Réponse à consultation – Proposition de Règlement

Artificial Intelligence Act

L'AFNUM salue tout d'abord l'approche privilégiée par la Commission Européenne afin de règlementer l'Intelligence Artificielle. Cette technologie révolutionnaire, à l'origine du bouleversement de nombreuses pratiques, constitue une opportunité formidable pour améliorer la vie de nos concitoyens, mais représente également un potentiel de développement économique, de croissance et d'emplois sans commune mesure.

Dès lors, les nombreux choix faits par la Commission, qui montrent le souci de promouvoir le développement économique de l'IA et le potentiel de croissance représenté par cette technologie, répondent aux attentes des adhérents de l'AFNUM. La volonté, d'une part, de ne pas fragmenter le marché européen en favorisant un texte d'application directe dans tous les Etats membres, et d'autre part, l'approche par le risque visant à ne pas soumettre toutes les applications IA aux mêmes obligations, nous apparaissent très positifs.

La proposition de Règlement indique, dans ses grandes lignes, une réelle prise en compte des réalités de l'IA, par la différenciation entre ce qui relève de la recherche et ce qui peut être mis à disposition sur le marché. L'idée d'un cadre s'appliquant à l'échelle européenne, est non seulement profitable pour l'ensemble des acteurs économiques mais permet également l'établissement de normes harmonisées et de standards essentiels au développement pérenne d'un secteur.

Toutefois, afin que les objectifs de la Commission, à savoir assurer un équilibre entre protection et innovation tout en créant des standards exportables dans le cadre de la concurrence internationale, soient atteints, certains aspects de la proposition de Règlement doivent d'être améliorés.

Un cadre général qui peut gagner en précision

La définition d' « AI system » semble trop étendue

En premier lieu, la proposition de Règlement définit l'ensemble des techniques d'IA derrière la notion de « *AI system* »[1]. Si cette définition très large permet **d'inclure les produits contenant de l'IA**, élément essentiel pour les adhérents de l'AFNUM, l'étendue de cette définition interroge sur l'inclusion de certains logiciels et techniques logicielles. En effet, de nombreuses applications IA initialement exclues du périmètre de la proposition de Règlement pourraient se retrouver sous le joug de ce texte, du fait de certaines imprécisions de rédaction.

L'AFNUM recommande de clarifier la définition d'« *AI system* », notamment au regard de la diversité importante de techniques et réalités sous-jacentes à cette définition et aux techniques listées au sein de l'annexe I.

Ainsi, alors que les deux premières familles de techniques énumérées à l'annexe I(a) « *machine learning* » et I(b) « *knowledge based* » sont intrinsèquement identifiées à l'IA, le paragraphe (c) « *statistical approaches, Bayesian estimation, search and optimization methods*» liste des techniques

[1] « *Software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;* »

qui ne sont pas liées sans équivoque à l'IA ou fonctionnent en tandem avec d'autres techniques d'IA. L'appellation « approches statistiques » manque en effet de précision tandis que « l'estimation bayésienne » est principalement utilisée avec le *machine learning*. Enfin, les méthodes de recherche et d'optimisation sont utilisées depuis des décennies dans notre vie quotidienne pour effectuer divers types de recherche, de formation et d'optimisation. Par exemple, l'estimation statistique des systèmes sans fil a été utilisée dans les systèmes cellulaires 2G.

Ainsi, tous les algorithmes de recherche, tous les problèmes d'optimisation, tous les calculs statistiques ne sont pas des applications d'IA. Pour cette raison, nous suggérons de supprimer le point (c) de l'annexe I, en se concentrant uniquement sur les approches et techniques d'IA énumérées aux points (a) et (b) de l'annexe I.

Certaines hypothèses d'applications à haut-risque doivent être clarifiées

L'AFNUM tient à rappeler ici son attachement à une approche par le risque et à la différenciation nécessaire entre les applications d'IA. Nous souhaitons également réitérer notre soutien à la définition de **certains préjudices graves pour les personnes comme des applications à haut-risque** (par exemple, des menaces pour la santé, la vie ou les droits fondamentaux) et à **l'interdiction de l'utilisation de technologies**, telles que la reconnaissance faciale pour la surveillance de masse ou le profilage racial, qui constituent de potentielles violations des droits de l'homme et des libertés fondamentales. Nous sommes en phase avec la Commission pour interdire l'utilisation de systèmes d'IA par les autorités chargées de l'application de la loi pour l'identification biométrique - sauf dans certains cas très limités, avec l'application de certaines garanties, comme cela est prévu dans le projet de règlement.

