartial et ses décisions contiennent des explications qui permettent de comprendre quelles dispositions légales et quels précédents peuvent les justifier.

Règles et principes opérationnels

Il est donc important que les outils d'intelligence artificielle soient correctement adaptés à l'environnement judiciaire en tenant compte des principes et de l'architecture procédurale qui sous-tendent les procédures. Avant que les outils d'intelligence artificielle ne soient mis en œuvre dans les systèmes judiciaires, il convient de définir et d'adopter un ensemble de règles et de principes régissant l'utilisation de l'intelligence artificielle. Les garanties minimales suivantes doivent tout particulièrement être respectées :

- **La possibilité d'identifier l'utilisation de l'intelligence artificielle** : toutes les parties impliquées dans une procédure judiciaire devraient toujours être en mesure d'identifier, lors d'une décision judiciaire, les éléments résultant de la mise en œuvre d'un outil d'intelligence artificielle.
- **La non-délégation du pouvoir de décision du juge** : en aucun cas le juge ne doit déléguer tout ou partie de son pouvoir de décision à un outil d'intelligence artificielle. En tout état de cause, le **droit à un juge naturel** doit être garanti à toutes les étapes de la procédure.
- **La possibilité pour les parties de vérifier la saisie des données et le raisonnement de l'outil d'intelligence artificielle**.
- **La possibilité pour les parties de discuter et de contester les résultats de l'intelligence artificielle de** manière contradictoire en dehors de la phase de délibération et avec un délai raisonnable.
- **Le respect des principes du RGPD**.
- **La neutralité et l'objectivité des outils d'intelligence artificielle** utilisés par le système judiciaire doivent être garanties et vérifiables.

Tel que cela a été démontré ci-dessus, il reste encore fort à faire pour évaluer de manière critique le rôle que les outils d'intelligence artificielle doivent jouer, le cas échéant, dans nos systèmes judiciaires. Le changement devrait être adopté là où il améliore ou du moins ne détériore pas la qualité des systèmes judiciaires. Les droits fondamentaux et le respect des normes éthiques qui sous-tendent les institutions fondées sur l'état de droit ne peuvent toutefois pas être subordonnés à de simples gains d'efficacité ou à des réductions de coûts, que ce soit pour les utilisateurs des tribunaux ou les autorités judiciaires.

Tout déploiement de ces outils devrait donc être **strictement réglementé et être précédé d'une évaluation et d'analyses d'impact approfondies** avec la participation de tous les acteurs et parties prenantes concernés.

C. Applications de l'intelligence artificielle à haut risque : l'utilisation de l'intelligence artificielle dans les systèmes de justice pénale

Une partie du travail des forces de police dans la **prévention des crimes**, y compris toutes les formes de surveillance technique telles que l'**interception, la collecte et l'analyse de données** (texte, audio ou vidéo) et l'**analyse de preuves physiques** (échantillons d'ADN, cybercriminalité, déclarations de témoins, etc.) pourrait, d'un point de vue technique, s'appuyer sur l'intelligence artificielle. Diverses questions se posent dès lors, par exemple, les **préjugés** inhérents aux outils utilisés pour prédire la criminalité ou évaluer le risque de récidive et les outils tels que la **technologie de reconnaissance faciale**, qui ne permettent pas d'identifier avec précision les personnes d'ethnicités différentes. Ces formes de discrimination constituent une menace pour les droits des citoyens. En outre, le recours à l'intelligence artificielle dans le domaine de l'**informatique légale** et de l'**évaluation des risques de**

récidive se heurte à des difficultés étant donné que les modes de fonctionnement spécifiques des algorithmes ne sont généralement pas divulgués aux personnes concernées par le résultat de leur utilisation. Le défendeur ne peut donc pas contester les prédictions faites par les algorithmes. Une autre source d'inquiétude concerne l'**inégalité des armes** qui peut survenir entre les capacités plus avancées dont les procureurs peuvent disposer et les ressources plus limitées à la portée des avocats.

Le CCBE estime que l'utilisation de **systèmes d'identification biométrique (par exemple la reconnaissance faciale) dans les espaces accessibles au public** ne devrait pas avoir lieu tant que ne sont pas en place des lignes directrices ou une législation spécifiques à l'échelle de l'UE qui soient pleinement conformes à la Charte des droits fondamentaux de l'Union européenne et à la Convention européenne des droits de l'homme, y compris la jurisprudence pertinente.

