Feuille de route stratégique

La normalisation de l'Intelligence Artificielle

Résumé

Alors que l'Intelligence Artificielle s'impose rapidement dans tous les secteurs économiques, la maîtrise de cette technologie et la prise en compte des préoccupations sociétales qu'elle implique pose la question, au premier plan, de la confiance. Afin de répondre à ces enjeux, le Gouvernement français a lancé un Grand Défi visant à « *Sécuriser, certifier et fiabiliser les systèmes fondés sur l'intelligence artificielle* », piloté par le Secrétariat Général pour l'Investissement et financé par le Plan d'Investissement d'Avenir. Dans ce cadre, AFNOR est chargé de « *créer l'environnement normatif de confiance accompagnant les outils et les processus de certification des systèmes critiques à base d'Intelligence Artificielle* ».

La présente stratégie de normalisation de l'IA, construite à partir d'une consultation nationale réalisée auprès de 260 acteurs français du domaine et d'entretiens ciblés auprès d'experts, présentes plusieurs enjeux.

D'un point de vue technologique tout d'abord, l'IA apparait comme un sujet éminemment transverse car elle constitue une brique interconnectée avec d'autres technologies (Iot, edge-computing, cloud etc.) permettant de construire des applications elles-mêmes interconnectées dans un écosystème numérique. A ce titre, les changements apportés par l'Intelligence Artificielle, et par conséquence leurs normes, auront une dimension systémique qui impose une grille de lecture générique et horizontale.

Alors que tous les organismes de normalisation sectoriels (aéronautique, santé, assurance, automobile…) ont naturellement lancé des réflexions normatives en la matière, la coordination entre ces derniers nécessitera une articulation entre leurs travaux pour s'assurer de l'interopérabilité de leurs produits. Une architecture coordonnée entre normalisation horizontale et sectorielle reste ainsi à développer. Dans un premier temps, la terminologie et les concepts-clés devraient par exemple être du ressort de la normalisation horizontale, tandis que les exigences techniques (sûreté, sécurité etc.) resteront nécessairement sectorielles.

La normalisation de l'IA présente également des enjeux réglementaires. En effet, la Commission Européenne a présenté en avril 2021 un projet de directive encadrant son emploi (*AI Act*)[1] : l'IA en Europe devra être « de confiance » et faire l'objet d'analyses de risques.

Dans cette classification des systèmes d'IA en fonction de leur niveau de risque, les « systèmes à haut risque » nécessiteront une certification pour être mis sur le marché. Pour toutes ces applications – qui comprennent la majorité des projets industriels - les critères de certification s'appuieront sur des normes dites « harmonisées » qui détailleront les exigences

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

techniques nécessaires. La conformité aux normes harmonisées constitue ainsi une présomption de conformité à la réglementation européenne.

Nombreux sont les acteurs qui, craignant des textes règlementaires trop flous ou trop contraignants, n'ont pas perçu que le corpus normatif accompagnant la règlementation pouvait répondre à leurs préoccupations, apporter clarification et flexibilité, pour peu qu'ils participent à son élaboration. De fait, une normalisation structurée, accessible et opérationnelle, est de nature à soutenir l'innovation et l'économie européenne en réduisant les incertitudes liées à la règlementation.

Enfin, la normalisation de l'IA revêt une dimension stratégique. Dans un contexte de rapport de force au niveau international, les compétences de la France en matière d'Intelligence Artificielle constituent l'opportunité de promouvoir ses intérêts et de constituer une force européenne puissante favorisant l'innovation.

La normalisation de l'IA se présente comme complexe et nécessite une vision globale « d'architecte » à promouvoir au niveau international. En effet, c'est à ce niveau que le corpus normatif s'imposera à tous, directement ou indirectement, grâce à sa prise en compte par les écosystèmes industriels de tous les pays. Pour porter les intérêts à ce niveau, il convient d'investir tous les échelons de la normalisation : national, européen et international.

Aussi les activités de normalisation françaises devront privilégier le soutien de la règlementation européenne, en s'appuyant sur les organismes européens (CEN, CENELEC et ETSI). D'autre part, le CEN-CENELEC s'appuiera fortement sur les normes ISO-IEC (et notamment celles du SC 42, dédié à l'IA), ce qui nécessite une participation significative à ces instances afin de s'assurer que les prismes d'analyse nationaux et européens soient bien pris en compte.

Au regard des enjeux géopolitiques relatifs à la normalisation – et davantage encore dans le domaine de l'IA - il revient aux pouvoirs publics de réinvestir le champ de la normalisation du numérique. En finançant et en mobilisant les acteurs académiques et les acteurs de l'innovation d'une part, mais également en animant le pilotage des activités stratégiques liées à la souveraineté numérique.

De la même manière, le monde de la Défense sera impliqué, bien que non concerné par le projet d'*AI Act*. La Défense aura en effet également besoin d'un corpus normatif pour la spécification et la qualification des systèmes d'armes. La pression relative aux examens de licéité et de sécurité des armements induit que le référentiel normatif Défense soit, *a minima,* équivalent à l'état de l'art dans le monde civil. Une utilisation significative de normes civiles par la Défense apparait comme probable.

Afin de prioriser les actions à mener pour traiter ces enjeux, certains leviers d'actions ont été identifiés à travers 6 axes stratégies de normalisation :

1. Développer les normes portant sur la confiance

Autrefois résumée à ses composantes sécuritaires (sécurité et sûreté), la confiance est désormais définie comme un ensemble de caractéristiques mesurables, intégrant également les préoccupations sociétales, dans le prolongement de la Déclaration des droits de l'Homme et du Citoyen et de la défense de la souveraineté nationale.

Si à ce jour une trentaine de caractéristiques de la Confiance ont pu être répertoriées, une douzaine semblent prioritaires et identifiées par la Commission Européenne, parmi lesquelles l'explicabilité, la robustesse,

l'équité, la responsabilité, la transparence, la supervision humaine… en plus des exigences de sécurité et de sûreté.

Après s'être accordé sur une terminologie (ontologie), il conviendra de détailler les exigences techniques sous-jacentes, ainsi que les métriques et les contrôles permettant leur évaluation.

2. Développer les normes sur la gouvernance et le management de l'IA

La confiance concerne également les organisations qui devront démontrer qu'elles ont les compétences, les méthodes et les outils pour utiliser de l'IA, mais également qu'elles maitrisent les analyses de risques sur le développement et l'emploi de ces systèmes. Des normes sur l'organisation des entreprises (AI Management System), sur l'évaluation des risques (AI Risk management) seront incluses dans le périmètre des travaux normatifs et donneront lieu à des certifications d'entreprises.

3. Développer des normes sur la supervision et le reporting des systèmes d'IA

Identifier la place de l'homme dans la conception, la qualification et l'utilisation des systèmes d'IA est essentiel. Il s'agit d'une exigence sociétale, politique et règlementaire qui va entraîner des conséquences fondamentales sur la conception des systèmes, sur l'organisation des entreprises, des organismes de certification, voire sur l'organisation des secteurs critiques.

Il convient donc de s'assurer que les systèmes sont contrôlables (capacité à reprendre la main), que la supervision (capacité à observer le fonctionnement d'un système, notamment dans les phases critiques), fortement automatisée, permettra de remettre l'homme dans la boucle de décision aux moments critiques où l'IA sortira de son domaine de fonctionnement nominal.

4. Développer des normes sur les compétences des organismes de certification

Les organismes notifiés, rouages essentiels de l'écosystème européen de la confiance, car en charge de la certification des produits, des processus et des services considérés comme à « haut risque », devront également démontrer leurs compétences qui seront normalisées.

5. Développer la normalisation de certains outils numériques

L'utilisation de la simulation comme source de données et de scénarios, pour la spécification, la conception, l'entrainement, la validation, le test, la qualification et l'audit des systèmes à base d'IA devrait se développer rapidement (simulation, jumeaux numériques…). Au regard des enjeux, et de la place centrale que prendront ces outils dans le développement des systèmes d'IA, un rapport technique présentant l'ensemble des problématiques, et une démarche normative possible en lien avec les besoins du marché, doit être développé.

6. Simplifier l'accès et l'utilisation des normes

Le corpus normatif de l'IA qui se profile sera donc très conséquent, couvrant la terminologie, la confiance, les organisations, le management des risques, l'interopérabilité, le cycle de vie et la qualité des données, ou encore les processus d'engineering. Pour soutenir le monde de l'innovation, des *start-ups* et des PME, la normalisation devra être accessible et opérationnelle. Les normes devront donc pouvoir être « lues » par des machines qui en extrairont automatiquement les exigences, les métriques et les contrôles

associés. La prise en compte de ces exigences dans les processus industriels permettra d'accélérer le développement des produits et sera un des éléments clés dans l'évaluation de conformité.

Ces axes stratégiques seront déclinés en une série d'actions opérationnelles au sein d'une feuille de route mobilisant un grand nombre d'acteurs. Pour s'assurer de la cohérence et de la bonne conduite des actions identifiées, un groupe de réflexion piloté par AFNOR sera chargé de suivre et veiller à l'implémentation de cette feuille de route.

De plus, des coordinations européennes et internationales seront mises en place afin de porter les intérêts français dans les espaces de décisions pertinents. Cette stratégie de normalisation de l'IA constitue donc une étape indispensable pour poser les bases d'une IA efficiente et maitrisée, et au-delà, d'un monde numérique de confiance.

Table des matières

Introduction

Alors que la Commission Européenne s'apprête à réguler l'Intelligence Artificielle, il apparaît désormais clairement que la confiance autour de cette dernière va se construire grâce à la règlementation, la normalisation et l'évaluation de conformité aux exigences règlementaires.

Les liens clairs entre régulation et normalisation (via entre autres l'outil des normes harmonisées européennes) nécessitent d'investir le champ de la normalisation et de développer une démarche stratégique nationale et européenne. En effet, si la loi fixe un cadre général, c'est bien la normalisation qui en précisera sur certains points les modalités (notamment leurs modalités techniques). Une conformité à la norme (et aux normes harmonisées) équivaut à une conformité aux directives européennes.

Dans le cadre du Grand Défi « Sécuriser, Certifier et Fiabiliser les Systèmes fondés sur l'Intelligence Artificielle », le Secrétariat Général Pour l'Investissement (SGPI) a développé une approche basée sur trois piliers : la recherche, les applications et la normalisation.

Ce troisième pilier normatif, piloté par AFNOR, vise à « *créer l'environnement normatif de confiance accompagnant les outils et les processus de certification des systèmes critiques à base d'Intelligence Artificielle* ».

Pour cela, la démarche employée consiste à mettre en place une plateforme de coopération entre acteurs français de l'IA, d'implémenter des actions stratégiques en normalisation et de développer des coopérations européennes et internationales. En structurant l'écosystème de cette manière, l'objectif est de permettre le développement des normes sur l'Intelligence Artificielle cohérentes et adaptées aux intérêts français et européens.

