Sur le contexte de cette contribution

Après avoir exposé ses orientations politiques en vue de *« promouvoir l'innovation européenne »*, votre Commission, sous l'égide de sa Présidente, Mme Ursula von der Leyen, a publié, le 20 février 2020, un Livre Blanc intitulé *« Intelligence artificielle : une approche européenne axée sur l'excellence et la confiance »*.

L'European Expertise & Expert Institute (EEEI) a souhaité répondre à la consultation que votre Commission a engagée auprès des différentes parties prenantes, et ce, en limitant son analyse à l'étude des sujets les plus susceptibles d'être étroitement liés au rôle ainsi qu'aux fonctions judiciaires ou non de l'Expert.

En effet, l'EEEI a pour objectif de contribuer, par ses travaux, à la convergence des systèmes nationaux d'expertise judiciaire en vue de garantir, dans tout l'espace judiciaire européen, la sécurité juridique et technique des décisions judiciaires par la qualité des expertises réalisées.

L'EEEI réunit en son sein des représentants des hautes juridictions, des barreaux, des compagnies d'experts, des professeurs d'université ainsi que d'autres personnalités ressortissantes de la plupart des États de l'Union, concernées par ces questions.

In fine, l'EEEI souligne qu'il est indépendant de toute « Autorité publique » comme de toute « Organisation privée », et en particulier être complètement indépendant de l'association Arborus dont les travaux seront mentionnés plus bas.

La présente contribution a été rédigée par un groupe de travail constitué par l'EEEI et dont on trouvera la liste des membres en fin de ce document.

Propos introductif

L'adaptation de l'économie mondiale aux capacités offertes par les outils numériques en général et les systèmes d'intelligence artificielle (IA) en particulier, transforme nos sociétés de façon profonde mais aussi insidieuse en soulevant des questions qui mettent en jeu les fondements mêmes de notre système de valeurs.

En effet, l'augmentation continue de la taille des réseaux, de la puissance de calcul des ordinateurs, l'arrivée de nouvelles technologies comme l'apprentissage automatique (en anglais « machine learning », la disponibilité de données en grande quantité accentuée par l'internet des objets, accélèrent la pénétration de l'IA dans des secteurs aussi divers que la santé, la défense, les transports, l'éducation, l'énergie, la justice, etc…

Plus particulièrement, les progrès fulgurants réalisés via l'auto-apprentissage permettent à une machine de construire de nouvelles connaissances à partir de sa propre expérience.

Néanmoins, la fiabilité des algorithmes qui fondent les décisions prises par ces systèmes à base d'IA est souvent hautement discutable (fragmentation, biais, discrimination, exclusion, etc.). Par définition un algorithme n'est qu'un modèle offrant une représentation simplifiée du réel.

En outre, pour « *les algorithmes issus du paradigme de réseaux de neurones artificiels, en particulier, de l'apprentissage profond (c'est-à-dire comptant plusieurs couches reliées de nœuds qui traitent des informations différentes et qui les agrègent ensuite)* » il est impossible pour les ingénieurs d'expliquer le résultat produit dans la mesure où, « *contrairement au système d'IA raisonnant de façon logico-déductive, il n'est pas possible d'extraire un arbre de décision clair et cohérent* ». [1]

Dès lors, comment accepter une décision si celle-ci n'est pas explicable, mesurable et prouvable ?

« *La logique de ces derniers* (les algorithmes) *a tendance à déporter la prise de décision vers les étapes techniques de conception d'un système »* [1]. Ceci va à l'encontre de l'impératif de rendre les algorithmes plus intelligibles et transparents.

Cela nous conduit à imaginer, à l'instar de ce que la réglementation européenne a déjà prévu en matière de protection des données à caractère personnel (RGPD) : la *« privacy by design* », que la gouvernance des algorithmes pourrait s'inscrire dans une démarche d'« *ethics by design* ». C'est donc un système de management qui devra être analysé aux regards de l'éthique et non un produit fini.