L'identification biométrique a tendance à présenter de graves défauts qui mettent en danger les droits des citoyens. De nombreuses études ont démontré que la technologie de reconnaissance faciale est inexacte dans l'identification de personnes ethniquement différentes. Par ailleurs, il est très préoccupant que les mots déclencheurs utilisés par les agences de sécurité nationale ne soient pas suffisamment affinés et que les conversations téléphoniques et la correspondance électronique de millions de personnes soient ainsi surveillées sans fondement juridique.

En outre, l'utilisation généralisée des systèmes d'identification biométrique peut présenter des risques graves pour une société ouverte et pluraliste si elle n'est pas utilisée proportionnellement à l'objectif visé, tel que celui d'assurer la sécurité publique. Dans de nombreuses situations, l'anonymat est la plus grande protection de la liberté, et les techniques d'identification biométrique qui couvrent de vastes zones d'espace public mettent en danger cette liberté. Plus elles sont précises et plus leur utilisation est répandue, plus elles deviennent dangereuses.

Par conséquent, en ce qui concerne l'utilisation des outils d'intelligence artificielle dans les systèmes de justice pénale, la plupart des règles et principes énoncés ci-dessus aux points I et II.B s'appliqueront également. Tout déploiement de ces outils doit donc être **strictement réglementé et être précédé d'une évaluation et d'analyses d'impact approfondies** avec la participation de tous les acteurs et parties prenantes concernés.

D. Exigences obligatoires d'un éventuel cadre réglementaire

Le CCBE convient que les exigences obligatoires suivantes sont importantes pour l'établissement d'un futur cadre réglementaire pour l'intelligence artificielle :

- **la qualité des ensembles de données sur la formation ;**
- **la tenue des registres et des données ;**
- **l'information sur l'objectif et la nature des systèmes d'intelligence artificielle ;**
- **la robustesse et la précision des systèmes d'intelligence artificielle ;**
- **le contrôle humain ;**
- **des règles claires en matière de responsabilité et de sécurité.**

En outre, le CCBE précise également que l'exigence d'**explicabilité** est particulièrement importante dans l'environnement de la justice, c'est-à-dire la capacité à expliquer à la fois les processus techniques d'un système d'intelligence artificielle et les décisions humaines qui s'y rapportent.

Comme indiqué ci-dessus au point II.A, il est important que les exigences prévues par la loi soient adaptées aux besoins de secteurs et de circonstances spécifiques.

E. Cadre de conformité

Quant à savoir **comment garantir que l'intelligence artificielle est digne de confiance, sûre et respectueuse des valeurs et règles européennes,** le CCBE estime qu'une combinaison de **mécanismes de conformité au préalable et de mise en œuvre ultérieure** est nécessaire.

Toutefois, au lieu d'adhérer à un cadre de conformité très générique et abstrait, il est nécessaire d'envisager les mesures de conformité appropriées et les adapter aux besoins de secteurs et de circonstances spécifiques. Les destinataires du cadre de conformité dépendront donc également du domaine exact visé par les mesures de conformité et différeront.

Il est également important de veiller à ce que les outils d'intelligence artificielle ne soient pas déployés, en particulier dans le secteur public, sans en avoir préalablement défini le cadre de conformité.

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

I. Nécessité de modifier le cadre législatif actuel de l'UE en matière de responsabilité

En abordant la question du modèle de responsabilité juridique des systèmes d'intelligence artificielle, il peut être tentant de dire que le droit est déjà bien développé, notamment en ce qui concerne la responsabilité du fait des produits défectueux ainsi que d'autres régimes de responsabilité juridique en vigueur dans les États membres, et qu'il suffit de l'appliquer pour protéger les victimes potentielles. D'autre part, l'intelligence artificielle étant un phénomène nouveau, d'aucuns pourraient vouloir réinventer le droit de la responsabilité pour traiter les questions qu'elle pose.