La présente stratégie est donc une première étape, une grille de lecture commune permettant de mettre en place les actions identifiées. Elle résulte d'une construction collective, par l'analyse croisée d'une cartographie des normes et initiatives sur l'IA, des besoins identifiés lors d'une grande consultation nationale, et d'entretiens qualitatifs et ciblés avec les acteurs de l'IA.

Une mise en perspective a ainsi été réalisée entre l'environnement normatif et la compréhension des enjeux révélés par la cartographie, les besoins et priorités exprimés par l'écosystème, et la réalité industrielle partagée lors des entretiens. Ces premières actions permettent ainsi de définir des leviers actionnables pour les différents acteurs en matière de normalisation de l'IA, en d'en dégager une feuille de route.

Le champ normatif est complexe, très évolutif et les intérêts des Etats, mais aussi de certains acteurs privés, apparaissent clairement en jeu. La stratégie de normalisation devra donc être discutée, affinée et surtout mise à jour régulièrement avec l'ensemble des partenaires régaliens et économiques (entreprises, PME, association d'entreprises, et plus généralement le tissu de l'innovation).

La précision et la pertinence des différents axes de cette stratégie permettra ainsi d'implémenter des actions adaptées aux enjeux et intérêts français dans la normalisation de l'IA.

Ces intérêts s'inscrivent en outre dans un cadre international et européen. Alors que les normes techniques sur les nouvelles technologies s'élaborent au niveau mondial, il est nécessaire d'y porter cette stratégie afin de

faire valoir les intérêts identifiés. Identifier les structures pertinentes pour y contribuer de manière active et nouer des partenariats au niveau international constituent des actions indispensables pour promouvoir les intérêts français.

Ainsi, pour répondre aux enjeux et accomplir les objectifs de cette feuille de route, une mobilisation de tous les acteurs est nécessaire. Pour ce faire, le suivi de sa déclinaison doit être sera effectuée dans un cadre de coordination multisectoriel qui sera mis en place par AFNOR au cours de l'année 2022.

Contexte

Les normes comme outil de régulation volontaire

Tout d'abord il est impératif de constater et d'analyser la relative incompréhension nationale au sujet de la normalisation. La dimension stratégique des normes ne semble pas être intégrée par une partie des entreprises françaises et les acteurs économiques semblent s'en désintéresser alors même que la mise en conformité et l'application de la règlementation les préoccupe.

Les *start-ups*, PME et ETI, quant à elles, ne sont pas suffisamment bien intégrées dans les écosystèmes de normalisation pour en appréhender les enjeux, et prendre la décision de dégager du temps et des ressources dédiées dans l'élaboration des normes.

Des causes culturelles peuvent aider à comprendre cette méconnaissance de la « *soft law* » et de son importance. En s'appuyant sur des acteurs privés et publics pour définir des règles volontaires pour l'intérêt général, la normalisation heurte notre vision politico-juridique, et explique le désintérêt des administrateurs pour les sujets techniques et leur méfiance à l'égard du secteur privé.

Cependant on ne peut pas définir un cadre technique à l'économie de façon purement *top-down.* La normalisation présente l'avantage de faire participer les experts des organisations directement concernées. La parole des acteurs économiques est alors valorisée et leur permet de contribuer à l'élaboration de ces règles de manière directe, tant au niveau national qu'au niveau européen et international.

De ce fait, la normalisation incarne une forme de régulation volontaire permettant aux entreprises d'inscrire leurs activités dans un contrat collectif compris et accepté par tous. La mise en conformité constitue ainsi une présomption de qualité, de fonctionnement et d'interopérabilité.

Néanmoins, dans certains cas jugés indispensable pour la bonne conduite du marché européen, certaines normes s'inscrivent dans un cadre réglementaire.

La catégorie de « normes harmonisées » sont initiées par un mandat de la Commission Européenne afin de s'assurer que les produits et services respectent les prescriptions techniques de la législation correspondante.

A ce titre, la participation à leur élaboration permet non seulement d'anticiper l'interprétation technique de la réglementation, mais surtout de définir les modalités de cette déclinaison, qui deviendront – *de facto* – les exigences d'une réglementation à venir.

La normalisation de l'IA, un support technique à la réglementation

Concernant les technologies d'Intelligence Artificielle, le projet de Règlementation de la Commission Européenne s'inscrit dans une évolution législative sur le numérique de plus en plus importante de la part de l'Union Européenne : le *Data Governance Act* présenté le 25 novembre 2020[2], le Règlement

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

Général sur la Protection des Données du 27 avril 2016[3], ou encore l'étude sur le rôle de l'IA dans le *Green Deal* Européen, réalisée par le Parlement Européen[4].

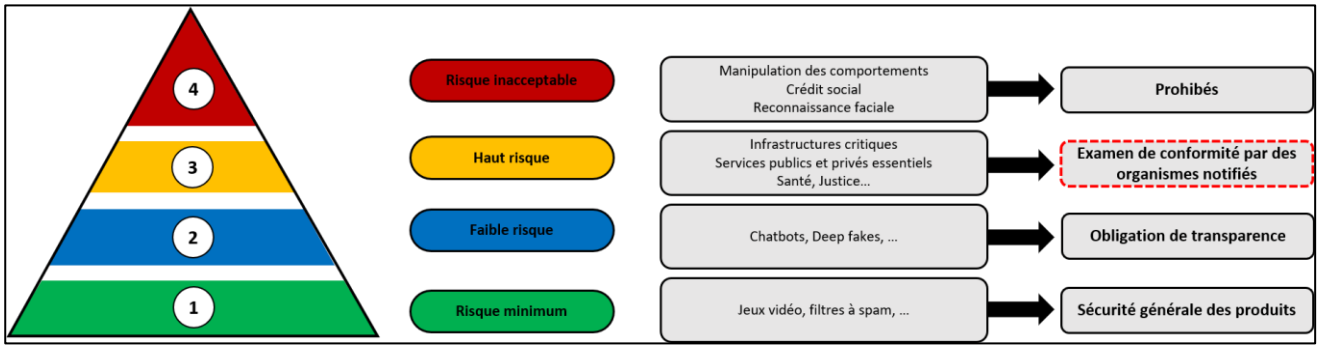
Le prisme européen s'avère ainsi incontournable pour anticiper l'évolution réglementaire et normative de l'Intelligence Artificielle. D'une part, ce nouveau cadre juridique encadrant l'utilisation des systèmes d'IA va structurer les domaines applicatifs et par conséquent, façonner les différents marchés.

D'autre part la démarche de la Commission donne au corpus normatif une place fondamentale, représentant le point de rencontre entre exigences réglementaires et déclinaisons opérationnelles par le marché.

En effet, le futur règlement opère une classification des systèmes d'IA en fonction du niveau de risque, répartie en 4 catégories : les systèmes de niveau 4 (risque inacceptable) seront prohibés, et les deux premiers niveaux (risque minimum, faible risque) seront soumis à un code de conduite.

En revanche les systèmes d'IA à haut risque (niveau 3) seront soumis à des exigences réglementaires via un examen de conformité par des organismes notifiés. Ces exigences obligatoires, portant sur des caractéristiques de la confiance (l'explicabilité, la robustesse, la responsabilité, la transparence, la supervision humaine etc.), seront détaillées à travers des normes harmonisées, sur lesquelles les critères de certification s'appuieront.

Pour tous les systèmes considérés à « haut risque » donc, qui comprennent une grande partie des applications industrielles, les normes harmonisées constitueront les exigences techniques nécessaires pour être conforme à la réglementation.



Dans ce cadre, les normes constituent un élément incontournable pour le futur marché de l'Intelligence Artificielle. C'est pour cette raison que le Grand Défi IA intègre un pilier dédié à la normalisation, afin de définir une stratégie pour les acteurs français et européen dans un domaine un grand nombre d'acteurs mettent en avant leurs intérêts.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[4] https://www.europarl.europa.eu/committees/en/the-role-of-ai-in-the-european-green-dea/product-details/20210607CAN61223

La normalisation comme outil d'influence

La normalisation représente de fait un outil d'influence conséquent tant pour le positionnement des entreprises sur le marché que pour la stratégie industrielle des Etats.

Pour les entreprises, les travaux de normalisation permettent de diffuser des spécifications favorables à leurs intérêts. Les normes adoptées auront ainsi pour conséquences de structurer le marché en faveur de leurs technologies, entrainant d'un gain de part de marché jusqu'à l'éviction de leurs concurrents.

Les processus d'élaboration des normes font également l'objet d'actions d'influence plus indirectes, par exemple à travers l'utilisation des brevets. Alors que certaines exigences peuvent s'appuyer sur des briques technologiques initiées par des brevets, l'application de la norme requiert alors l'utilisation de cette propriété intellectuelle, permettant à l'entreprise propriétaire de toucher des redevances, d'imposer le recours à sa technologie, ou encore de bloquer l'utilisation de la norme.

Afin de contourner ces potentielles stratégies commerciales de la part des entreprises détentrices de brevets, les organismes de normalisation ont édicté des règles dédiées à la présence de ces brevets : ces derniers doivent être déclarés par les propriétaires au cours des travaux de normalisation et leur éventuelle utilisation doit faire l'objet de concession de licences, soit des conditions raisonnables et non discriminatoires (licence RAND), soit en excluant toute redevance (RF).[5]

Néanmoins, la question de la validité des brevets, leur périmètre et leur portée constituent autant d'éléments d'interprétations justifiant leur intégration dans les travaux normatifs. Les organismes de normalisation ne participants ni à l'établissement des contrats de licence, ni au règlement des litiges, la présence de ces brevets à des fins de stratégie commerciale par les entreprises représente tant un levier d'influence qu'un point de vigilance.

A l'inverse, l'absence de normalisation peut également constituer une stratégie d'hégémonie de la part de certaines entreprises sur le marché. En bloquant la constitution de normes, les acteurs dominants peuvent ainsi imposer leurs technologies propres et créer un modèle de dépendance sur toute la chaine de valeur : ce que l'on appelle un « *standard de fait* ».

La normalisation représente également une opportunité d'intelligence économique importante pour les entreprises impliquées. Les travaux de normalisation apportent en effet une plus-value en termes d'information stratégique : les entreprises participantes acquièrent un avantage concurrentiel en termes de connaissance, de compréhension des tendances et de temps.[6]

En effet, le déroulement des travaux de normalisation conduit les parties prenantes à diffuser de la documentation industrielle, communiquer sur des innovations, afficher une feuille de route ou encore soutenir un agenda spécifique. Tous ces éléments constituent autant d'informations stratégiques dont la captation et l'analyse permettent de

[5] https://www.wipo.int/patent-law/fr/developments/standards.html

[6] https://sisse.entreprises.gouv.fr/files_sisse/files/outils/rapports/synthese_publique_rapport_normalisation_11_janvier_2012.pdf

mettre en place des stratégies commerciales, concurrentielles – mais également normatives.