Cependant, **certaines applications d'IA qualifiées à haut-risque selon les processus décrits à l'article 7 et à l'annexe III interrogent l'AFNUM**. En effet, ceux-ci pourraient inclure des utilisations qui ne sont pas à haut risque, par exemple dans le domaine des ressources humaines.

En outre, **certains cas d'applications à haut-risque doivent être clarifiés**. La notion de « *safety component* » ainsi que celle de « *road traffic* »[2] sont à préciser, leur incertitude pouvant présenter un problème de sécurité juridique. S'il s'agit d'applications IA intégrées directement dans un véhicule, il y aurait un **enjeu de cohérence avec la réglementation homologation** (2018/858). En effet, certaines applications IA intégrées dans une automobile, par exemple un assistant vocal, ne sont pas couvertes par l'homologation parce qu'elles n'ont pas d'impact sur la sécurité. Dès lors, la dénomination employée dans la proposition de Règlement manque de précision et risque d'inclure ces applications dans l'ensemble d'applications à haut-risque, alors que **la législation sectorielle a considéré que cela n'était pas nécessaire**. Cela aurait pour conséquence de soumettre toutes ces applications à une processus de certification. Ainsi, il conviendrait de **préciser quel type d'application est visé** par la dénomination employée dans la proposition de règlement et préciser s'il s'agit des applications déjà intégrées dans le véhicule, qui sont soumises à une homologation sous législation sectorielle et devraient donc exclues du champ d'application du présent règlement ou bien s'il s'agit d'applications non intégrées directement au véhicule, mais qui, ayant un impact sur l'infrastructure routière, serait soumises au présent règlement en vertu de l'annexe III.

L'Annexe III gagnerait ainsi en clarté en excluant les applications intégrées dans les véhicules et pour que les applications concernant la gestion de l'infrastructure routières soient limitées à celles qui ne

[2] « *AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity* »

sont pas intégrées dans les véhicules et qui sont développées avec un usage prévu (« *intended use* ») clairement lié à la sécurité et qui actionnent des composants d'infrastructure routière.

Plus largement, la Commission devrait envisager de réduire la liste des systèmes d'IA de l'annexe III afin qu'elle n'englobe que les systèmes d'IA qui présentent des "risques élevés" systémiques pour les personnes physiques qui interagissent avec eux.

Il est nécessaire d'assurer une cohérence entre les textes

Par ailleurs, il nous apparaît important de rappeler que, bien que cette proposition de Règlement s'inscrive dans un contexte règlementaire global, les liens avec les autres textes mentionnés dans « *l'explanatory memorandum* » (Digital Services Act, RGPD, Data Governance Act etc.) **manquent de lisibilité**. En effet, le texte évoque peu l'accès aux données, pourtant essentiel au fonctionnement de l'IA, en renvoyant trop implicitement aux précédentes ou prochaines évolutions règlementaires.

Il apparaît ici primordial de rendre l'ensemble de ces éléments cohérents et clairement lisibles afin d'assurer la sécurité juridique de l'ensemble des acteurs.

De même façon, la présente proposition de Règlement n'aborde pas la question des responsabilités, traitées dans un autre texte annoncé d'ici à la fin de l'année 2021 (« *Liability Act* »). **Sur ce point, l'AFNUM recommande de conserver la logique de clarté et de sécurité juridique qui a présidé jusqu'alors à la définition des responsabilités du fait des produits défectueux** (Directive 85/374/CE[3])**, qui est parfaitement adaptée aux défis posés par l'émergence de nouvelles technologies.**

De ce point de vue, la définition d'un usage intentionné (« *intended purpose* » en anglais) et d'un « producteur » responsable de la mise sur le marché va dans la bonne direction puisqu'elle permettrait de **clarifier les rôles et responsabilités**. Néanmoins, la complexité des chaines de valeurs de l'utilisation de logiciels et d'applications d'Intelligence Artificielle devrait être prise en compte. La définition large de système d'IA et, par la suite, de fournisseur (« *provider* » en anglais), ne permet pas de déterminer efficacement quels systèmes d'IA et quelles entités (fournisseurs) entreraient dans le champ d'application du règlement.

Pour cette raison, **nous suggérons que le règlement clarifie la différenciation des rôles dans la chaîne de valeur de l'IA, de sorte que les entités développant des boîtes à outils ou des bibliothèques logicielles d'IA à usage général ne soient pas considérées comme des « *providers* ».** Par exemple, la proposition de règlement pourrait préciser que ces tiers concernés ne sont pas considérés comme des fournisseurs de systèmes d'IA au sens du règlement, car ces entités ne seront pas en mesure de déterminer à l'avance l'utilisation prévue de leurs outils IA et ne pourraient donc pas prévoir une utilisation à haut-risque ou empêcher une « mauvaise utilisation raisonnablement prévisible ».