L'examen des modèles de responsabilité juridique existants permet de dégager quelques approches possibles pour traiter la question de la responsabilité civile en matière d'intelligence artificielle : 1) un système de responsabilité reposant sur le concept de faute ou 2) un système de responsabilité stricte. À l'intérieur de ces grandes catégories, il peut y avoir des possibilités d'approches différentes. Par exemple, en ce qui concerne ce deuxième, le système pourrait être soit un régime de responsabilité stricte pure (où la responsabilité est engagée qu'il y ait ou non un défaut et où aucun moyen de défense permettant d'exclure ou de réduire la responsabilité n'est autorisé) soit un système de responsabilité stricte qui autorise plusieurs moyens de défense, sur le modèle de la directive 85/374/CEE[6] (directive européenne sur la responsabilité du fait des produits défectueux). De plus, d'autres régimes de responsabilité pourraient être envisagés dans le contexte de l'intelligence artificielle. Par exemple, le rapport du groupe d'experts mentionne la responsabilité indirecte (responsabilité découlant des actions d'autrui) en ce qui concerne les technologies autonomes. En outre, la responsabilité contractuelle ou d'autres régimes d'indemnisation pourraient être appliqués dans certains écosystèmes numériques parallèlement ou à la place de la responsabilité délictuelle[7].

Les approches semblent différer sensiblement quant au meilleur régime pour traiter cette question de la responsabilité en matière d'intelligence artificielle ainsi que la décision politique qui devrait être adoptée à cet égard. Malgré l'approche adoptée, il est clair que certaines modifications importantes devront être apportées au cadre législatif actuel, compte tenu des différences fondamentales qui existent entre les produits traditionnels et l'intelligence artificielle, notamment en ce qui concerne les notions de produit, de faute et de défaut. Les questions consistant à savoir qui pourrait être concerné

---

6 Directive 85/374/CEE du Conseil du 25 juillet 1985 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de responsabilité du fait des produits défectueux.

7 Commission européenne : Rapport du groupe d'experts sur la responsabilité juridique et les nouvelles technologies New Technologies Formation : Liability for Artificial Intelligence and Other Emerging Digital Technologies, pp.36-37.

par la responsabilité, ainsi que la charge de la preuve et les moyens de défense doivent également être réexaminées.

Le CCBE privilégie un instrument séparé sur les questions de responsabilité en matière d'intelligence artificielle plutôt qu'une modification de la directive en matière de responsabilité du fait des produits défectueux qui est reconnue comme efficace en ce qui concerne les produits traditionnels. Tenter d'introduire des mesures supplémentaires dans la directive en matière de responsabilité du fait des produits défectueux afin de faire face à l'intelligence artificielle aurait nécessairement un effet négatif sur le processus de recherche et de développement d'autres produits, ce qui n'est pas souhaitable. Tout produit d'intelligence artificielle relevant actuellement de la directive en matière de responsabilité du fait des produits défectueux devrait alors être retiré du champ d'application de la directive et être intégré dans le champ d'application de la nouvelle directive.

Cependant, la Commission semble seulement envisager, du moins pour le moment, les modifications qui pourraient devoir être apportées aux instruments de l'UE *existants,* notamment à la directive en matière de responsabilité du fait des produits défectueux, ainsi qu'aux régimes nationaux de responsabilité, et non la possibilité de créer un instrument. En tout état de cause, le CCBE estime que des aspects tels que l'indemnisation des dommages et l'attribution de la responsabilité, ainsi que les règles relatives à la charge de la preuve, doivent être réglementés au niveau de l'UE. Une autre approche pourrait conduire à une situation où les réglementations nationales adaptées différeraient sensiblement entre les États membres.

Plus précisément, la Commission européenne doit prendre en compte les observations suivantes :

II. Questions à prendre en considération lors de la modification du cadre législatif actuel

A. Notion de produit

Tel que déjà mentionné ci-dessus, il existe des différences fondamentales entre les produits traditionnels et l'intelligence artificielle. Premièrement, en ce qui concerne la notion de produit, il est nécessaire de garder à l'esprit que les systèmes d'intelligence artificielle sont de plus en plus utilisés, à la fois comme systèmes autonomes (qui peuvent fonctionner sur des ordinateurs ordinaires) et comme éléments de produits plus complexes. Le logiciel de diagnostic médical utilisé pour analyser les scanners de dépistage précoce du cancer et les véhicules autonomes en sont des exemples.

Le CCBE estime que l'intelligence artificielle doit être définie de manière exhaustive dans le nouvel instrument législatif.