La création de normes participe dans plusieurs cas aux actions de renseignement économique menés par des entreprises dans le cadre de stratégies étatiques. En conditionnant le marché au profit de la technologie ou du savoir-faire de ces entreprises nationales, les Etats peuvent ainsi mettre en place des actions de contrôle sur des entreprises étrangères, de la captation d'information voir même des transferts de technologies.

A travers ces stratégies de normalisation se jouent en effet les rivalités géopolitiques qui ont toujours traversé le monde des normes. En tant qu'outil de *soft power*, la normalisation représente en premier lieu un canal de diffusion de la culture économique d'un pays. L'internationalisation d'un usage traduit en effet l'expansion d'une pratique culturelle : la norme ISO 9001 (*Management de la qualité*) constitue un bon exemple, en diffusant des pratiques professionnelles anglo-saxonnes.

Levier d'influence américain afin de soutenir sa puissance économique au niveau mondial, les travaux de normalisation témoignent aujourd'hui de l'émergence de la Chine et de l'influence croissante de ses entreprises à travers les organismes tels que l'ISO, UIT ou encore le 3GPP. Active et impliquée dans la définition des règles du monde numérique, l'émergence chinoise traduit le nouveau rapport de force entre la Chine et les Etats-Unis, illustré par la confrontation technologique autour des normes et infrastructures de la 5G.

Au cœur de cette nouvelle configuration internationale, l'Europe apparait comme positionnée pour défendre ses intérêts et promouvoir son économie, grâce à la place unique du CEN-CENELEC et à la présence centrale de l'Allemagne et de la France dans les instances internationales (respectivement 1ère et 6ème à l'ISO au nombre de secrétariats de TC, PC et SC)[7].

L'enjeu pour l'Europe et pour la France est double : promouvoir leurs intérêts et leur économie au sein d'un monde de plus en plus polarisé par la rivalité sino-américaine, mais également incarner une position intermédiaire dans le rapport de force entre mondialisme et souverainisme.

En effet, les technologies du numérique, par les enjeux qu'elles posent en termes de dépendance, d'autonomie et d'influence, apparaissent comme le nouvel espace principal de ces préoccupations de souveraineté.

Au regard de l'intensité de l'activité américaine et chinoise en matière de normalisation des technologies de l'information et de la communication, les ressources et compétences européennes dans les secteurs stratégiques - IA, Cloud, Cyber ou encore Quantique - imposent aux pays de l'Union Européenne de faire valoir leur vision et de développer leur influence, tout en se protégeant des offensives technologiques et économiques.

[7] En 2020, l'Allemagne comptait 130 secrétariats à l'ISO (TC, PC et SC) et 676 membres. La France comptait 75 secrétariats et 608 membres.

L'Intelligence Artificielle, un enjeu de souveraineté et de compétitivité

L'Intelligence Artificielle concentre ainsi un grand nombre des enjeux stratégiques futurs : contrôle des infrastructures, souveraineté des données, technologies duales, écosystèmes connectés ou encore couche cognitive et impacts sociétaux.

Par les innombrables types d'applications qu'elle peut recouvrir, l'IA se destine à constituer un système multisectoriel et interconnecté. L'exemple de la ville intelligente (smart city) nous permet d'appréhender aujourd'hui les contours d'un écosystème connecté et d'en ressortir les premières attentes :

- L'Interopérabilité apparait comme le prérequis au fonctionnement de tout écosystème connecté. La dimension transverse et l'implication totale de l'IA dans l'économie de demain impose une réflexion anticipée sur la manière de faire le lien entre les secteurs d'activités et les technologies. Dans cette économie interconnectée, le fonctionnement en silo apparait comme obsolète et constituerait un frein majeur à l'innovation. La mise en place d'une grille de lecture commune et transversale sur les grands principes de l'IA et de son application représente une condition préalable au développement de cette dernière.

- La souveraineté des actifs liés à l'IA (infrastructures, technologies et données) s'impose également comme un enjeu central pour sa maîtrise et son développement. La criticité de nombreuses applications et les données utilisées engagent des exigences tant sécuritaires que démocratiques. Les applications liées à la santé, à la Défense, à la sécurité publique, mais également aux données comportementales, ne sauraient évoluer dans un environnement de confiance si leurs différentes couches technologiques ne font pas l'objet de conditions maîtrisées et choisies. De la même manière, le patrimoine technique et scientifique français tel que les technologies duales, les travaux de R&D et les projets d'innovation nécessitent le même niveau de maîtrise et d'autonomie.

- La confiance représente enfin la clef de voute du développement de l'Intelligence Artificielle. Au regard de l'imbrication de cette dernière dans l'économie, chacun sera non seulement utilisateur et consommateur, mais également acteur de l'IA. Définir sa nature, son cadre d'utilisation, ses limites et ses objectifs s'impose alors comme une action prioritaire pour penser et choisir la place de l'humain dans ces écosystèmes d'IA.

Face à ces perspectives, l'enjeu pour l'écosystème français et européen est d'être partie prenante de la définition des règles de ce futur environnement. Les ressources humaines, scientifiques et technologiques peuvent nous permettre d'occuper une place face aux grands acteurs américains et chinois.

Cette influence découlera notamment de notre capacité à conserver des filières industrielles puissantes et capables de défendre leurs intérêts de manière coordonnée, de la mobilisation des PME et *start-ups* qui constituent un vivier stratégique important dans le secteur de l'IA, et de l'implication des acteurs scientifiques dans les travaux de normalisation.

Pour ce faire, une organisation fondée sur la coopération est indispensable pour construire une vision forte et convaincante qui puisse être défendue au niveau européen et promue au niveau international. La mise en place d'une feuille de route nationale proposant des stratégies d'influence est ainsi nécessaire pour promouvoir la position française et valoriser ses intérêts.

I. Les caractéristiques de la confiance

En matière d'IA, le besoin de très haut niveau, politique et sociétal, tel qu'exprimé par la Commission européenne est de disposer d'une IA de « confiance ». La confiance est un concept abstrait qui va nécessiter une mise en œuvre opérationnelle pour s'appliquer au monde du numérique.

Le travail de la normalisation va permettre de traduire des besoins règlementaires en spécifications techniques utilisables notamment par les entreprises. La démarche va consister à décomposer la « confiance » en caractéristiques, elles-mêmes redécomposées, jusqu'à obtenir des éléments manipulables, vérifiables, et dans certains cas, certifiables.

La principale difficulté provient que de nombreux termes et concepts liés à la « confiance » restent fondamentalement mal définis et donc sources d'interprétations divergentes et d'incertitudes juridiques. Parmi les termes et concepts à clarifier, on peut notamment citer : l'explicabilité, l'interprétabilité, la transparence, la robustesse, la supervision, l'auditabilité, la souveraineté, l'équité (« *fairness* ») ou encore la responsabilité.

De plus, les caractéristiques de la confiance ne sont pas nécessairement indépendantes les unes des autres et il existe de nombreux recouvrements. Ainsi, l'explicabilité, caractéristique de la confiance induite par la dimension *« boîte noire de l'IA »*, est déjà une caractéristique intrinsèque de la sécurité mais pas seulement puisqu'elle intervient également dans les exigences d'équité (non-discrimination).

On notera que l'imbrication des caractéristiques de la confiance, notamment autour de la sécurité, peut expliquer en partie les réticences actuelles des secteurs « conventionnels » des systèmes critiques à adhérer à une démarche horizontale. Cette situation pourrait néanmoins évoluer.

Au niveau européen, il semble y avoir un consensus pour qu'un certain nombre de caractéristiques de la confiance fasse l'objet d'un traitement prioritaire au titre du développement du référentiel normatif soutenant le projet de règlementation européenne (Articles 13 (*Transparency and provision of information to users*), 14 (*Human oversight*), 15 (*Accuracy, robustness and cybersecurity) et* 52 (*Transparency obligations for certain AI systems*) et 5 (*nudging*)[8]…).

Après prise en compte de l'ensemble des éléments nationaux, européens et internationaux, la liste de ces caractéristiques prioritaires retenue pour la stratégie française de normalisation est :

- La sécurité
- La sûreté
- L'explicabilité (dont interprétabilité, auditabilité)
- La robustesse
- La transparence
- La supervision et la contrôlabilité
- L'équité (dont non-discrimination)

Chaque caractéristique devra faire l'objet d'une définition, d'une description du concept,

[8] *Nudging : concept associé à la manipulation subliminale issue d'un profilage par l'IA (reconnaissance des émotions…), suivi d'une stratégie pour inciter un acteur à agir statistiquement d'une certaine façon*

des exigences techniques et des métriques et contrôles associés.

La caractéristique de sécurité devra être traitée en partenariat avec les secteurs applicatifs dans une approche conjointe. La prise en compte de l'approche système, avec ses différentes variations sectorielles, est en effet indispensable.

La caractéristique de sûreté, intégrant les dimensions « Privacy » et « Confidentialité » devra être traitée selon les processus du domaine « Cybersécurité ». En France, une liaison avec la CN-cybersécurité et l'ANSSI devra permettre de garantir une compréhension commune, une coordination et une couverture des besoins. Au niveau Européen, une liaison avec le CEN-CENELEC JTC 13 et l'ENISA devra être recherchée.

A terme, d'autres caractéristiques de la confiance devront être développées et normalisées, par exemple la traçabilité, les biais, le *nudging*, ou encore la résilience.

La traçabilité pourrait en effet s'avérer être un élément important juridiquement et techniquement tant dans la dimension qualité des données et des systèmes d'IA que dans l'explicabilité du comportement de ces IA. De même, le *nudging* (manipulation subliminale) pourrait s'avérer à terme être un enjeu sociétal majeur qu'il convient de préciser, tout comme la reconnaissance faciale.

Il conviendra de profiter de travaux extérieurs pour soutenir ces sujets.

II. Conformité des organisations en matière de gouvernance, management et certification des systèmes d'IA

Les organisations utilisant ou développant des systèmes d'IA

La transformation numérique des organisations, désormais bien entamée, va subir une forte accélération avec la généralisation des techniques d'IA à tous les niveaux : gouvernance, management, utilisation et conception de nouveaux produits et services à base d'IA etc.

Cette transformation en profondeur va nécessiter un nouveau leadership et une nouvelle gouvernance des organisations qui devront s'adapter et démontrer leur prise en compte de toutes les dimensions des implications de l'IA : recrutement et formation des personnels, gestion des risques, nouvelles exigences règlementaires et sociétales, nouveaux processus et outils de production, nouvelles stratégies de validation et de tests, etc...

