AI *Act*

Le temps de l'action.

Capgemini invent

Sommaire

Edito

AI code is low

Savez-vous ce que le nucléaire, les antibiotiques et la chimiothérapie ont en commun ? Ils n'auraient jamais vu le jour si les lois actuelles s'étaient appliquées à l'époque de leur invention. Savez-vous à présent ce que les véhicules autonomes, les stations de recharge à hydrogène, l'édition du génome et le cloud souverain ont en commun ? Ils n'émergeraient jamais sans une législation appropriée.

En amont du forum de Davos, nous avons interrogé plus de 2 000 cadres supérieurs de nos clients sur la perspective d'une réglementation européenne de l'IA. Loin de s'y opposer, une grande majorité en soutenait activement le principe. Pour ces responsables, l'IA générative se place sans ambiguïté du côté des technologies qui ont besoin de législation pour canaliser leur développement.

L'AI Act est cette législation. Ce règlement a sans doute été le plus attendu et le plus commenté de l'agenda législatif européen de ces dernières années. Avec plus de 100 articles et 13 annexes, il est aussi exceptionnellement long pour une législation européenne et, en toute humilité, ni nos équipes ni nos clients n'ont encore pris la pleine mesure de son contenu et de ses implications. Il faut dire que l'inflation du texte au fil des discussions au Parlement européen n'a pas non plus favorisé la préparation à son application, pourtant indispensable et désormais urgente.

Dans ce livre blanc, nous avons essayé de rassembler les questions que vous vous posez et que, souvent, vous nous posez, au sujet de l'AI Act et d'y répondre de la manière la plus claire et synthétique possible, dans la mesure de ce qu'il est aujourd'hui possible d'affirmer. L'excellence des équipes de Capgemini Invent sur ce sujet qui est à la fois technologique, juridique et métier, s'inscrit dans la continuité de plusieurs années de R&D sur l'IA de confiance tant chez Capgemini Invent que chez Quantmetry, qui a rejoint le groupe Capgemini il y a un an. Ces travaux nous ont conduit à élaborer une plateforme qui permet de cartographier vos risques et accompagne vos démarches de mise en conformité en matière d'IA. Cet outil est incroyable ! Il a le pouvoir de vous faire gagner du temps au moment où vous n'en avez plus beaucoup devant vous.

Chez nos clients, l'attention s'est beaucoup focalisée ces derniers mois sur les dispositions de l'AI Act concernant les IA génératives et les modèles fondationnels (articles 51 et suivants). Un débat s'est installé entre une Europe qui légifère vite et une Amérique qui innove à grandes enjambées. De manière générale, l'AI Act opère une classification fondée sur la production des systèmes et leur finalité. Il établit une surveillance renforcée, via une procédure d'évaluation ex ante, pour toutes les IA considérées « à haut risque », en particulier celles qui mettent en jeu la santé, l'éducation, la sécurité ou les droits fondamentaux. Loin d'être figée, cette liste des IA à haut risque (annexe III) sera actualisée par la Commission européenne elle-même. C'est l'un de ces points sur lesquels l'application du texte et les premiers pas du futur Bureau de l'IA européen seront scrutés avec une grande attention.

En ce qui concerne les modèles de langage, la confiance doit être considérée du point de vue de leurs productions et non des conditions de leur entraînement. Cet enjeu ne se prête pas à un raisonnement binaire : le langage, lorsqu'il est « naturel », ne discrimine pas le vrai du faux, lesquelles n'obéissent d'ailleurs que très rarement à une relation binaire (ce peut être le cas sous la contrainte d'une méthodologie scientifique appropriée, en médecine ou en ingénierie par exemple).

On appréhende donc les risques des modèles d'IA génératifs via un examen régulier de leurs résultats (ce qu'on appelle le red teaming), des boucles d'apprentissage (grounding) et la forme des questions qui leur sont posées (prompt engineering). L'AI Act demande aux producteurs de tels modèles d'« identifier, réduire et mitiger » l'ensemble des « risques raisonnablement prévisibles ». Derrière ces mots, c'est par conséquent toute une ingénierie d'audit des modèles d'IA génératifs qui doit se mettre en place.