Rappelons que l'éthique est une volonté de responsabilisation qui ne saurait se réduire à la seule expression d'une conviction ou d'une opinion. Par ailleurs, relevons que l'éthique normative, et en particulier le conséquentialisme qui se distingue du droit et de la conformité, peut parfois remplir une fonction visant à évaluer la justesse des règles que celui-ci édicte. En outre, elle peut le préfigurer s'agissant, en particulier, de l'évaluation des risques.

Concernant cette évaluation, on dispose de méthodes et outils déjà bien éprouvés pour l'analyse des sûretés de fonctionnement et de maîtrise des risques liés aux systèmes complexes, dont l'IA n'est qu'un nouveau modèle de construction ; à cette réserve près, toutefois, que ces méthodes et outils s'appliquent à « des produits » et non à « des systèmes de management » comme c'est le cas, en l'espèce.

Ainsi, nous considérons que l'acceptabilité des systèmes à base d'IA, qui ne se fera qu'à des conditions qui permettront d'assurer la confiance **(I)**, suppose d'une part leur évaluation rigoureuse, notamment en élaborant des référentiels, des chartes, des labellisations et des certifications **(II)**, et d'autre part, la mise en place de mécanismes susceptibles d'établir une réelle graduation des risques afin, le cas échéant, de rapporter la preuve irréfragable de la chaîne de responsabilités **(III)**.

I – Établir la confiance

Sur les mécanismes fondant la confiance

La confiance accordée à un système par ses utilisateurs dépend essentiellement de leur perception de la maîtrise par son concepteur des risques inhérents à ce système.

Afin d'accroitre cette perception, le fournisseur du système peut mettre en œuvre différents procédés commerciaux de reconnaissance

- Adhérer spontanément à une charte, qui intègrera le plus souvent les principes généraux de respect des droits fondamentaux, de non-discrimination, de qualité et de sécurité, de transparence et de neutralité, de maîtrise par l'utilisateur et de contrôle humain, du respect de la vie privée, etc…
- Obtenir un label établi sur un référentiel proche d'une charte, sous le contrôle d'un organisme attribuant ce label selon des critères parfois plus ou moins transparents.
- Obtenir une certification, laquelle se fondera généralement sur un référentiel de même type que les précédents, cette fois estampillé par un organisme officiel de normalisation tel que l'ISO ; ce référentiel, ainsi doté d'un statut de « norme d'application volontaire », vient alors compléter les normes de droit que sont les lois et règlements ; l'organisme « certificateur » , pour pouvoir délivrer son certificat, devra lui-même se soumettre à un processus d'accréditation, se conformant à une autre norme d'application volontaire.

On relèvera que ces normes et certifications, d'évidence, génèrent de très lucratives activités pour ces organismes formateurs et certificateurs. A la question de la confiance dans le système se substitue alors celle de la confiance dans les procédés d'accréditation de ce système.

Quel niveau de confiance accorder à ces mécanismes de charte, label et certification ? Ces mécanismes n'offrent déjà qu'une garantie très relative en matière technique. Par exemple le Boeing 737 Max avait sa certification pour voler. En matière de cybersécurité, les entreprises certifiées ISO 27001 ne sont pas à l'abri de fuites de données et d'attaques par des hackers…. S'agissant d'engagements d'ordre éthique, les exemples ne sont pas rares de non-conformité ou de non-respect par des produits pourtant distribués par des entreprises labellisées ou certifiées. Cela provoque alors des scandales, parfois à l'échelle européenne, dont on citera, pour exemple, celui survenu en 2012 des « prothèses mammaires », celui en 2013 des « lasagnes à la viande de cheval », celui en 2015 des « moteurs diesel » ; les rappels les labels Bio qui prolifèrent, sans parler des contrefaçons de conformité sur des produits, où on appose un label sans aucun contrôle.