B. Manque de prévisibilité dans le fonctionnement des systèmes d'intelligence artificielle : répercussions sur les notions de faute et de défaut

Deuxièmement, l'attribut d'auto-apprentissage et de prise de décision autonome dans les systèmes d'intelligence artificielle milite contre l'utilisation du raisonnement juridique traditionnel reposant sur le concept de « prévisibilité » comme fondement de responsabilité juridique. Dans ce contexte, un système d'intelligence artificielle peut causer des dommages soit à la suite d'un « défaut » traditionnel dans le logiciel par exemple, soit à la suite de ses « propres » actions déterminées par les données et les algorithmes, sans aucun « défaut » au sens traditionnel. Ainsi, la responsabilité des dommages ne peut pas être facilement attribuée à une « faute » de la part d'une personne (physique ou morale) ni à l'existence d'un défaut dans un produit, au sens d'un dysfonctionnement spécifique de ce produit.

Dans ces conditions, il serait possible de dire que la responsabilité des actions entreprises par un système d'intelligence artificielle ne doit pas nécessairement être liée à la notion de faute (dans son

sens traditionnel) ni de « défaut » (dans son sens traditionnel). Il convient de noter que la directive européenne existante sur la responsabilité du fait des produits défectueux, bien que fondée sur l'existence d'un « défaut », définit le « défaut » non pas dans le sens traditionnel, mais en fonction du résultat, c'est-à-dire « Un produit est défectueux lorsqu'il n'offre pas la sécurité à laquelle on peut légitimement s'attendre compte tenu de toutes les circonstances » (article 6, paragraphe 1).

C. Destinataire de la responsabilité

Troisièmement, il convient de se demander qui la responsabilité juridique pourrait concerner. Cette tâche peut s'avérer difficile étant donné l'opacité des systèmes d'intelligence artificielle et compte tenu de la multiplicité des personnes potentiellement impliquées, éventuellement dans plusieurs juridictions et, dans le cas de certaines personnes, il se peut qu'elles ne sachent pas que leur travail sera ensuite utilisé dans un système d'intelligence artificielle.
Il existe plusieurs possibilités d'identifier les différents acteurs auxquels la responsabilité juridique pourrait être attribuée. À titre d'exemple, le rapport du groupe d'experts suggère que non seulement le *producteur*, mais également l'*opérateur* devraient être tenus responsables, selon les circonstances[8].

L'introduction de la notion d'« opérateur » comme étant la « personne qui maîtrise le risque lié à l'exploitation de l'intelligence artificielle et qui bénéficie de son exploitation » doit être saluée à cet égard, avec une distinction entre opérateur frontal et opérateur dorsal. Ces opérateurs, ainsi que les producteurs, devraient se conformer à des obligations spécifiques de diligence, ce qui entraînerait une responsabilité juridique en cas de non-respect de ces obligations.

D. Défenses

Si le législateur européen instaure un régime de responsabilité stricte pour les produits d'intelligence artificielle, ce qui signifie que chaque fois que l'intelligence artificielle a causé un dommage, le destinataire de la responsabilité de cette intelligence artificielle doit être tenu de répondre du dommage, il convient d'examiner en détail les défenses nécessaires à apporter.

Les défenses spécifiques actuellement prévues dans la directive en matière de responsabilité du fait des produits défectueux devraient toutefois être reconsidérés. En particulier, les exceptions prévues à l'article 7 b) (l'absence d'existence du défaut au moment où le produit a été mis en circulation) et e) (la défense fondée sur l'état des connaissances techniques) doivent être rejetées en ce qui concerne l'intelligence artificielle. Le CCBE approuve à ce sujet la considération exprimée dans le rapport du groupe d'experts selon laquelle une défense fondée sur le risque de développement ne devrait pas s'appliquer dans le contexte des technologies numériques émergentes : le producteur doit être strictement responsable des défauts même si ceux-ci apparaissent après la mise en circulation du produit, tant que le producteur contrôle encore les mises à jour ou les mises à niveau de la technologie[9].

E. Types de dommages et victimes

En ce qui concerne les dommages, il est nécessaire de considérer non seulement les dommages physiques et matériels mais également la destruction des données de la victime comme dommages indemnisables dans des conditions spécifiques.

---

8 Commission européenne : Rapport du groupe d'experts sur la responsabilité juridique et les nouvelles technologies – New Technologies Formation : Liability for Artificial Intelligence and Other Emerging Digital Technologies, pp. 39-46.

9 Commission européenne : Rapport du groupe d'experts sur la responsabilité juridique et les nouvelles technologies – New Technologies Formation : Liability for Artificial Intelligence and Other Emerging Digital Technologies, p. 6.