Sur ce point-là, nous suggérons aussi que le règlement prévoit la possibilité pour les fournisseurs de systèmes d'IA et leurs utilisateurs de répartir contractuellement leurs responsabilités. Les utilisateurs sont en effet souvent mieux placé pour assurer le respect de certains exigences dans la pratique (par exemple, la transparence, la surveillance humaine, la cybersécurité, etc.).

[3] 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

Les obligations pour les applications à haut-risque doivent être affinées.

L'AFNUM soutient plusieurs des obligations prévues par la proposition de Règlement, notamment pour les applications à haut-risque. Certaines d'entre elles sont déjà mises en œuvre par plusieurs de nos adhérents afin de sécuriser leurs produits, tel que le « *risk-management* » prévu à l'article 9[4]. Néanmoins, si plusieurs de ces obligations, telles que les obligations de transparence (article 13[5]) ou de supervision par l'individu (article 14[6]), semblent être de réels outils pour aider à développer la confiance dans l'IA et contribuer à son développement, **certaines de ces mesures doivent être clarifiées pour assurer la sécurité juridique des fournisseurs d'applications IA.**

En effet, les obligations de « *record-keeping* » (article 12[7]), par exemple, interrogent **les responsabilités de chaque acteur** (fournisseur et utilisateur de l'application IA), ainsi que **la faisabilité** de l'enregistrement de telles données. De même manière, si certaines obligations, telle que le « *risk-management* », sont déjà appliquées pour des produits actuellement sur le marché, leur transcription aux nouveaux produits mis sur le marché pose la question de la mise en œuvre – les processus actuels peuvent-ils être étendus tels quels aux nouveaux produits ? **Le « *record keeping* » et le « *risk management* » devraient suivre les procédures définies dans les législations sectorielles référencées à l'Annexe II pour les applications à haut-risque que cette Annexe couvre.**

Parallèlement, les applications « *stand alone* » listées à l'Annexe III qui, elles, ne sont pas soumises à de telles obligations, nécessiteront la définition de procédures claires, pour une mise en œuvre dans les meilleures conditions.

Enfin, la notion de « *free of error* »[8] figurant à l'article 10[9] au sujet de la gestion des données, **apparaît impossible à garantir pour les fournisseurs d'applications IA sans une définition plus précise de sa mesure**. Indépendamment de l'impossibilité d'assurer juridiquement une absence totale d'erreur, cette mesure ne prend pas en compte l'hypothèse d'applications IA alimentées par les données des clients – sur lesquelles le fournisseur n'a pas de moyens de contrôler le taux d'erreur. Une possibilité serait alors de s'inspirer d'autres processus de certification pendant lesquels un pourcentage limite d'erreur à ne pas dépasser est fixé sur un échantillon donné pour que le test soit validé.

L'AFNUM recommande donc une clarification des obligations prévues aux articles 10 et 12.

---

[4] « *A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems* »

[5] « *High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider* »

[6] « *High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which the AI system is in use.* »

[7] « *High-risk AI systems shall be designed and developed with capabilities enabling the automatic recording of events ('logs') while the high-risk AI systems is operating. Those logging capabilities shall conform to recognised standards or common specifications.* »

[8] « *Training, validation and testing data sets shall be relevant, representative, free of errors and complete.* »

[9] « *High-risk AI systems which make use of techniques involving the training of models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5.* »

Les mécanismes de certification sont au service de la sécurité juridique des produits uniquement

Nous saluons le processus proposé pour que les entreprises utilisent des normes harmonisées et procèdent à une évaluation de la conformité de certains de leurs produits, y compris par une auto-évaluation lorsque cela est prévu par les législations sectorielles. Ces mécanismes, rassemblés au sein du « *New Legislation Framework* » pour le marché européen, se sont avérés efficaces pour **stimuler l'innovation, développer et mettre sur le marché européen des technologies sûres et fiables**. Le système des organismes d'évaluation de la conformité est bien établi et efficace. Ces mécanismes sont d'ailleurs déjà mis en œuvre et bien maitrisés par les adhérents de l'AFNUM.