Quand les usagers, qu'ils soient citoyens ou organisations, voient trahie leur confiance fondée sur ces procédés, et cela sera aussi nécessairement le cas pour les systèmes à base d'IA, il leur reste le recours au droit et à la justice. Ainsi appelée en cas de manquement à la confiance, l'organisation juridique et judiciaire devra alors elle-même démontrer qu'elle est digne de

confiance : il lui faudra garantir aux justiciables qu'en cas de défaillance des mécanismes commerciaux de confiance, la justice saura établir les responsabilités.

Sur les critères applicables aux systèmes à base d'IA ?

La confiance est toujours une prédiction, un pari sur l'avenir avec une part réelle d'incertitude.

Comme l'indique le « Livre Blanc », une IA « digne de confiance » devrait être fondée sur les valeurs et règles européennes.

La législation européenne sur la protection des données, le respect de la vie privée ou la non-discrimination s'applique déjà aux systèmes à base d'IA. Compte tenu de leurs spécificités, faut-il y adjoindre une législation complémentaire, et laquelle ?

Des chartes éthiques, telles que celles de la CEPEJ [3], ou du collectif Arborus [4], fournissent des recommandations aux concepteurs, développeurs et utilisateurs d'IA.

Si l'engagement à respecter une charte constitue un élément de confiance, il ne constitue aucune certitude absolue quant à l'absence de risque. L'application effective d'une charte ne donne pas toujours lieu à contrôle. La signature de la charte vient témoigner d'une démarche intentionnelle, qui bien souvent ne recouvre qu'une opération de marketing et d'amélioration d'image.

De même, les processus de labellisation et certification de produits et services, en fournissant une assurance « raisonnable » du respect d'un jeu prédéfini d'exigences, apporteront un élément de confiance en matière d'IA, comme le font les systèmes de certification en matière de qualité, sécurité ou environnement.

L'objectif de ces processus est d'inspirer la confiance en faisant constater, par un organisme tiers, la conformité à un ensemble d'exigences. La confiance envers ces processus de reconnaissance se déduit ainsi du choix du référentiel d'exigences et du crédit accordé aux organismes certificateurs et accréditeurs.

Au-delà du référentiel de certification, l'attribution du certificat suppose l'existence d'un modèle d'évaluation qui définirait les règles qui suivent :

- qui est en charge d'évaluer la conformité au référentiel ?
- selon quel processus ?
- quels éléments de preuve pourront être exigés et vérifiés ?

Autant de questions auxquelles il faudra trouver des réponses, avant d'envisager la certification des systèmes à base d'IA.

II – Réduire et maîtriser les risques

Il est désormais courant de considérer la confiance comme un « mécanisme de réduction des risques ».
Pour réduire les risques, il convient d'abord de les évaluer. Cette évaluation est contextuelle et non absolue ; elle va évoluer au cours de la vie du système à base d'IA. Le niveau de risque d'une IA dépend de multiples facteurs : des technologies mises en œuvre, du domaine d'application, des cibles utilisateurs visées et de l'entreprise qui met en œuvre le système, entre autres.
Le « Livre Blanc » identifie les risques potentiels de l'IA : l'opacité des prises de décision, la discrimination fondée sur le sexe ou d'autres motifs, l'intrusion dans la vie privée, l'utilisation à des fins criminelles.

Une distinction est proposée entre les systèmes ordinaires et ceux à haut risque, qui nécessitent des mesures de protection particulières. Si cette distinction est nécessaire, l'établir n'est pas forcément évident. Afin de la rendre plus objective, il serait raisonnable de définir une échelle partagée des niveaux de risque. Réussir cet exercice nous semble néanmoins très difficile, car on ne peut pas parler de risque dans l'absolu, mais plutôt de perception et de sensibilité à des risques.

Utilisateurs et fournisseurs des systèmes à base d'IA auront, chacun, leurs propres perceptions et sensibilités, et il y a très peu de chances qu'elles soient les mêmes. Il est aussi peu probable que soient identiques les perceptions et sensibilités aux risques de deux fournisseurs de systèmes à base d'IA pourtant similaires, au sens de leur couverture fonctionnelle.