Les risques et les dommages inhérents pouvant être causés par l'intelligence artificielle n'étant pas prévisibles en tant que tels, les dommages couverts ne doivent pas se limiter aux dommages prévisibles. Le lien de causalité doit être pris en compte. En outre, les systèmes d'intelligence artificielle étant en constante évolution, il ne doit pas y avoir de limitation de responsabilité concernant les dommages lorsqu'il est prouvé qu'elle était prévisible, pour autant que, dans tous les cas, l'utilisation faite de l'intelligence artificielle soit raisonnable et qu'il soit prouvé que la perte a été causée par cette utilisation de l'intelligence artificielle (selon les règles en matière de preuve expliquées ci-dessous).

Toutes les personnes ayant subi une perte (qu'il s'agisse de personnes physiques ou morales) doivent pouvoir demander une indemnisation sans restriction aux consommateurs et aux professionnels par exemple ou à ceux qui utilisent l'intelligence artificielle dans le cadre de leur activité professionnelle.

F. Règle de preuve et renversement de la charge de la preuve dans certaines situations

Les questions relatives à la charge de la preuve doivent également être réexaminées dans le contexte des systèmes d'intelligence artificielle étant donné que l'auto-apprentissage et les caractéristiques d'apprentissage approfondi de l'intelligence artificielle entraîneront nécessairement une diminution de la prévisibilité. Les liens de cause à effet entre le comportement des entrées et celui du système peuvent être difficiles à élucider[10]. Dans ces conditions, il est impossible d'attendre que la victime fournisse toujours des preuves des dysfonctionnements internes qui ont entraîné les dommages.

Les victimes doivent avoir droit à une facilitation de la preuve dans les situations où les difficultés à prouver l'existence d'un élément de responsabilité sont disproportionnées, allant au-delà de ce qui devrait raisonnablement être attendu. Dans certains cas, le renversement de la charge de la preuve peut être approprié, par exemple en l'absence d'informations enregistrées sur la technologie d'exploitation (enregistrement de conception) ou en l'absence d'un accès raisonnable de la victime à ces informations.

Lorsque plusieurs personnes ont coopéré à la création d'une unité d'intelligence artificielle et que la victime ne peut pas prouver quelle personne précisément a créé l'élément à l'origine du dommage, ces règles de facilitation doivent également pouvoir conduire à une responsabilité conjointe de ces personnes envers la victime. Les recours entre les auteurs des préjudices doivent être rendus possibles.

G. Question de l'assurance obligatoire

Enfin, l'assurance responsabilité civile obligatoire pourrait être considérée comme une solution pour donner aux victimes un meilleur accès à l'indemnisation dans les situations exposant les tiers à un risque accru de préjudice et pourrait également protéger les auteurs potentiels du risque de responsabilité juridique[11]. Lors de l'examen de cette possibilité, des questions plus larges de politique socio-économique peuvent également devoir être prises en compte : par exemple, l'opportunité perçue de garantir, d'une part, qu'aucune personne subissant des pertes du fait de l'utilisation d'un système d'intelligence artificielle ne soit privée d'indemnisation et, d'autre part, la crainte qu'il puisse y avoir un effet paralysant sur l'innovation ou une ingérence indésirable dans les relations entre entreprises.

---

[10] Herbert Zech, Liability for autonomous systems: Tackling specific risks of modern IT ; « Des voitures autonomes - Une offre de loi », essai, juillet 2018, n°02.226

[11] Commission européenne : Rapport du groupe d'experts sur la responsabilité juridique et les nouvelles technologies – New Technologies Formation : Liability for Artificial Intelligence and Other Emerging Digital Technologies, pp. 61-62.

En outre, il convient de tenir compte d'autres facteurs dans le cadre d'un régime d'assurance obligatoire. Par exemple, en ce qui concerne la question de savoir quels acteurs devraient être obligés de souscrire une telle assurance, il peut arriver que le nombre de personnes ayant contribué (à des moments et des degrés divers) à un système d'intelligence artificielle soit très important. Les risques potentiels des systèmes d'intelligence artificielle peuvent également être très différents selon les secteurs dans lesquels le système d'intelligence artificielle est utilisé.

Le CCBE invite donc la Commission à examiner attentivement toutes ces questions et à peser les avantages et les inconvénients de ces possibilités.