In fine, les entreprises démontrant leur aptitude à développer et utiliser des systèmes à base d'IA, et notamment les systèmes à risques (selon la typologie des risques définie par la Commission européenne), seront considérées comme matures et « digne de confiance ».

Cette aptitude des entreprises à prendre en compte l'ensemble des dimensions de l'IA fait l'objet d'un projet de norme ISO/IEC 42001, en cours de rédaction. Tout comme la norme ISO 9001, référence internationale, qui s'intéresse au management de la qualité, les entreprises manipulant de l'IA exigeront chacune que leur écosystème démontre également leur aptitude et leur engagement à développer et utiliser des IA de confiance. L'ISO 42001 pourrait donc se généraliser à l'ensemble de l'écosystème économique développant ou utilisant des systèmes à base d'IA.

En support, de la norme ISO 42001, une norme sur le management des risques, ISO CD 23894.2 est également en cours de développement.

Une analyse approfondie de ces deux normes devra être effectuée pour décider si elles sont suffisantes, ou si elles devront être complétées par des normes portant sur :

- L'identification des risques (*Risk identification*)
- L'évaluation (probabilité et impact) des risques IA (*Risk assessment*)
- Les mesures d'atténuation des risques IA (*Risk mitigation*)
- Un catalogue de risques IA (*Risks catalogue*)

Les organismes de certification

Parmi les organisations très concernées par l'IA, notamment au titre de la conformité aux exigences règlementaires, on trouve les organismes de certification indispensables au déploiement des systèmes à haut risque (selon la typologie de la Commission Européenne).

Les organismes de certification devront être accrédités et démontrer leur aptitude à effectuer des opérations de certification. Un

référentiel normatif décrivant leurs compétences est donc nécessaire, notamment dans un cadre européen où une compétition vers le bas sur la certification des organismes, produits ou services pourrait se développer au détriment des utilisateurs.

Deux normes vont donc devoir être envisagées :

- Une norme (ISO 17021 Partie XX) portant sur les exigences de compétences pour les organismes de certification en matière de système de management (future ISO 42001), et inclure éventuellement des aspects de la norme sur le management des risques (future ISO CD 23894.2),

- Une norme (ISO 17065 Partie XX) portant sur les exigences de compétences pour les organismes de certification en matière de produits, processus et services à base d'IA.

III. Favoriser l'innovation

Au regard du cadre règlementaire se mettant en place en Europe sur l'IA, des inquiétudes s'expriment quant à l'impact sur les capacités d'innovation des entreprises d'une réglementation trop stricte et de normes contraignantes. Il est fréquent d'entendre de la part des différents acteurs de l'IA en Europe - et en particulier les PME et *start-ups* - qu'à trop vouloir réguler l'Intelligence Artificielle, les pouvoirs publics risquent aussi de freiner l'innovation.

Il convient tout d'abord de clarifier la différence entre règlementation et normalisation parfois source d'incompréhension pour les entreprises. Les normes - qui restent volontaires - arrivent parfois en appui d'une règlementation. Elles sont là afin d'aider à l'implémentation des décisions règlementaires au niveau de l'industrie, du terrain et à leur clarification.

Comme le souligne le commissaire européen Thierry Breton, la Règlementation européenne apportera "*une sécurité juridique*" permettant aux entreprises européennes de développer leurs produits et services d'IA en conformité avec un "environnement règlementaire stable" *inscrit dans la durée* et "*favorisant ainsi l'innovation*" et la confiance des utilisateurs.

Il apparaît donc essentiel que les entreprises s'impliquent dans la rédaction des normes qui accompagneront la règlementation afin de positionner leur technologie sur le marché. En effet, le dispositif de certification européen pour une IA de confiance pourrait être le premier au monde et s'exporter à l'instar d'autres marquages CE favorisant ainsi l'export de technologies nouvelles européennes sur l'IA par les normes.

Un tel dispositif de certification en Europe nécessite ainsi une vraie politique d'accompagnement des *start-ups* et PME afin de s'assurer qu'elles auront les moyens de se préparer à la mise en conformité règlementaire de leurs produits et à l'adoption des standards européens.

Par ailleurs, on note une réelle inquiétude devant la difficulté d'accès aux normes – et à leur compréhension – qui s'amplifie en raison de la multiplication des initiatives normatives sur l'IA à l'international.

A ce titre, la mise en place d'un guichet unique au niveau régional peut constituer une source de simplification, en centralisant les réponses aux préoccupations réglementaires et normatives tout en permettant de remonter les besoins terrains et les différentes propositions provenant des acteurs de l'innovation.

Plusieurs recommandations sont formulées afin de répondre aux inquiétudes soulevées :

- Simplifier l'accessibilité à la norme par le développement d'outils ad hoc. C'est le sens des travaux actuels à l'ISO, au CEN et dans d'autres instances sur les « *smart standards* » ou normes intelligentes dématérialisées. Un tel outil permettrait d'intégrer rapidement les normes et la règlementation existantes dans les processus de conception et de qualification d'un produit/système d'IA, d'identifier les manques et de mener les actions correctrices.

- Mise en place d'un accompagnement efficace des entreprises dans leur mise en conformité : déblocage de ressources afin d'aider les entreprises à contribuer davantage aux normes, prise en compte des coûts de mise en conformité dans la phase de développement, éléments de langage à destination des investisseurs, formation à l'outil normatif, sensibilisation des acteurs

etc. Pour répondre à ces objectifs, AFNOR a mis en place un partenariat avec France Digitale.

En effet, la participation à la normalisation dans l'IA constitue un gain important de connaissances et de méthodes pour les *start-ups* impliquées. La participation aux travaux de normalisation permet d'une part de prendre connaissance de méthodes et de références optimisant les processus d'innovation. D'autre part ils permettent pour les *start-ups* de diffuser elles-mêmes des idées disruptives afin de faire évoluer le marché dans leur intérêt.

Par une participation aux règles du jeu du marché, les *start-ups* et PME peuvent ainsi se créent les conditions favorables au partage et au développement de nouveaux produits et services.

IV. Les approches sectorielles

En matière d'approche règlementaire sur l'IA, la Commission a examiné différentes options stratégiques pour assurer le bon fonctionnement du marché unique en créant les conditions nécessaires au développement et à l'utilisation d'une IA digne de confiance dans l'Union. Quatre options stratégiques comportant différents degrés d'intervention réglementaire ont été évaluées :

- Option 1 : un instrument législatif européen mettant en place un système de labélisation volontaire ;
- Option 2 : une approche sectorielle, "ad-hoc" ;
- Option 3 : un instrument législatif horizontal de l'UE suivant une approche proportionnelle fondée sur le risque ;
- Option 3+ : un instrument législatif horizontal de l'UE suivant une approche proportionnelle fondée sur le risque ainsi que des codes de conduite pour les systèmes d'IA ne présentant pas de risque élevé
- Option 4 : un instrument législatif horizontal de l'UE établissant des exigences obligatoires pour tous les systèmes d'IA, quel que soit le risque qu'ils présentent.

Selon la méthodologie établie par la Commission, chaque option politique a été évaluée en fonction de ses impacts économiques et sociétaux, avec une attention particulière pour les impacts sur les droits fondamentaux.

L'option privilégiée est l'option 3+, un cadre réglementaire pour les systèmes d'IA à haut risque uniquement, avec la possibilité pour tous les fournisseurs de systèmes d'IA sans risque de suivre un code de conduite. Les exigences porteront sur les données, la documentation et la traçabilité, la fourniture d'informations et la transparence, la surveillance humaine, la robustesse et la précision, et seront obligatoires pour les systèmes d'IA à haut risque. Les entreprises qui introduiraient des codes de conduite pour d'autres systèmes d'IA le feraient sur une base volontaire.

Le projet européen de régulation de l'IA (AI Act) s'inscrit donc dans « *une approche horizontale pour libérer le potentiel de l'intelligence artificielle dans tous les domaines. Une technologie à vocation transversale ne peut être efficacement réglementée que par des règles horizontales qui fournissent des solutions aux défis communs.* » (Thierry Breton).

De fait, l'IA est une technologie horizontale qui irriguera tous les secteurs économiques et sociétaux (santé, éducation, aéronautique, automobile, énergie, télécommunications…).

En conformité avec l'approche horizontale de la Commission Européenne, les racines de l'IA, à savoir l'utilisation des données avec des méthodes mathématiques et statistiques, militent pour le développement d'un socle commun normatif, socle horizontal dont l'épaisseur reste néanmoins à identifier et à concrétiser de façon opérationnelle.

Si le débat entre la normalisation horizontale et la normalisation sectorielle (ou métier) n'est pas nouveau, la normalisation de l'IA pose désormais de façon particulièrement aigüe la question d'un « dé-silotage » des activités normatives.

Historiquement, les différents secteurs d'activités n'ont eu que des interactions très limitées : les spécificités sectorielles l'emportant largement, une approche en silo avait tout son sens.

Les industries des systèmes « critiques » (Energie, Transport…) se sont structurées par secteur d'activité et se sont concentrées sur les critères de « sécurité » et de « sûreté » au titre de la « *sécurité des personnes et des biens* ». D'autres secteurs (Banque-assurance, …), moins concernés par la sécurité des personnes, se sont eux intéressés, toujours dans une approche sectorielle, aux conséquences de l'utilisation de l'IA au titre des risques juridiques et financiers pour leur activité (risque sur la discrimination des personnes dans l'attribution des prêts par exemple).

Cette situation privilégiant les approches sectorielles est en train d'évoluer du fait :

- De l'approche systémique notamment dans la gestion des risques et de la Safety,
- Du renforcement des technologies « horizontales » du numérique dans la valeur ajoutée des produits.

Par effet domino, cette transversalité intrinsèque des technologies du numérique génère la création d'un monde de services reposant sur la valorisation de la donnée où tous les produits sont susceptibles d'être interconnectés. De fil en aiguille, apparaissent le besoin d'interconnectivité et d'interopérabilité intersectorielles des systèmes d'IA et des données ainsi qu'une dépendance à des outils et méthodes de conception et de qualification des systèmes d'IA multi-sectoriels.

Ainsi, à titre d'exemple, les véhicules « autonomes » devront être interopérables avec les routes intelligentes, dans le cadre de Smart Cities, et d'une distribution énergétique apportée par les Smart Grids. L'ensemble sera conçu en utilisant des outils et des méthodes de l'Industrie 4.0 s'appuyant sur des jumeaux numériques qui devront être donc interopérables…

En parallèle, certains acteurs majeurs des TIC, forts de leurs compétences en matière de captation, stockage, gestion et valorisation des données, tentent d'investir désormais des domaines a priori en dehors de leur champ d'intervention (média, banque, spatial, automobile etc.). Ces mêmes acteurs veulent s'imposer par la force de leur écosystème, et proposer ainsi des services innovants disruptifs et surtout fortement intégrés (services de la smart city, de la smart mobilité, des smart grids). Ces tentations sont d'autant plus fortes qu'elles sont concomitantes à une baisse du ticket d'entrée de certains secteurs spécialisés (automobile, espace…).