Les systèmes à base d'IA sont très complexes, car ce sont le plus souvent des systèmes de systèmes à base d'IA et l'analyse des risques de tels systèmes est une tâche permanente. C'est pourquoi nous pensons que le niveau de risque d'un système à base d'IA devrait ainsi être évalué en amont de sa conception (by design), puis réévalué à intervalles réguliers. Labels et certifications éthiques des systèmes à base d'IA devraient nécessairement s'appuyer sur une identification des risques, leur réévaluation régulière et un contrôle de la mise en place effective des mesures de leur réduction. Rappelons en effet que l'évaluation des risques ne constitue qu'une première étape du management des risques, qu'il convient de faire suivre par une étape de réduction soit de l'occurrence, soit de l'effet.

Il nous semble que les méthodologies d'analyse et de management des risques largement utilisées en milieu industriel, telles que l'AMDEC, peuvent être utilement appliquées aux systèmes à base d'IA, moyennant leur adaptation au contexte et une transposition des vocables aux modes de défaillance spécifiques des Intelligences Artificielles. Enfin, plus précises que de simples chartes, labellisations et certifications, celles-ci peuvent contribuer à définir des règles communes afin de favoriser l'émergence d'une concurrence loyale entre les concepteurs des systèmes à base d'IA au bénéfice de leurs utilisateurs.

III – Rapporter la preuve

Encore faut-il que ces systèmes de labellisation et certification reposent sur un système de preuve suffisamment solide et digne de confiance.

Afin d'aborder la problématique de la preuve, nous sommes partis de la charte Arborus sur l'intelligence artificielle [4]. Conçue pour créer un cadre de confiance vis à vis de l'intelligence artificielle, cette charte cherche essentiellement à en prévenir les biais potentiels par rapport à l'égalité des genres.

« *Elle est un document de référence aussi bien pour les entreprises de la Tech que pour toutes celles qui mettent en œuvre l'IA afin de respecter la diversité en veillant à ce que l'ensemble de la chaine de la valeur de la donnée soit responsable et que les biais discriminatoires soient identifiés et maîtrisés.* » [4]

Notre objectif ici est de mettre en exergue, de façon concrète, les moyens requis par une recherche de preuves par rapport à des allégations, et de souligner les difficultés d'une évaluation rigoureuse du respect de ces allégations. Nous ne cherchons nullement à critiquer l'initiative d'Arborus, qui ne peut avoir que des effets positifs dans la poursuite de son objectif.

Même si cette charte ne recouvre pas tous les domaines adressés par les autres initiatives actuelles de labellisation ou de certification d'une IA éthique et de confiance, elle apparait comme très représentative des problèmes que pourront rencontrer les certificateurs, de même que les experts devant rechercher des responsabilités après un sinistre.

Examinons l'un après l'autre, les 7 engagements pris par les signataires de cette charte et interrogeons-nous sur les façons de **démontrer à un tiers indépendant** la tenue de chaque engagement. Cet exercice n'est pas exhaustif, il est juste illustratif :

1. **Promouvoir la mixité et la diversité dans les équipes qui travaillent sur des solutions à base d'IA.**

Comme éléments de preuves de ce premier engagement, on peut imaginer de :

- Regarder le résultat : décompter les équipes travaillant sur l'IA et comparer le rapport femmes / hommes au même ratio pour le reste de l'entreprise ?
- Examiner le travail de « promotion » qui aura été fait, il s'agit alors d'évaluer les moyens déployés ?
- Collecter ces chiffres dans le temps pour évaluer l'efficacité des moyens déployés ?

Nous n'avons examiné que le rapport femmes / hommes, l'objectif ici étant la diversité, il faudrait sans doute aller plus loin dans l'analyse ? Nous pourrions également imaginer la collecte d'indicateurs plus micros, faire des analyses par site au lieu de prendre en compte toute l'entreprise, ou encore, employer de définitions strictes ou larges de la notion « d'équipes travaillant sur l'IA » ....