ANNEXE - Projet de réponse du CCBE au questionnaire de la consultation sur l'intelligence artificielle

ANNEXE - Projet de réponse du CCBE au questionnaire de la consultation sur l'intelligence artificielle

Consultation sur le Livre blanc sur l'intelligence artificielle — Une approche européenne

Les champs marqués d'un * sont obligatoires.

Introduction

L'intelligence artificielle (IA) est une technologie stratégique qui offre de nombreux avantages pour les citoyens et pour l'économie. Elle va entraîner des changements dans nos vies en améliorant les soins de santé (précision accrue des diagnostics ou meilleure prévention des maladies, par exemple), en rendant l' agriculture plus efficiente, en contribuant à l'adaptation au changement climatique et à l'atténuation de ses effets, en augmentant l'efficacité des systèmes de production par la maintenance prédictive, en renforçant la sécurité des Européens et la protection des travailleurs, et de bien d'autres façons que nous commençons à peine à entrevoir.

Toutefois, l'IA s'accompagne aussi d'un certain nombre de risques potentiels, tels que les risques pour la sécurité, la discrimination fondée sur le sexe ou sur d'autres motifs, l'opacité de la prise de décisions ou l'intrusion dans nos vies privées.

L'approche européenne en matière d'IA vise à promouvoir les capacités d'innovation de l'Europe dans le domaine de l'IA tout en soutenant le développement et l'adoption d'une IA éthique et digne de confiance dans toute l'UE. Selon cette approche, l'IA devrait être au service des citoyens et constituer un atout pour la société.

Pour que l'Europe puisse tirer pleinement parti des possibilités offertes par l'IA, elle doit développer les capacités industrielles et technologiques dont elle a besoin et les renforcer. Comme indiqué dans la stratégie européenne pour les données, qui accompagne le Livre blanc, elle doit également prendre des mesures qui lui permettront de devenir un pôle mondial de données.

La consultation publique actuelle va de pair avec le **Livre blanc sur l'intelligence artificielle — Une approche européenne**, qui vise à promouvoir un écosystème européen d'excellence et de confiance dans l'IA, et avec un rapport sur les aspects de l'IA liés à la sécurité et à la responsabilité. Le Livre blanc propose:

- des mesures qui permettront de rationaliser la recherche, d'encourager la collaboration entre les États membres et d'accroître les investissements dans le développement et le déploiement de l'IA;
- des options pour un futur cadre réglementaire de l'UE qui définirait les types d'exigences légales applicables aux acteurs concernés, en mettant particulièrement l'accent sur les applications à haut risque.

La présente consultation permet à tous les citoyens européens, aux États membres et aux parties prenantes concernées (y compris la société civile, le secteur industriel et le milieu universitaire) de faire connaître leur point de vue sur le Livre blanc et de contribuer à une approche européenne en matière d'IA.

À cette fin, le questionnaire ci-dessous est divisé en trois sections :

- **la section 1** renvoie aux actions spécifiques proposées dans le chapitre 4 du Livre blanc pour la construction d'un écosystème d'excellence capable de soutenir le développement et de favoriser l'adoption de l'IA dans l'ensemble de l'économie et de l'administration publique de l'UE;
- **la section 2** renvoie à une série d'options en vue d'un cadre réglementaire pour l'IA, défini dans le chapitre 5 du Livre blanc;
- **la section 3** renvoie au rapport sur les aspects de l'IA liés à la sécurité et à la responsabilité.

Les répondants peuvent donner leur avis en choisissant la réponse la plus appropriée parmi les réponses proposées pour chaque question, ou en exposant leurs propres idées dans des encadrés spécifiques. Les commentaires peuvent également être fournis sous la forme d'un document (par exemple, un document de prise de position) qui peut être téléchargé au moyen du bouton disponible à la fin du questionnaire.

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	○	○	○	○	○	●
Cibler les efforts de la communauté de la recherche et de l'innovation	○	○	○	○	○	●
Compétences	○	○	○	●	○	○
Accorder une place de choix aux PME	○	○	○	●	○	○
Partenariat avec le secteur privé	○	○	○	○	○	●
Encourager le secteur public à adopter l'IA	○	○	●	○	○	○

D'autres actions devraient-elles être envisagées ?