La demande d'un audit des données d'entraînement nous apparaît aujourd'hui comme l'un des sujets les plus épineux soulevés par le texte. Compte tenu de leur volume, cet audit peut être difficilement praticable (on parle d'« unfathomable dataset »). Le compromis législatif européen a donc ajouté une série de dispositions spécifiques pour les seuls modèles fondationnels et d'IA générative, dont la portée repose sur un faisceau de présomptions. Ces règles s'appuient en effet sur des seuils de puissance computationnelle en dépit des incertitudes sur les lois de mise à l'échelle des modèles d'IA génératifs (la fameuse « loi de Chinchilla »). Au moyen d'actes délégués, la Commission européen adaptera donc la législation au fil du temps, des progrès et des usages. Il en découle certes une incertitude juridique importante, mais c'est en partie à dessein, de manière à pouvoir s'adapter à des technologies en pleine évolution. Formulons néanmoins le vœu que le cadre se stabilise rapidement. Quoi qu'il en soit, nous vous recommandons de prendre les devants et d'inscrire votre approche de ces sujets dans votre politique d'entreprise en élaborant votre propre code de conduite, conforme à vos valeurs et votre stratégie.

« Code is law » écrivait Lawrence Lessig en 1999, aux prémices de l'essor d'Internet. Dans son célèbre ouvrage, Lessig rappelait que le web n'est pas seulement un entrelacs de code informatique, mais aussi une architecture de règles qui sont amenées à être déterminantes pour notre vie commune et qui, de ce fait, doivent obéir à des principes de transparence et d'ouverture. Les écrits de Lessig sont aujourd'hui encore une référence pour redéfinir les contours de l'open source, repenser l'influence de la blockchain sur le droit des contrats, ou encore envisager les sources de souveraineté digitale. Avec l'AI Act, jamais code informatique et code juridique ne s'étaient trouvés si étroitement intriqués. Avec lui, les législateurs européens ont posé des ancres dans un océan législatif potentiellement infini. Nous vous donnons quelques boussoles pour y naviguer.

Etienne Grass
Directeur exécutif
Capgemini Invent France

Résumé

L'AI Act a connu de nombreuses réécritures. De ce fait, il est difficile de trouver des publications auxquelles se fier parmi les très nombreuses qui lui ont été consacrées. Ce guide vise à pallier ce déficit de documentation. S'appuyant sur une veille active tout au long de la gestation du texte, l'analyse approfondie de sa version finale et l'expérience déjà longue de Capgemini dans la mise en œuvre de systèmes d'IA respectant les enjeux d'éthique, de fiabilité et de sécurité, ce guide répond au besoin urgent d'une information claire, synthétique, pratique et, surtout, à jour sur l'AI Act.

L'essentiel à retenir, selon nous, est que votre organisation devra, à très court terme, recenser tous ses cas d'usage de l'IA et prendre, pour chacun d'eux, des mesures de précaution, fonction du type de système utilisé et de sa finalité, des risques engendrés et du rôle qu'elle aura joué dans son élaboration.