2. S'organiser pour évaluer et réagir à toutes formes de discrimination qui pourraient résulter de données biaisées ou stéréotypées.

Concernant ce deuxième engagement, on peut s'interroger sur la définition de la survenance d'une discrimination : est-ce un cas particulier isolé ? ou faut-il un nombre de cas suffisant pour déclarer qu'il y a survenance d'une discrimination ?

Une fois cela défini, on pourrait alors rechercher des éléments de preuve dans l'existence d'une procédure d'évaluation et de réaction en cas de discrimination. Il s'agirait là d'une preuve indirecte. Pour aller plus loin, il faudra s'interroger sur la matérialité de cette procédure : Est-elle documentée ? Est-elle connue ? par combien de personnes des équipes ? Est-elle appliquée ? Son application est-elle tracée ? A-t-elle déjà été utilisée ? Quels sont les résultats de son utilisation tant au niveau de l'évaluation que de la réaction ? A-t-elle été modifiée au fil du temps pour l'adapter aux réalités rencontrées ? quelles sont les leçons tirées ?....

3 Veiller à la qualité des données utilisées pour garantir des systèmes les plus équitables possible : une donnée unifiée, cohérente, vérifiée, traçable et exploitable.

Nous partons du principe qu'il s'agit là des données employées pour la mise au point des algorithmes. Il s'agit donc de données d'apprentissage (en cas de machine learning) et des données de tests. Les qualificatifs concernant ces données sont ici requis en nombre.

Les deux premiers « unifiée, cohérente » nécessitent une explicitation pour savoir comment vérifier ces points. Le suivant « vérifiée », par rapport à quel référentiel ?

La traçabilité, nous la comprenons comme étant un archivage probant des données d'apprentissage et de test. Il faudrait donc pour vérifier ce point, s'assurer que ces données ont bien été sauvegardées et que la sauvegarde qui est présentée est bien celle des données qui ont servi à la mise au point de l'algorithme. Comme en général il y a plusieurs versions successives, il faudrait être capable de retracer ces données pour chacune des versions.
Et en cas de recherche de preuves a posteriori, il faudrait s'assurer que la version opérationnelle au moment de l'incident est bien la version qui est présentée à un « vérificateur » externe.

Le dernier qualificatif, « exploitable », nécessite également une explicitation pour savoir comment vérifier son application.

4 Former pour sensibiliser et responsabiliser les concepteurs, développeurs et tous les acteurs impliqués dans la fabrique de l'IA, aux stéréotypes, aux biais pouvant générer des discriminations.

Cet objectif est un objectif de formation.

On pourrait donc en chercher des preuves en termes de mise en œuvre de moyens ; par exemple : le nombre d'heures de formation sur ce thème par personne concernée. Cet indicateur peut être affiné en distinguant différentes catégories de la population concernée.

On pourrait également rechercher des preuves de résultats : comment la formation a-t-elle agi sur les personnes concernées ? Y-a-t-il eu des évaluations des étudiants à la fin de chaque séance de formation ? quels en sont les résultats : interroger au hasard des personnes ayant suivi la formation pour vérifier leur niveau de connaissance ?

5 Sensibiliser les prescripteurs des solutions à base d'IA (RH, finances, relations clients, marketing), aux risques de biais et stéréotypes pouvant générer des discriminations et intégrer dans les cahiers des charges des points de contrôle et d'évaluation itérative.

Là aussi on est dans une logique de formation / sensibilisation, les mêmes remarques que pour le paragraphe précédent s'appliquent avec les deux logiques : quels sont les moyens mis en œuvre, et alors il faudrait se poser la question, sont-ils suffisants ? adaptés ? et une logique de résultats, qu'on pourrait mesurer de différentes façons, sur le niveau de sensibilisation des prescripteurs et sur les contenus des cahiers des charges. S'agissant de ces derniers, on pourrait, là aussi, mesurer principalement, des intentions.