Le CCBE soutient pleinement l'idée que le financement à échelle européenne soit mis à la disposition des régulateurs sectoriels (y compris les barreaux) étant donné qu'ils sont les mieux placés pour répondre aux besoins de formation de leur secteur respectif (tels que les avocats), notamment en ce qui concerne la manière dont l'intelligence artificielle peut être utilisée dans le respect de leurs codes de déontologie.
L'interaction entre tous les secteurs, privés et publics, est cruciale pour garantir que les valeurs éthiques soient intégrées dans les systèmes d'intelligence artificielle eux-mêmes.
Veuillez consulter la réponse séparée du CCBE.

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	○	○	○	○	○	●
Établir des centres d'essai constituant une référence mondiale pour l'IA	○	○	○	○	○	●
Encourager le secteur public à adopter l'IA	○	○	○	○	○	●
Accroître le financement des start-ups innovantes dans le domaine de l'IA	○	○	○	○	○	●
Développer les compétences en matière d'IA et adapter les programmes de formation existants	○	○	○	○	○	●
Construire l'espace européen des données	○	○	○	○	○	●

D'autres domaines devraient-ils être envisagés ?

500 caractère(s) maximum

<u>Une communauté de la recherche et de l'innovation unie et renforcée qui vise l'excellence</u>

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	○	○	○	○	○	●
Créer un réseau des centres d'excellence existants dans le domaine de la recherche en IA	○	○	○	○	○	●
Mettre en place un partenariat public-privé pour la recherche industrielle	○	○	○	○	○	●

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

500 caractère(s) maximum

Une attention particulière pour les petites et moyennes entreprises (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	○	○	○	○	●	○
Donner accès aux centres d' essai et de référence	○	○	○	○	●	○
Promouvoir le transfert de connaissances et soutenir le développement de l'expertise en matière d'IA pour les PME	○	○	○	●	○	○
Soutenir des partenariats entre les PME, les grandes entreprises et les universités autour de projets d'IA	○	○	○	○	○	●
Fournir des informations sur le financement en fonds propres pour les start-ups dans le domaine de l'IA	○	○	○	○	○	●

[Ces points sont expliqués plus en détail dans le document séparé du CCBE joint à la réponse à cette consultation.]

Y a-t-il d'autres tâches que vous jugez importantes pour les pôles d'innovation numérique spécialisés ?

500 caractère(s) maximum

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	○	○	○	○	●	○
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.)	○	○	○	○	●	○
L'utilisation de l'IA peut entraîner des résultats discriminatoires	○	○	○	○	●	○
L'IA peut prendre des mesures dont les motifs ne peuvent pas être expliqués	○	○	○	○	●	○
Il peut être plus difficile pour les personnes ayant subi un préjudice du fait de l'utilisation de l'IA d'obtenir réparation	○	○	○	○	●	○
L'IA n'est pas toujours exacte	○	○	○	○	●	○

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

500 caractère(s) maximum

- ***L'intelligence artificielle peut conduire à des résultats injustes et juridiquement contraignants***
- ***L'intelligence artificielle peut entraver l'accès à la justice***
- ***L'intelligence artificielle risque de porter atteinte au droit à un procès équitable***

En général, le recours à l'intelligence artificielle dans les processus décisionnels automatisés peut remodeler l'interaction entre les citoyens et les décideurs publics ou privés, ce qui peut nuire à la capacité des citoyens à demander des conseils, à contester ou à tenter de renverser des décisions. Il convient donc de garantir des mécanismes de recours solides ainsi qu'une implication étroite des acteurs qui ont une fonction de protection des droits des citoyens (les avocats et les juges par exemple).

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 ?

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

Autre (veuillez préciser) :

500 caractère(s) maximum

Dans certains domaines, une nouvelle législation pourrait s'avérer nécessaire, contrairement à d'autres, ou alors seules des clarifications supplémentaires sont nécessaires quant à la manière dont les règles existantes s'appliquent aux nouvelles circonstances résultant du recours à l'intelligence artificielle. Veuillez consulter la réponse séparée du CCBE pour obtenir plus d'informations.

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
- ○ Autre
- ○ Sans avis

Autre (veuillez préciser) :

500 caractère(s) maximum

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
- ● Autre
- ○ Sans avis

Autre (veuillez préciser) :

500 caractère(s) maximum

Non. Le CCBE craint qu'un exercice de catégorisation des risques comme « élevés » ou « faibles » selon des critères abstraits soit trop simpliste et conduise à une réglementation structurellement défectueuse. Une approche plus ciblée est nécessaire. Il n'est pas approprié d'accorder le même traitement juridique à des choses qui sont techniquement différentes, par exemple l'intelligence artificielle, l'internet des objets et d'autres technologies numériques, même si elles partagent parfois des caractéristiques communes. Une approche plus ciblée est nécessaire (voir le document du CCBE ci-joint).