Dans ces conditions, la question de l'articulation entre normalisation horizontale et normalisation sectorielle se pose, tout comme la prise en compte des problématiques de positions dominantes de certains acteurs.

Une articulation possible reposant sur un socle horizontal fédérateur :

Du côté de la normalisation horizontale :

- La terminologie,
- Les concepts de haut niveau liés à la confiance,
- L'identification générique des risques liés aux technologies d'IA,
- Les normes générales sur les risques, la gouvernance et le management de l'IA et des données dans les organisations,
- Les considérations sociétales et éthiques,
- La cybersécurité,
- Les espaces de données,
- L'interopérabilité.

Du côté de la normalisation sectorielle :

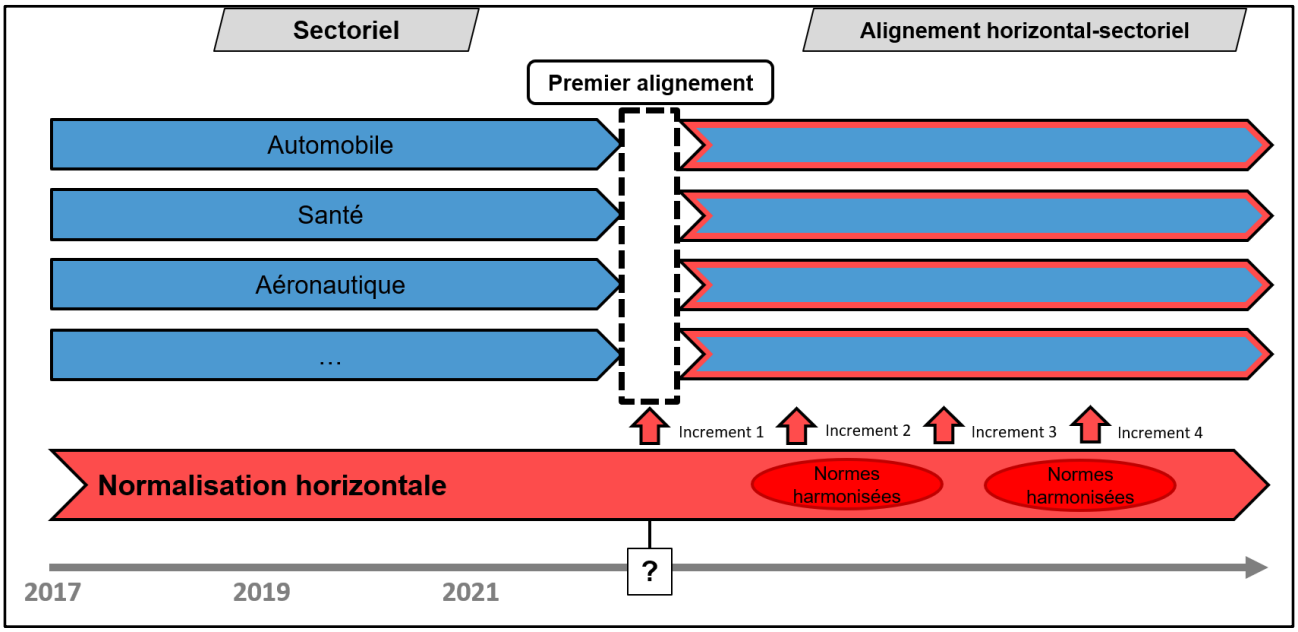
- La déclinaison sectorielle des éléments de la normalisation horizontale,
- La connaissance du milieu, les use case, les analyses de risque propres à ceux-ci,
- La définition des domaines d'emploi,
- La définition des critères et métriques de *sécurité* et de la *sûreté*,
- La définition des stratégies de qualification,
- Les approches « systémiques »,
- Les formats de données spécifiques.

Dans la pratique, il faut développer les échanges entre secteurs de normalisation dans un cadre non-contraignant. Ces échanges pourraient être organisés par la commission européenne, force de régulation et source de financement.

Dans ces échanges, il conviendra de reconnaître les avancées de certains secteurs (aéronautique, automobile, finance…) qui n'ont pas attendus les travaux de normalisation horizontale pour se saisir du sujet.

Certains travaux sectoriels pourraient d'ailleurs être repris dans la normalisation horizontale. On notera à titre d'exemple que la normalisation ISO-IEC s'est très largement inspiré des travaux du secteur automobile pour la définition des niveaux d'automatisation des systèmes d'IA.

Chaque secteur pourrait proposer et détailler les modalités d'articulation entre normalisation horizontale et sectorielle et esquisser une démarche d'alignement selon le schéma suivant :



Le cas particulier de la Défense

En matière de normalisation IA, le secteur Défense nécessite une analyse particulière dans la mesure où une exemption Défense de la règlementation européenne sur l'IA est envisagée.

Cette exemption pourrait laisser penser que la Défense ne sera pas concernée par le corpus normatif international et européen qui accompagnera la règlementation.

Les principes de gouvernance des entreprises et des données, et notamment le management de l'IA, vont être définis par des normes civiles donnant lieu à la certification des organisations. La certification, ou non, des grandes entreprises à partir de référentiels sera forcément scrutée par des organismes non gouvernementaux (*rating*…), des fonds d'investissement, ou des médias qui pourraient considérer une non-certification comme une source de risques.

Par ailleurs, le secteur de la Défense est largement irrigué par les technologies du numérique issues du monde civil. Les acteurs de la Défense, dont certains fortement duaux, auront dès lors beaucoup de mal à s'affranchir des référentiels normatifs internationaux qui régissent leur propre écosystème industriel.

Enfin, force est de constater que la Défense n'a pas les ressources pour développer et surtout entretenir un référentiel normatif IA complet, sans compter qu'un certain nombre de ses systèmes seront amenés à opérer et interopérer dans des environnements ouverts civils.

La Défense tendra donc mécaniquement à prendre en considération les référentiels internationaux existants, qu'ils soient horizontaux ou sectoriels, notamment dans le cadre des examens de licéité des armements.

Le choix du secteur de la Défense d'adopter, d'adapter, de déroger aux référentiels internationaux ou de construire son propre corpus normatif lui revient. Quel que soit le choix retenu, forcément complexe, il sera difficile d'ignorer une base normative commune horizontale, approuvée au niveau européen, qui serait de plus de nature à

faciliter l'interopérabilité entre systèmes militaires et civils[9].

V. Le rôle de l'Etat

L'enjeu pour l'Etat est d'anticiper et de préparer le tissu économique et industriel français à la future réglementation européenne sur l'IA et la data. Cette anticipation nécessite de contribuer activement au développement d'un corpus normatif accessible, flexible et opérationnel y compris et surtout pour les PME et *start-ups*.

Au regard de la dimension stratégique du numérique, l'Etat a un rôle prépondérant à jouer dans la normalisation de l'Intelligence Artificielle. Comme l'évoquait dès 2012 le Rapport Revel[10], l'influence normative française au niveau international dans les technologies stratégiques nécessite la définition de stratégies « en amont » et la mise en place d'une architecture d'influence et de valorisation de la part de l'Etat.

Penser une stratégie de normalisation homogène et à long terme constitue la brique indispensable d'une politique industrielle. Par une coordination étroite entre le CCPN[11] et les acteurs de la normalisation au niveau interministériel, la priorité doit être donnée à l'identification des enjeux technologiques principaux ainsi que des opportunités et des risques qu'ils entrainent pour l'économie française. Aussi, cette connaissance doit entrainer l'analyse des opportunités normatives au regard des forces présentes au sein du tissu industriel français.

De ce fait, l'adoption d'une approche horizontale – comme engagée par le Commission Européenne sur l'Intelligence Artificielle – permet une compréhension transverse des différents impacts des technologies du numériques. Coordonner les différents secteurs industriels sur ces technologies transverses est nécessaire pour que l'Etat pilote des actions stratégiques efficientes.

Outre cette coordination nécessaire, la structuration des filières apparait comme un élément indispensable pour produire une influence normative forte. Bien que la construction de filières puissantes requière en premier lieu des actions de la part des entreprises, l'Etat peut jouer un rôle sur l'articulation entre les différentes composantes de la filière (l'éducation, la recherche académique, le développement, les entreprises, les acteurs publics et dans certains cas, l'armée). Au niveau sectoriel en effet, l'influence d'une filière dépend en grande partie de sa capacité à avancer de manière cohérente et multipartite.

Les actions de soutien opérationnel doivent également être renforcées afin de valoriser les

[9] Nota : le Fond Européen de Défense prévoit le financement d'activités de normalisation

[10] https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/14133.pdf

[11] Comité de coordination stratégique et de pilotage de la normalisation

ressources françaises en matière de technologies du numérique.

Comme souligné par un grand nombre d'acteurs, l'implication des *start-ups* et PME dans la normalisation n'est pas suffisante, du fait de la complexité des processus normatifs, mais également par manque de sensibilisation à la dimension stratégique de la normalisation. Ces dernières doivent ainsi être accompagnées et valorisées en termes de pédagogie et de conseil.

A l'image des stratégies de soutien observés dans d'autre pays comme l'Allemagne et les Etats-Unis, l'intégration des *start-ups* et PME aux travaux de normalisation est réalisée par des coopérations public-privé. L'identification et le ciblage des *start-ups* stratégiques pour la politique industrielle française doivent être soutenu par un accompagnement dans leur influence normative et par une action de suivi de la part de l'Etat.

De la même manière, l'Etat doit encourager la participation des acteurs académiques dans les travaux de normalisation du numérique. Alors que dans un grand nombre de pays – notamment européens – on constate une collaboration entre chercheurs et industriels dans l'élaboration des normes, cet engagement fait encore défaut au niveau français, privant les travaux de normalisation de la haute expertise disponible dans les technologies du numérique.

Alors que ce constat est identifié depuis de nombreuses années – déjà au sein du rapport de la Délégation Interministérielle à l'Intelligence Economique daté de 2012[12] -, nous pouvons constater que les recommandations successives n'ont jamais été implémentées durablement et structurellement.

Pour encourager la participation des acteurs académiques à la normalisation et à la certification règlementaire, une réflexion sur le calcul du Crédit Impôt Recherche doit être envisagé.

La prise en compte de la participation des chercheurs aux travaux de normalisation dans le CIR est un premier pas mais nécessiterait d'être élargie[13].