Si on voulait aller plus loin, il faudrait tester les points de contrôle en cours d'élaboration du système et le contenu des évaluations. Si on voulait être complet, il faudrait également suivre les évolutions des cahiers des charges en cours de développement. Si on est dans une logique agile, où la documentation sur les développements est faible, cela nécessiterait de retracer toutes les itérations.

Être exhaustif risque de demander un effort considérable, même avec la contribution active de l'organisation auditée.

6 Veiller à bien choisir les fournisseurs et les évaluer de manière itérative afin de s'assurer que toute la chaîne de valeur de l'IA soit non discriminatoire.

Ici, nous tenons à signaler que la plupart des systèmes actuellement en développement et bon nombre de systèmes en service sont en fait déjà des combinaisons de systèmes à base d'IA. C'est-à-dire que les fournisseurs de systèmes à base d'IA font en réalité de l'assemblage, une intégration.

Certains systèmes à vocation large sont standardisés et disponibles sur étagère (par exemple une reconnaissance vocale), d'autres doivent être développés de façon plus spécifique. Certains fonctionnent dans le cloud, d'autres dans les locaux de l'utilisateur ou ceux du prestataire offrant le service au public.

Face à une telle diversité et variété de situations, comment les responsables achats pourront-ils évaluer leurs fournisseurs, répartis dans différents endroits de la planète et dont les produits évolueront en permanence ? Comment iront-ils chercher des preuves a posteriori ? Et comment pourra en attester l'organisme certificateur ?
Et surtout des problèmes peuvent naitre de la simple intégration de ces systèmes. Le système A fonctionne correctement, le système B aussi, connecter le système A à B pose des problèmes. Ce genre de situation est classique en informatique, mais l'impact avec des systèmes à base de neurones peut être très important.

7 Contrôler les solutions à base d'IA et adapter en continu les processus.

Les données de test sont là pour contrôler et valider les solutions à base d'IA. Il en va ainsi pour tout logiciel qui est mis sur le marché.

Existe-t-il cependant un seul logiciel commercialisé qui soit sans faille fonctionnelle et sans faille de sécurité ? La réponse est hélas, non.

Ce sont en général les utilisateurs qui remontent les failles fonctionnelles et les hackers, éthiques ou non, qui révèlent les failles de sécurité. Il ne pourra pas en être autrement des systèmes à base d'IA.

On pourrait, certainement, plus facilement évaluer les réactions aux remontées des défaillances : Vérifier s'il existe un processus ? s'il est documenté ? connu des gens qui doivent le mettre en œuvre ? Si les réactions ont permis de combler les failles ? Compter les fréquences d'apparition des failles ? De la proportionnalité et de l'adaptation des réactions aux problèmes rencontrés ?

Conclusion : « *Science sans conscience n'est que ruine de l'âme* »[5]

L'Europe numérique, la confiance, ses leviers.

En février 2020, la commission européenne proposait sa vision d'une Europe numérique fondée sur le développement de technologies fiables pour promouvoir une société ouverte et démocratique et une économie dynamique et durable. À cette occasion, Mme Ursula von der Leyen, s'est exprimée en ces termes : « *Je tiens à ce que cette Europe numérique reflète le meilleur de notre continent : l'ouverture, l'équité, la diversité, la démocratie et la confiance*.»

Comme tout outil ou technique créé par l'homme, la machine doit rester au service de l'Homme.

Le professeur P. MOATI, agrégé d'économie, fondateur du « Labo de la confiance » à l'université Paris-Diderot [6], est un observateur reconnu des mécanismes de formation de la confiance. S'appuyant sur la littérature académique récente, il en identifie les trois facteurs constitutifs suivants : **les compétences, l'intégrité et la bienveillance**.