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 ») :

500 caractère(s) maximum

- ***L'utilisation des outils d'intelligence artificielle par les tribunaux à différentes phases, c'est-à-dire avant le procès, pendant le procès, pendant les délibérations et la prise de décision, et après la condamnation.***
- ***L'utilisation des outils d'intelligence artificielle à des fins répressives.***

Pour plus d'explications, il est fait référence au document séparé du CCBE joint à la réponse de cette consultation.

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	○	○	○	○	●	○
Conservation des dossiers et des données	○	○	○	○	●	○
Informations sur la finalité et la nature des systèmes d'IA	○	○	○	○	●	○
Robustesse et précision des systèmes d'IA	○	○	○	○	●	○
Contrôle humain	○	○	○	○	●	○
Règles claires en matière de sécurité et de responsabilité	○	○	○	○	●	○

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 :

Les systèmes d'identification biométrique ont tendance à présenter de graves défauts qui mettent en danger les droits des citoyens. De nombreuses études ont démontré que la technologie de reconnaissance faciale est inexacte dans l'identification de personnes ethniquement différentes. Par ailleurs, il est très préoccupant que les mots déclencheurs utilisés par les agences de sécurité nationale ne soient pas suffisamment affinés et que les conversations téléphoniques et la correspondance électronique de millions de personnes soient ainsi surveillées sans fondement juridique.

En outre, l'utilisation généralisée de la reconnaissance faciale peut présenter des risques graves pour une société ouverte et pluraliste si elle n'est pas utilisée proportionnellement à l'objectif visé, tel que celui d'assurer la sécurité publique. Dans de nombreuses situations, l'anonymat est la plus grande protection de la liberté, et les techniques de reconnaissance faciale qui couvrent de vastes zones d'espace public mettent en danger cette liberté. Plus elles sont précises et plus leur utilisation est répandue, plus elles deviennent dangereuses.

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 ?

500 caractère(s) maximum

Quel est le meilleur 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

Veuillez préciser tout autre système de contrôle du respect

500 caractère(s) maximum

Avez-vous d'autres suggestions sur l'évaluation de la conformité ?

500 caractère(s) maximum

Au lieu d'adhérer à un cadre de conformité très générique et abstrait, il est nécessaire d’envisager les mesures de conformité appropriées et les adapter aux besoins de secteurs et de circonstances spécifiques.

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 ?

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

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

500 caractère(s) maximum

Oui, d'autres risques sont à prendre en compte en ce qui concerne l'utilisation de l'intelligence artificielle dans la justice. Les outils d'intelligence artificielle doivent être correctement adaptés à l'environnement judiciaire en tenant compte des principes et de l'architecture procédurale qui sous-tendent les procédures (voir la réponse séparée du CCBE).

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

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

500 caractère(s) maximum

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 ?

500 caractère(s) maximum

Le cadre législatif actuel doit être modifié compte tenu des différences fondamentales qui existent entre les produits traditionnels et l'intelligence artificielle, notamment en ce qui concerne les notions de produit, de faute et de défaut. Les questions consistant à savoir qui pourrait être concerné par la responsabilité, ainsi que la charge de la preuve et les moyens de défense doivent également être réexaminées. Le CCBE privilégie toutefois un instrument séparé sur les questions de responsabilité en matière d'intelligence artificielle plutôt qu'une modification de la directive en matière de responsabilité du fait des produits défectueux qui est reconnue comme efficace en ce qui concerne les produits traditionnels.

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 :

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

500 caractère(s) maximum

Le CCBE n'est pas en mesure de se prononcer sur la manière dont les réglementations nationales actuelles concernant la responsabilité en matière d'indemnisation des dommages et d'attribution de la responsabilité devraient éventuellement être adaptées. Le CCBE est néanmoins convaincu que ces aspects, tels que les règles relatives à la charge de la preuve, doivent être réglementés au niveau de l'UE et intégrés dans une directive révisée en matière de responsabilité du fait des produits défectueux (ou au sein d'un instrument séparé). Une autre approche pourrait conduire à une situation où les réglementations nationales adaptées différeraient sensiblement entre les États membres.