Ainsi, sur les sujets considérés comme stratégiques ou qui soutiennent directement la réglementation, le calcul du CIR pourrait prendre en compte non seulement la participation en termes de temps, mais également les contributions fournies aux commissions de normalisation. La participation effective en termes d'action ainsi que l'implication au niveau européen et international devraient également être inclues dans le calcul du CIR.

La mise en œuvre de contrats de consultance entre chercheurs et industriels ou encore l'ajout de la contribution aux travaux de normalisation dans le calcul de l'indice h sont autant de propositions régulièrement publiées qui n'ont pas fait l'objet de mise en place opérationnelle.

Au regard des enjeux stratégiques des technologies du numérique, du besoin complexe de transversalité qu'elles entrainent, et de la nature systémique de leurs impacts, une mobilisation des acteurs académiques semble urgente et indispensable.

[12] https://sisse.entreprises.gouv.fr/files_sisse/files/outils/rapports/synthese_publique_rapport_normalisation_11_janvier_2012.pdf

[13] https://bofip.impots.gouv.fr/bofip/6507-PGP.html/identifiant%3DBOI-BIC-RICI-10-10-20-50-20160706

Structurer la coopération et les financements : un NIST à la française ?

Pour mettre en place une véritable force d'influence française dans l'Intelligence Artificielle, il serait nécessaire de structurer davantage la gouvernance et d'accentuer la coopération entre le monde de la recherche, l'application industrielle et les travaux normatifs.

La mise en place d'un centre de compétences étatique en matière d'Intelligence Artificielle (Intégrant la robotique et les données) pourrait être envisagée sur le modèle de l'ANSSI ou de l'ENISA. Pour mémoire, l'ANSSI combine des compétences techniques, une implication dans la règlementation, la normalisation et l'audit, et est garante de la souveraineté de l'Etat pour la cybersécurité. Cette structure est répliquée au niveau européen par l'ENISA.

Aux Etats-Unis, l'Etat fédéral dispose du NIST, centre de compétences couvrant les activités de normalisation du numérique. Ce dernier mobilise les chercheurs et les industriels afin de développer les technologies du numérique, la métrologie et les normes correspondantes. Cette approche intégrée - de la recherche fondamentale à l'application industrielle conforme à des standards - constitue un outil d'influence et de rayonnement économique central dans la stratégie américaine.

Soutenu tant politiquement que financièrement - plus d'1 milliard de dollars de budget en 2021 - le NIST occupe une place de premier plan au sein de la task force « stratégie scientifique et technologique internationale » des Etats Unis. Il est notamment considéré comme une structure clef de l'écosystème d'Intelligence Artificielle américain, et comme point de rencontre entre les différents acteurs de la chaîne de valeur.

Preuve de son rôle stratégique, la Commission de Sécurité Nationale sur l'Intelligence Artificielle considère qu'il doit « diriger la communauté IA », et plaide pour une augmentation de 64 millions de dollars du budget de sa R&D afin de l'intégrer davantage dans la recherche militaire.

Par ailleurs, la transversalité des activités du NIST permet des programmes de recherche intégrant plusieurs dimensions (IA, robotique, données), à l'origine de développements particulièrement adaptés aux enjeux horizontaux des technologiques du numérique.

En conséquence, une structuration des ressources et des expertises régaliennes des technologies du numérique sur le modèle du NIST, venant en soutien d'une politique publique de la recherche à la normalisation, pourrait ainsi permettre de valoriser l'Intelligence Artificielle française au sein d'une structure favorisant les synergies.

La mise en place d'une stratégie adaptée de la part de l'Etat requiert des compétences techniques d'autant plus importante que les enjeux de souveraineté, de sécurité sont prégnants.

En ce sens, la seconde phase de la stratégie nationale en IA, présentée par Cédric O en novembre 2021 apporte des premières réponses, tant dans le soutien à la recherche sur l'IA de confiance, que dans le renforcement des formations.

Sur l'Intelligence Artificielle, il est impératif de disposer d'une expertise à des niveaux ciblés, comme par exemple au sein des équipes

gérant les appels d'offre publics ou les programmes de financement. L'utilisation de l'IA par les organismes publics et administratifs nécessite également une maîtrise de son fonctionnement et des normes associées.

De la même manière, la compréhension précise des enjeux d'intelligence économique à tous les niveaux de la chaine technique apparait comme essentielle. Comprendre les conséquences et les objectifs d'un projet de développement algorithmique, d'un partenariat de recherche, ou encore de la modification d'une exigence dans une norme nous assurera la maîtrise de la technologie, par une meilleure appréciation des intérêts français. Cette stratégie de veille et de maîtrise technique des enjeux conduira en outre à un ciblage plus fin des actions à implémenter.

Par ailleurs, dans la cadre de la consultation nationale sur la normalisation de l'IA, une grande majorité des acteurs de l'IA ont exprimés le souhait d'une plus forte implication de l'Etat dans la normalisation des sujets sociétaux et éthiques, à l'image des problématiques d'identification numérique et de reconnaissance faciale.

Or, à ce jour, les actions envisagées par les entreprises portent davantage sur les questions de sécurité et fiabilité des systèmes d'IA que sur les problématiques éthiques, laissant l'Etat comme seul dépositaire des enjeux sociétaux et éthiques de l'IA.

Ainsi, l'Etat doit développer ses compétences techniques, d'une part pour effectuer des choix stratégiques en matière d'investissements et d'orientations des politiques publiques, et d'autre part afin d'accompagner les actions d'influence menées par les entreprises françaises au niveau normatif, réglementaire et économique.

VI. Les enjeux Européens et internationaux

Dans le monde numérique, encore plus qu'ailleurs, la normalisation va sous-tendre et accompagner la règlementation. La prise en compte des problématiques technico-sociétales (éthique, discrimination…) dans les activités de normalisation renforce l'importance de la défense des intérêts sociétaux, industriels et économiques européens dans les normes internationales. En effet, l'Europe structure son marché selon un principe d'ouverture et s'appuie autant que possible sur des normes internationales, notamment sur celles de l'ISO-IEC.

En raison des enjeux d'interopérabilité du monde numérique, les normes sur l'Intelligence Artificielle devront principalement être développées à l'international. Une stratégie française de normalisation en IA doit certes être consolidée au niveau national afin de s'entendre sur les besoins les plus importants, mais cette stratégie doit être portée et valorisée à l'international. Ainsi, la production d'une cartographie des différentes instances productrices de normes et standards doit permettre d'identifier les alliances à construire pour promouvoir nos intérêts.

En effet, au regard des enjeux économiques, de très nombreuses organisations, nationales et internationales, essaient d'influer sur la normalisation de l'IA et produisent parfois des documents de nature quasi-normative. Il est parfois très compliqué, même pour les spécialistes les plus aguerris, de naviguer dans l'ensemble des documents et d'identifier le référentiel le plus pertinent. Si ce foisonnement met en relief le besoin de référentiels techniques partagés, l'effet final peut être contraire à l'intérêt collectif : trop de normes tue la norme.

Ainsi, à ce jour, on constate des activités sur l'IA dans les organismes de normalisations traditionnels : à l'ISO-IEC, à l'ITU, ou au CEN-CENELEC. Les consortia internationaux produisent également des travaux de standardisation à l'image de l'IEEE ou de l'ETSI. Les domaines techniques (automobile, aéronautique, santé, ferroviaire…) ont également tendance à développer des référentiels normatifs sectoriels, que ce soit au travers des bureaux de normalisation nationaux ou au travers d'organisations plus spécifiques comme SAE ou EURCOCAE. Enfin, les organisations internationales telles que l'ONU ou l'OCDE s'emparent également du sujet, et de très nombreuses structures, sans avoir le statut d'organisation de normalisation, essaient également de développer des standards de fait.

Force est de constater que les problèmes rencontrés par l'ensemble des acteurs sont toujours les mêmes et commencent systématiquement par des problèmes de terminologie. A moins d'accepter une tour de Babel normative et règlementaire, il est indispensable de reposer sur un corpus terminologique et conceptuel unifié : il ne peut s'agir que de celui de l'ISO-IEC.

D'une façon générale, le cadre normatif devra être le plus générique et transverse possible. Ce cadre sera fourni préférentiellement par l'ISO-IEC. Une éventuelle adaptation pourra être faite au niveau Européen par le CEN-CENELEC pour s'assurer du bon alignement avec la règlementation.

Par ailleurs, on ne peut ignorer les spécificités européennes qui vont structurer la normalisation : Green Deal, AI Act, Data Act, Data Governance Act… sont autant de politiques européennes qui vont à la fois utiliser des normes, orienter des travaux de

normalisation, et éventuellement aboutir à développer des normes purement européennes.

Parmi les spécificités européennes, on retiendra, non seulement l'élargissement de la notion de risques au respect des droits fondamentaux et des valeurs et principes qui fondent l'Europe, mais aussi le calendrier législatif. A ce jour, les hypothèses de travail fournies par la Commission Européenne, sont une promulgation de l'AI Act début 2023, avec une applicabilité prévue 2 ans plus tard.

Les normes harmonisées européennes soutenant l'AI Act devront donc être disponibles au plus tard d'ici fin 2024, et donc être présentées à l'homologation début 2024. Or, il apparaît d'ores et déjà que certaines exigences règlementaires pourraient ne pas être couvertes par l'ISO-IEC au regard des délais de développement des normes. Des solutions alternatives doivent donc être étudiées, notamment si nécessaire auprès d'autres organismes de normalisation (IEEE, SAE…). Le développement de normes européennes spécifiques, avec un temps d'élaboration plus court, permettrait si nécessaire de ne pas laisser se développer une incertitude règlementaire et apporterait au tissu économique européen un cadre normatif suffisant pour ne pas freiner l'innovation.

Un partage de vision et une concertation avec d'autres partenaires européens, notamment l'Allemagne, pourrait être envisagée lors de la présidence française de l'Union Européenne. A cet égard, la mobilisation et le soutien des acteurs étatiques pour porter les messages d'urgence et de besoin d'un pilotage politique des activités de normalisation du numérique est indispensable.

VII. Les axes stratégiques de la normalisation

Au regard de cet état des lieux et afin de répondre aux enjeux évoqués, il est proposé de structurer la stratégie nationale de normalisation de l'IA en 6 axes.

Axe 1 : Développer les normes portant sur la confiance (exigences, critères et métriques)

Un consensus international se développe autour de la notion de confiance qui doit s'organiser autour d'un ensemble de caractéristiques vérifiables[14]. Il en ressort néanmoins que les caractéristiques seront nombreuses, qu'elles auront de nombreux recouvrements et intersections, et qu'elles devront être sélectionnées en fonction des besoins du marché et des analyses de risques sectorielles particulières.