Cependant, le processus de certification, tel que décrit dans la proposition de Règlement, semble être un processus lourd et coûteux pour les nouveaux produits et nouveaux acteurs sur le marché, ce qui pourrait constituer un frein à l'innovation. De plus, au regard de la définition donnée pour les applications d'IA (« *AI system* »), de tels mécanismes de certification s'appliqueraient aussi bien aux produits qu'aux logiciels. Dans la seconde hypothèse, **l'AFNUM s'interroge** sur le fait que ces standards soient applicables en l'état aux logiciels**, notamment lorsqu'ils concernent les algorithmes ou les jeux de données**.

Aussi, **il apparaît essentiel d'accorder un délai suffisant afin de mettre en œuvre ce processus et de s'interroger sur la cohérence des normes avec la réalité du marché et de la technologie visée**. Par ailleurs, il n'y a pas de processus d'évaluation de la conformité (auto-évaluation ou certification) sans standard international. Ces derniers devraient être pris en compte pour définir les règles.

Enfin, la notion de composant de sécurité (« *safety component* » en anglais) gagnerait à être clarifiée et mise en cohérence avec le cadre européen de la sécurité des produits. La définition pourrait être sujette à interprétation et devenir une source d'incertitude pour la définition des systèmes d'IA à haut risque.

Pour réduire cette ambiguïté, nous pensons qu'il est important que **l'évaluation d'un composant de sécurité renvoie à la législation harmonisée de l'Union, pour s'aligner sur toutes les exigences essentielles pertinentes**. En d'autres termes, lors de l'évaluation d'un système d'IA aux fins de l'article 6, paragraphe 1, un composant de sécurité doit être défini tel qu'il l'est dans la législation d'harmonisation de l'Union pertinente énumérée à l'annexe II.

Un cadre pour la transparence et pour l'innovation favorable aux entreprises

L'AFNUM soutient les principes de transparence et d'explicabilité en matière d'IA prévus par le texte (article 52[10]). Il est primordial, pour développer la confiance dans cette technologie, que les consommateurs soient informés qu'ils interagissent avec une IA, même pour des applications à risque faible.

L'AFNUM s'interroge toutefois sur la formulation « *unless this is obvious from the circumstances and the context of use* » (article 52, alinéa 1), qui semble exonérer les utilisateurs d'IA de l'obligation

[10] « *Providers shall ensure that AI systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an AI system, unless this is obvious from the circumstances and the context of use.* »

d'informer les consommateurs de leur interaction avec une application d'IA. Cette formulation nous paraît être **source d'insécurité juridique** du fait de son manque de clarté.

Enfin, l'AFNUM salue vivement l'approche privilégiée par la Commission s'agissant des applications ne présentant pas de risque, à savoir les **incitations à adopter des codes de bonne conduite ainsi que les mesures en faveur de l'innovation** (Article 53[11]). Les bacs à sable règlementaires sont des outils propices au développement d'une technologie encore jeune.

Sur l'innovation, l'AFNUM note que les petites entreprises sont, à juste titre, privilégiés. **Il conviendrait toutefois que le cadre règlementaire permette plus aisément les collaborations entre les acteurs de différentes tailles afin d'améliorer l'accès à l'innovation et le développement des applications d'intelligence artificielle.**

A propos de l'AFNUM

L'AFNUM (Alliance Française des Industries du Numérique) représente, en France, les industriels du secteur IT, des réseaux, de l'électronique grand public, de l'impression, de la photographie et des objets connectés. Le poids économique des 56 entreprises adhérentes de l'AFNUM est de 31.000 emplois directs et de 60.000 emplois indirects et induits en France pour 26 milliards d'euros de chiffre d'affaires. L'AFNUM est membre de la FIEEC, du MEDEF et de Digitaleurope.

(Airbus DS, Alcad, Alcatel Lucent Enterprise, Amazon, Apple, Art-Fi, Brother, Cae, Canon, Cisco, Continental, Crosscall, Dell, Doc up, Epson, Erard, Ericsson, FP Francotyp-Postalia, Fracarro, Fujifilm, HP, IBM, Intel, Kodak alaris, Leica, Lenovo, Lexmark, LG, Lumiere Imaging, Microsoft, Nikon, Nokia, Oppo, Optex Normand, Panasonic, Quadient (ex-Neopost), Qwant, Ricoh imaging, Samsung, Sequans Communications, Sigma, Sony, Storit.io, Tamron, TCL, Technicolor, Televes, Tetenal, Toshiba, Trax, Triax, Verbatim, Vitec Imaging Distribution, WDC, WISI)

[11] « *AI regulatory sandboxes established by one or more Member States competent authorities or the European Data Protection Supervisor shall provide a controlled environment that facilitates the development, testing and validation of innovative AI systems for a limited time before their placement on the market or putting into service pursuant to a specific plan.* »