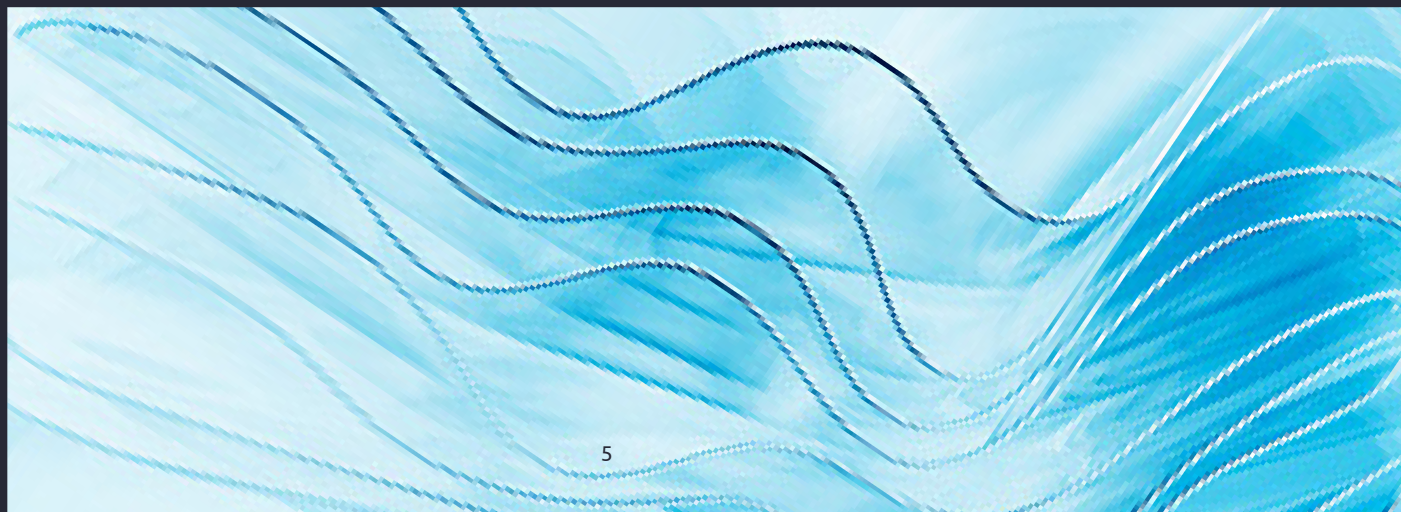
Se conformer à l'AI Act passera donc par la mise en place de pratiques systématiques et rigoureuses d'analyse, de remédiation et de suivi des systèmes d'IA, mêlant des considérations technologiques, réglementaires et business. Ces pratiques s'appuieront sur un ensemble de règles, de normes et de standards (actuellement en cours d'élaboration), ainsi que sur un outillage adéquat, à l'image de la plateforme de pilotage de la conformité que nous avons développée.

Structurer et généraliser de telles pratiques à l'échelle de l'organisation prendra nécessairement du temps. La mise en conformité avec l'AI Act sera donc un programme éminemment transverse, au long cours, dont les enjeux exigent qu'il soit suivi au plus haut niveau et piloté par un binôme associant le technologique et le réglementaire.

Alors que les premières obligations sont pour fin 2024 et que les premières sanctions pourraient être prononcées dès mi-2025, il n'y a donc pas un instant à perdre pour lancer ce chantier. D'autant que si un certain nombre d'éléments restent à finaliser (institutions, normes…), les certitudes sont suffisantes pour débuter.

À défaut de pouvoir aussitôt appliquer tout le texte à la lettre, les organisations doivent commencer par s'en approprier l'esprit : l'IA est un outil puissant dont l'usage n'est pas sans risque et ce sont ces risques, très concrets, qu'il faut envisager et prévenir. Il faut s'attacher dès maintenant à ce que cette culture de responsabilité imprègne toute l'organisation et préside dorénavant à toutes ses initiatives en matière d'IA. Ceci permettra, notamment, de sécuriser les développements en cours du point de vue de la conformité car ils ne seront alors sans doute pas très éloignés des exigences de l'AI Act.

À travers ses obligations, l'AI Act trace un chemin vers des usages de l'IA maîtrisés, sécurisés, responsables et acceptés par les utilisateurs finaux, que ce soit les collaborateurs, les clients ou les citoyens. La mise en conformité nous apparaît donc comme une opportunité pour accélérer l'adoption de l'IA et pour étendre sa mise en œuvre à l'échelle, de manière à pouvoir exploiter pleinement et rapidement tout son potentiel pour créer de la valeur et relever les immenses défis économiques, démocratiques, sociétaux et environnementaux d'aujourd'hui et de demain.



1 S’approprier urgemment un texte dense et ambitieux pour agir malgré l’incertitude juridique

Nouvelle brique de l’édifice européen de régulation du numérique, l’AI Act est un texte de portée mondiale qui vise à réguler tous les systèmes d’IA utilisés en Europe, quelle que soit leur origine. En dépit de marges d’évolution assumées, qui créent une part d’incertitude juridique, les organisations doivent s’en emparer pour s’engager dès à présent sur la voie de la mise en conformité.