A ce jour, dans le cadre d'une stratégie nationale, les caractéristiques prioritaires à normaliser retenues sont :

- La sécurité
- La sûreté
- L'explicabilité (dont interprétabilité, auditabilité)
- La robustesse
- La transparence
- L'équité (dont non-discrimination)

Chaque caractéristique devra faire l'objet d'une définition, d'une description du concept, des exigences techniques et des métriques et contrôles associés.

La caractéristique de *sécurité* devra être traitée en partenariat avec les secteurs applicatifs dans une approche conjointe. La prise en compte de l'approche système, avec ses différentes variations sectorielles, est en effet indispensable.

A terme, d'autres caractéristiques de la confiance devront être développées et normalisées, par exemple la traçabilité, les biais, la résilience, la souveraineté…

De plus en plus de systèmes d'IA vont évoluer dans des environnements ouverts, c'est-à-dire dans des environnements non contrôlés ou faiblement contrôlés. Les environnements ouverts se caractérisent par la variabilité des scénarios possibles et l'imprévisibilité de certains événements.

---

[20] *Trustworthiness (Source ISO/IEC TR 24028:2020(en)) : ability to meet stakeholders' expectations in a verifiable way*

Note 1 to entry: Depending on the context or sector and also on the specific product or service, data and technology used, different characteristics apply and need verification to ensure stakeholders expectations are met.

Note 2 to entry: Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability.

Note 3 to entry: Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

Le développement des systèmes d'IA, notamment dans le cas du *machine learning*, pose alors la question du domaine d'emploi[15], de sa spécification et sa qualification, ainsi que sa supervision pour que le système reste bien dans son domaine d'emploi lors de son utilisation.

La notion de « domaine d'emploi » avec ses différentes implications techniques voire juridiques devra être précisée et normalisée.

A titre d'illustration, le besoin de supervision des systèmes d'IA va impliquer que ces derniers soient repris en main lors d'une sortie de domaine de fonctionnement autorisé. De même, le besoin de *reporting* des incidents sérieux et des dysfonctionnements des systèmes d'IA, tel qu'évoqué dans le projet d'AI *Act* de la Commission Européenne, nécessite également de définir ces concepts notamment pour des audits ultérieurs. En effet, l'alignement et la cohérence des différents domaines seront alors la première ligne d'analyse dans la recherche de responsabilité en cas d'accident.

Axe 2 : Développer les normes sur la gouvernance et le management de l'IA

L'IA génère de nouvelles applications. Elles seront toutes classées dans l'échelle de risques proposée par la Commission Européenne.

Si les risques porteront sur la sécurité des personnes et des biens ainsi que sur le respect des principes et valeurs européennes, l'origine des risques peut être très variée : mauvaise qualité des données, mauvaise conception, mauvaise qualification, mauvaise identification ou compréhension des risques.

Une analyse des risques pour les systèmes à base d'IA est donc essentielle et va obliger les entreprises à s'organiser et mettre en place un certain nombre de dispositifs : management de la qualité et management des risques. Ces dispositifs leur permettront de développer leurs produits et leurs services de s'identifier en tant qu'organisation « digne de confiance » capable de gérer et de développer des systèmes d'IA.

Dans le cadre des travaux ISO/IEC, deux normes sont en cours de développement portant sur :

- Un système de management de la qualité des IA : ISO 42001 (AI management System)
- Un système de management des risques IA : ISO 23894.2 (AI Risk management)

Il est possible que ces normes s'imposent au niveau mondial, de la même façon que l'ISO

[15] *Pour l'IA, différents domaines co-existent : La base d'apprentissage des IA (learning domain) ne va constituer qu'un sous-ensemble de l'environnement opérationnel (operating domain) du futur système d'IA. Cette même base d'apprentissage peut être distincte des spécifications initiales (specified operational domain) ou du domaine de conception (operational design domain) ou du domaine de qualification (qualification domain) voire du domaine de fonctionnement autorisé (authorized operational domain).*

Par ailleurs, il convient d'identifier un domaine d'échec (failure domain) dans lequel des modes de secours et de résilience devront être développés.

9001 s'est imposée comme référence internationale en matière de management de la qualité. Ces normes pourraient à terme constituer des normes harmonisées européennes.

Le caractère opérationnel de ces normes, notamment celle portant sur le management des risques, reste à vérifier. Ainsi, un corpus normatif complémentaire sur les risques est à envisager et pourrait couvrir : l'identification des risques (ainsi qu'un catalogue de risques), l'évaluation des risques (méthode, probabilité, *impact*) et les mesures d'atténuation des risques.

Certains risques liés notamment à la partie « *Sécurité-Sûreté* » resteront très sectoriels, d'autres seront très horizontaux, notamment ceux portant sur l'acceptation sociétale et le respect des valeurs et des principes. L'imbrication de l'ensemble de ces risques, peut générer des risques de nature systémique, c'est-à-dire un risque dont l'occurrence a des conséquences sur plusieurs secteurs d'activités, voire sur toute une économie, bien au-delà du secteur initial.

Une articulation dans la gestion des risques entre approche sectorielle, approche horizontale et approche systémique reste à préciser et pourrait faire l'objet de travaux, voire d'une doctrine nationale et européenne.

Axe 3 : Développer des normes sur la supervision et le reporting des systèmes d'IA

Identifier la place de l'homme dans la conception, la qualification et l'utilisation des systèmes d'IA est essentiel. Il s'agit d'une exigence sociétale, politique et règlementaire qui va entraîner des conséquences fondamentales sur la conception des systèmes, sur l'organisation des entreprises, des organismes de certification, voire sur l'organisation des secteurs critiques.

Il s'agit en effet de s'assurer que les systèmes d'IA sont contrôlables (capacité à reprendre la main), que la supervision (capacité à observer le fonctionnement d'un système, notamment dans les phases critiques), permettra de remettre l'homme dans la boucle de décision aux moments critiques où l'IA sortira de son domaine de fonctionnement nominal.

Enfin, des processus de *reporting*, éventuellement automatisés, devront permettre de faire remonter, conformément aux orientations du régulateur, les incidents majeurs afin de les traiter le plus en temps réel possible avant qu'ils ne se propagent. Les principes de supervision horizontale, sectorielle ou règlementaire restent à définir. En parallèle, les incidents et accidents nécessiteront des capacités d'audit (explicabilité) tant sur les produits que sur les standards sur lesquels ils reposent.

Il s'agit dans la pratique de construire un écosystème de confiance basé sur : la règlementation, la normalisation, la conformité. Ce type d'écosystème, avec les processus *ad hoc*, est déjà en place dans des industries critiques comme l'aéronautique qui dispose par exemple d'un Bureau Enquête

Accident et a une capacité à faire évoluer la règlementation.

Une « tour de supervision » de l'écosystème de confiance est probablement à envisager dans la mesure où des failles, tant dans la construction de la confiance que chez les acteurs qui en sont les garants, ne manqueront pas d'apparaître et devront être traitées avec diligence.

Les besoins de supervision de l'IA devront donc s'articuler autour :

- De la supervision des produits et services lors de leur conception et de leur vie opérationnelle,
- De la supervision des standards, des organisations et d'une manière générale de l'écosystème de confiance

Le premier point est couvert par les critères de la confiance, tandis que le deuxième point pourrait être couvert par la gouvernance des organisations, notamment au niveau national et européen. On notera que la commission européenne envisage de créer un « *European Artificial Intelligence Board* » qui pourrait répondre à ce besoin.

Axe 4 : Développer des normes sur les compétences des organismes de certification

Les organismes de certification vont être au cœur de l'écosystème de confiance européen en matière d'IA, notamment pour les systèmes à haut risques.

Il reviendra en effet à ces organismes de s'assurer, non seulement que les entreprises ont mis en place des processus de développement et de qualification des systèmes d'IA, mais également que les produits sont bien conformes aux exigences notamment règlementaires.

La technicité de l'IA va mécaniquement entrainer un besoin de montée en compétence des organismes de certification qui devront donc embaucher, former leurs personnels, et disposer des méthodes et outils d'évaluation des systèmes d'IA propres à leurs secteurs d'activité.

Au regard du fonctionnement des institutions européennes, la non-existence de normes sur la compétence des organismes de certification serait de nature à biaiser le marché européen en permettant le développement de stratégies de moins-disant tant dans la qualité des évaluateurs que dans la qualité et la pertinence des évaluations.

L'enjeu premier dans la compétence des organismes de certification est de maintenir la confiance dans les produits, les processus et les services. Le deuxième enjeu, tout aussi important, va consister à garantir la crédibilité des institutions européennes dans leur capacité à protéger les citoyens, et à s'assurer que le marché n'est pas biaisé.

Deux normes vont donc *a minima* devoir être envisagées :

- Une norme portant sur les exigences de compétences pour les organismes de certification en matière de système de management spécifique à l'IA,
- Une norme portant sur les exigences de compétences pour les organismes de certification en matière de produits et services à base d'IA.

Axe 5 : Développer la normalisation de certains outils numériques (simulation, jumeaux numériques…)

L'utilisation de la simulation comme source de données et de scénarios, pour la spécification, la conception, l'entrainement, la validation, le test, la qualification et l'audit des systèmes à base d'IA devrait se développer rapidement.

A terme, il est probable que la simulation sera l'un des outils clés de la qualification et de la certification des produits, sans pour autant se substituer intégralement aux besoins de tests réels. Ainsi, la simulation permettra de développer une approche statistique des performances de l'IA avec une grande couverture des scénarios de tests. La grande répétabilité des tests permettra également de mieux comprendre et expliquer certains comportements des systèmes d'IA.

Cette tendance à s'appuyer sur la simulation va générer une nouvelle série de besoins normatifs en matière de qualification des simulations, d'interopérabilité des simulations et des objets (jumeaux numériques) à tester.

L'un des enjeux consistera à disposer de simulations reposant sur des données synthétiques et non plus sur des données réelles. En effet, les données synthétiques ont l'avantage d'être entièrement maitrisables et leur caractère programmable permet d'explorer de nombreux scénarios qui pourraient ne pas exister dans une base de données réelles. On pourrait par exemple avoir une représentation synthétique d'une ville, dans toutes les bandes spectrales optiques et électro-magnétiques, sous différents angles, avec différentes météos à différentes saisons ou heures du jour.

La difficulté des environnements synthétiques provient du besoin de modéliser des phénomènes physiques complexes, des environnements complexes, et d'en maîtriser l'animation. La qualification de tels environnements est un projet à part entière qui a déjà commencé dans certains secteurs.

Au regard des enjeux, et de la complexité des simulations, un rapport technique présentant l'ensemble des enjeux, et une démarche normative possible en lien avec les besoins du marché, doit être développé dans un premier temps.