Mesurer, d'une façon objective, la présence chez un fournisseur de systèmes d'IA des deux derniers critères, d'une dimension morale, est un exercice très ardu, voire impossible. Seul le temps démontrera si le comportement de l'entreprise reste loyal à l'égard de ses clients.

Il reste possible d'objectiver le premier critère, la compétence. Cela passe par la certification des ressources, process ou produits de l'entreprise, la mise à l'épreuve par des tiers de confiance, par des engagements de durée tels que garantie ou continuité de service.

La présentation de la (Commission Européenne spécifiait « *dans les domaines haut risque, comme la santé, la police ou les transports, les systèmes d'IA devraient être transparents, traçables et garantir un contrôle humain. Les autorités devraient être en mesure de tester et de certifier les données utilisées par les algorithmes, tout comme elles procèdent à des vérifications sur les cosmétiques, les voitures ou les jouets.* »

L'objet de la présente contribution est surtout de montrer que selon nous, obtenir des preuves pour certifier qu'un produit fini est conforme à une norme est un exercice bien connu. Mais ceci a très peu à voir avec l'obtention de preuves qu'un système à base d'IA fonctionne bien, va bien fonctionner dans le futur et a bien fonctionné dans le passé, en cas de recherche de responsabilités.

"*Le code juridique n'a pas vocation à se soumettre au code informatique*" [7]

On sait que les systèmes d'informations ne sont pas infaillibles ni au plan fonctionnel, ni au plan de la sécurité. Les systèmes à base d'IA n'échapperont pas à la règle. Aussi, dans l'absolu, on peut penser qu'une classification ou une échelle des risques ne saurait constituer un objectif réalisable. Néanmoins, une telle classification est nécessaire et permettrait aux acteurs du domaine de partager des repères communs de lecture et d'appréciation.

Rendre le fournisseur comptable de la mise en œuvre d'une approche éthique et responsable, sous la supervision d'une autorité de contrôle de l'IA, à l'instar de ce qui a été prévu pour le RGPD, nous semble alors être une voie à creuser.

Membres du groupe de travail EEEI

Benoit de Clerck, Expert de justice en informatique,

Alice Louis, Consultante en gouvernance du patrimoine informationnel, Directrice du projet Fonds Cyber Ethique pour une Souveraineté Numérique

Martine Otter Expert de justice en informatique,

Eric Parize Expert de justice en informatique,

Table bibliographique

[1] Jocelyne Maclure et Marie-Noelle Saint Pierre, « Le nouvel âge de l'intelligence artificielle : une synthèse des enjeux éthiques », Les cahiers de la Propriété intellectuelle vol 30, p 758, le 19/09/19, disponible sur : http://www.ethique.gouv.qc.ca/fr/assets/documents/CPI_Maclure_Saint-Pierre.pdf

[2] CNIL, « Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle » Décembre 2017, disponible sur : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf#page=60

[3] Conseil de l'Europe, CEPEJ, Commission européenne pour l'efficacité de la justice (CEPEJ) Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires, Sept. 2019, disponible sur : https://rm.coe.int/charte-ethique-fr-pour-publication-4-decembre-2018/16808f699b

[4] Association ARBORUS, collectif d'entreprises européennes sous le patronage du Conseil Économique et Social Européen, dirigé vers la promotion de l'égalité entre les femmes et les hommes, première charte internationale pour une IA inclusive, avril 2020, disponible sur : https://charteia.arborus.org/

[**5] François Rabelais, Pantagruel**, 1534 ; Gargantua donne à son fils Pantagruel son programme d'études.

[6] Philippe Moati, Professeur agrégé d'économie à l'Université Paris Diderot, Fondateur et co-président de L'association L'ObSoCo, La confiance : fondements et enjeux, disponible sur : https://kuryo.typepad.com/lelabodelaconfiance/2011/11/la-confiance-dans-la-marque-fondements-et-enjeux-philippe-moati.html

[7] Gaëtan Guerlin, Intelligence artificielle, 2019, Edition Grand Angle, Dalloz, p 49.