Axe 6 : Simplifier l'accès et l'utilisation des normes

La complexité du corpus règlementaire et normatif relatif à l'IA, à la donnée et à la confiance est indéniable. Cette complexité risque de générer des craintes auprès de certains acteurs, alors même que l'existence d'un corpus normatif robuste permettrait de soutenir l'innovation en diminuant les incertitudes réglementaires et en facilitant l'interopérabilité et les échanges entre les acteurs économiques.

Afin que la réglementation et la normalisation ne soient pas des freins à l'innovation, mais

des facilitateurs apportant un cadre de confiance, 4 actions sont proposées :

1 **Se rapprocher des acteurs de l'innovation, notamment le Hub FranceIA et France Digitale, mais aussi BDVA/DAIRO au niveau européen**

Il s'agit de s'assurer que le tissu économique national (et européen), porteur de l'intérêt des PME et *start-ups*, s'implique plus fortement dans la normalisation et accompagne les organismes de normalisation dans leur stratégie de normalisation et dans leurs déclinaisons. La participation de ces acteurs, directement confrontés à l'utilisation des normes, doit permettre de s'assurer que les outils et les exigences sur le développement de normes opérationnelles sont bien ciblés.

Ce même tissu de l'innovation peut également être source de besoins normatifs particuliers. Les nouveaux canaux d'échanges entre innovation-recherche et normalisation doivent garantir la prise en compte du point de vue d'acteurs à ce jour faiblement impliqués dans la normalisation.

2 **Développer et préciser la notion de normes « opérationnelles » et militer en ce sens aux niveaux européen et international**

Les normes sont réalisées par des experts internationaux dans le cadre de processus complexes et de compromis sur les termes, les concepts et leurs déclinaisons en spécifications techniques. Les normes, en provenance de l'ISO et l'IEC au niveau international, et du CEN et CENELEC, sont approuvées par les organismes de normalisation des pays concernés dans le cadre de consultations nationales.

Certaines normes peuvent être perçues comme trop complexes, trop éthérées, et trop peu applicables par certains acteurs clés de l'économie. La prolifération normative, et la complexité des normes, peuvent dans certains cas aboutir à l'effet contraire recherché : freiner l'innovation.

Les normes doivent donc être « opérationnelles ». Ce terme recouvre simultanément simplicité de compréhension et facilité de déclinaison et de mise en œuvre par l'ensemble des acteurs économiques, y compris les PME et *start-ups*. Le sujet des normes opérationnelles doit être débattu et traité sans fard, notamment par le tissu économique profond et par les acteurs de l'innovation.

Il est donc indispensable qu'en parallèle du développement des normes, un travail soit effectué pour, d'un côté s'assurer que les normes sont bien opérationnelles, et pour de l'autre côté, s'assurer qu'il y a bien une architecture et une cohérence des standards.

Ce besoin de structurer, cartographier, et d'une certaine façon de hiérarchiser les normes, va être indispensable. Il est à noter que cette structuration devra être nécessairement développée dans le cadre du développement du concept de « *SMART Standard* ».

3 **Rédiger de guides techniques d'accompagnement de l'innovation pour la conception des systèmes d'IA**

De nombreux acteurs s'inquiètent, à juste titre, du « déluge normatif » en cours. A ce jour, plus de 250 documents de nature normative ou prénormative autour de l'IA ont été identifiés par l'organisation StandICT (financée par la commission européenne). Ces documents sont issus de nombreuses organisations de normalisation, qui sont *de facto* en concurrence sur un sujet transverse. Outre que les documents normatifs ou prénormatifs répertoriés ne sont pas tous au même niveau de maturité, ou au même niveau d'intérêt, il sera particulièrement compliqué pour les acteurs économiques de choisir la (ou les) norme(s) appropriée(s) à leur besoin.

L'ambition de cette action consiste à créer un document chapeau pour aider les acteurs à naviguer dans l'ensemble normatif. Il existe plusieurs options pour un tel document, allant du simple guide général pointant, en fonction des besoins, sur des normes particulières, ou d'un guide reprenant les principales exigences des normes sous-jacentes, et répondant aux besoins de la majorité des acteurs.

Ce guide d'accompagnement pourra intégrer une cartographie de la normalisation IA présentée sous forme visuelle. A noter qu'une telle cartographie doit être développée dans le cadre des activités de l'ISO-IEC et du CEN-CENELEC (respectivement SC 42 et JTC 21).

Un débat devra être initié dans les instances nationales et européennes sur la confirmation du besoin et les modalités de réalisation d'un tel document.

4 **Préparer dès à présent la future génération de normes électronique (SMART standards)**

A ce jour, les normes sont soit sous format papier, soit le plus souvent sous format électronique (PDF). Si le format électronique, permet une manipulation plus aisée, il n'en reste pas moins que l'utilisateur final doit lire l'ensemble de la norme, et en extirper lui-même les éléments et spécifications techniques d'intérêt.

Si cette activité ne pose pas de problème pour des normes simples, stabilisées, et surtout non dépendantes d'autres normes, il en va autrement pour les normes du numérique, complexes, fortement évolutives, contenant de nombreuses exigences et dont la manipulation est de moins en moins accessible aux capacités d'une seule personne.

Le concept de *SMART Standard*, en cours de développement par les organismes de normalisation, doit permettre un traitement automatisé des normes. Ainsi un utilisateur devra pouvoir à terme accéder directement aux exigences qui l'intéressent selon des filtres et des outils à définir.

Ce projet d'ampleur va probablement prendre de nombreuses années. Il va nécessiter de revoir les processus d'élaboration et de mise à jour des normes, la façon de rédiger les normes, la cohérence entre ces dernières, et enfin le *business model* des organisations de normalisation appelées à vendre du service et non plus des normes.

Le tissu économique national doit anticiper l'arrivée de ces futurs outils de manipulation et d'accessibilité à la norme, qui devraient contribuer à décomplexifier le corpus normatif et à le rendre plus cohérent.

6. Les angles morts de la stratégie de normalisation

Les échanges avec les différents acteurs ainsi que le suivi des débats européens et internationaux montrent l'existence d'angles morts dans la stratégie de normalisation telle qu'établie à ce jour.

Ainsi, toute la partie normalisation des données reste à construire avec des sujets comme l'interopérabilité des données et des systèmes, les transactions de données, les formats et conventions d'annotations, la qualité, la traçabilité… Ces sujets sont stratégiques car la maitrise des données, leur accessibilité et leur diffusion va conditionner le développement d'un écosystème de l'innovation, l'indépendance par rapport aux grands « capteurs » de données, et donc une souveraineté numérique.

De même, toute la dimension liée à une IA soutenant le développement durable (« *sustainable AI* », « *green AI* » …), en accompagnement du Green Deal de la Commission Européenne, reste à préciser.

Enfin, la normalisation de l'Intelligence Artificielle s'inscrit dans un besoin plus général de sensibilisation aux enjeux du rôle de la normalisation dans la construction d'un cyberespace de confiance. La mise en place d'une stratégie de normalisation globale et cohérente pour la France requiert des transformations de fond. Ce travail à mener peut-être définit par le triptyque suivant : sensibilisation aux enjeux stratégiques de la normalisation et accompagnement de la participation ; simplification administrative ; formation.

Formation et valorisation des carrières en normalisation

Afin de peser davantage dans les processus normatifs, une réflexion sur le vivier d'expert français en normalisation nécessite d'être engagée. La mobilisation des entreprises aux enjeux stratégiques de la normalisation passe ainsi par une véritable organisation sur la formation et la valorisation des carrières.

Tout d'abord, intégrer la normalisation dans les cursus académiques - de pair avec l'apprentissage de l'innovation et du fonctionnement des brevets - apparait comme nécessaire pour opérer cette sensibilisation des futurs décideurs. Plus spécifiquement, les études d'ingénieur nécessitent d'intégrer un apprentissage de la normalisation dans sa dimension stratégique et pas seulement industrielle et processuelle. Des filières de spécialistes en normalisation doivent également être envisagées, comme déjà proposé par des rapports précédents.

Au stade de l'entreprise, une sensibilisation des décideurs à l'importance stratégique de la normalisation est essentielle. Un changement de paradigme vers une valorisation des processus et du cadre de développement industriel est à encourager. A ce titre, il est intéressant d'observer que les grands acteurs du numérique axent leurs ressources financières et le recrutement de profils de haut niveau sur les métiers liés aux outils et aux processus.

Enfin, alors que l'influence des participants dans les instances de normalisation se construit sur une présence à long terme, nécessitant une expertise reconnue et des postes à haute

responsabilité, il convient de développer une véritable stratégie de positionnement des experts afin de construire une influence efficiente. Cette dernière s'appuie donc nécessairement sur des stratégies de carrières réfléchies et soutenues. La formation des experts, l'accompagnement dans les travaux de normalisation, la valorisation des missions et la mise en place d'une stratégie normative interne aux entreprises constituent des pistes de réflexion en ce sens.

Ces angles morts de la normalisation devront être repris et détaillés dans une version ultérieure de la feuille de route nationale.

IX. La feuille de route opérationnelle

Les 6 axes présentés lors de cette stratégie de normalisation de l'Intelligence Artificielle, doivent être implémentés grâce à une série d'actions opérationnelles, tant au niveau prénormatif et méthodologique que dans les travaux de normalisation en cours.

Afin de faire vivre cette stratégie et d'ajuster les actions pertinentes à mettre en place, une plateforme de concertation et de coordination sera créée par AFNOR pour mobiliser les parties intéressées et animer une communauté d'acteur autour de la normalisation de l'Intelligence Artificielle.

Outre la coordination, l'application des directions stratégiques identifiées dépendra de la mobilisation efficiente de toutes les forces concernées. Les filières tout d'abord, qui par leur capacité d'action et leurs ressources possèdent la taille critique pour peser dans l'élaboration du cadre normatif de l'IA. La bonne coordination et l'identification des priorités communes constitueront ainsi les actions indispensables pour faire entendre leurs intérêts. D'autre part, la mobilisation des différents types d'acteurs aux travaux de normalisation – juridiques, académiques, institutionnels, *start-ups* et associatifs – s'impose comme une nécessité afin d'adopter une démarche pluraliste, couvrant l'ensemble des enjeux économiques et sociétaux.

Enfin, alors que la Commission Européenne réaffirme la portée stratégique de la normalisation en déclarant que « *la souveraineté technologique de l'Europe, sa capacité à réduire ses dépendances et la protection des valeurs de l'UE dépendront de notre capacité à définir des normes à l'échelle mondiale* »[16], le soutien de l'Etat sera nécessaire dans les différentes orientations proposées par cette stratégie.

16 https://ec.europa.eu/commission/presscorner/detail/fr/IP_22_661

Vous souhaitez vous impliquer dans le projet contactez :
louis.morilhat@afnor.org

Pour suivre les normes volontaires :

norminfo.afnor.org

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex
Tél. : +33 (0)1 41 62 80 00
www.normalisation.afnor.org