L’IA selon l’AI Act

Dans son article 3, l’AI Act donne une définition assez large des systèmes d’IA auxquels il s’applique, car elle ne se fonde pas sur des critères purement technologiques, mais sur des propriétés de fonctionnement. Or, ces caractéristiques peuvent se retrouver dans diverses approches algorithmiques utilisées de longue date par les entreprises pour générer des contenus, des prédictions, des recommandations, voire des décisions : approches statistiques, moteurs de règles complexes, moteurs d’inférence, systèmes experts, etc. Le périmètre de l’AI Act s’étend donc bien au-delà des seuls systèmes d’IA de type machine learning ou deep learning.

» *Il faut être attentif au fait que cette définition peut éventuellement dépasser ce que l’entreprise considère elle-même comme de l’IA.*

L’approche par les risques

Les risques engendrés par l’utilisation de l’IA dans certains domaines sensibles comme la santé, l’alimentation, les médias, la sécurité ou encore la justice ont été à l’origine de l’AI Act. La notion de risque est donc le fil conducteur du texte, la clé de sa compréhension et la pierre angulaire de son application.

L’AI Act range les systèmes d’IA en trois catégories selon les risques qu’ils engendrent :

- Les systèmes interdits
- Les systèmes à haut risque
- Les systèmes de moindre risque

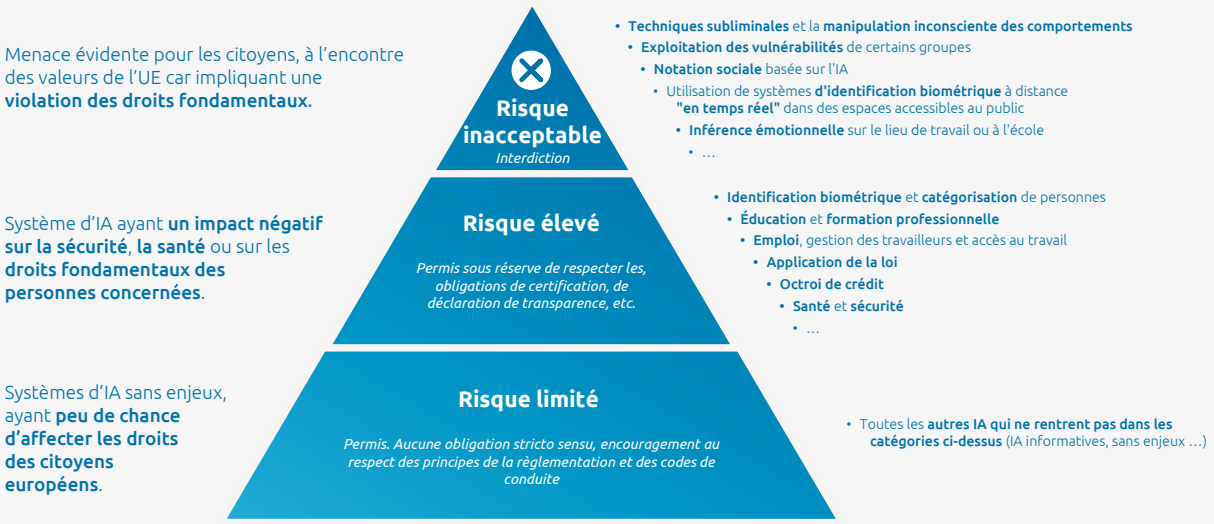


Fig. 1 – La pyramide des risques

Pour chaque cas d'usage, les obligations à respecter dépendent de leur classification ainsi que du rôle de l'organisation dans l'élaboration du système d'IA (fournisseur, déployeur, opérateur… voir partie 3) et de sa nature (entreprise privée, organisme public, startup…).
Certaines de ces exigences portent sur le système lui-même (gestion des données, cybersécurité, certification…), d'autres sur l'organisation (processus, transparence…). Dans tous les cas, il faut être en mesure de documenter ces dispositions et de les communiquer aux autorités de contrôle.

Les 8 dimensions de l'IA de confiance

Nous avons catégorisé ces exigences en 8 domaines, chacun ayant une portée à la fois technique et organisationnelle en termes de processus. Ces 8 domaines sont pour nous les 8 dimensions clés de l'IA de confiance et constituent une formidable grille de lecture pour travailler sur la conformité à l'AI Act (Fig. 2).

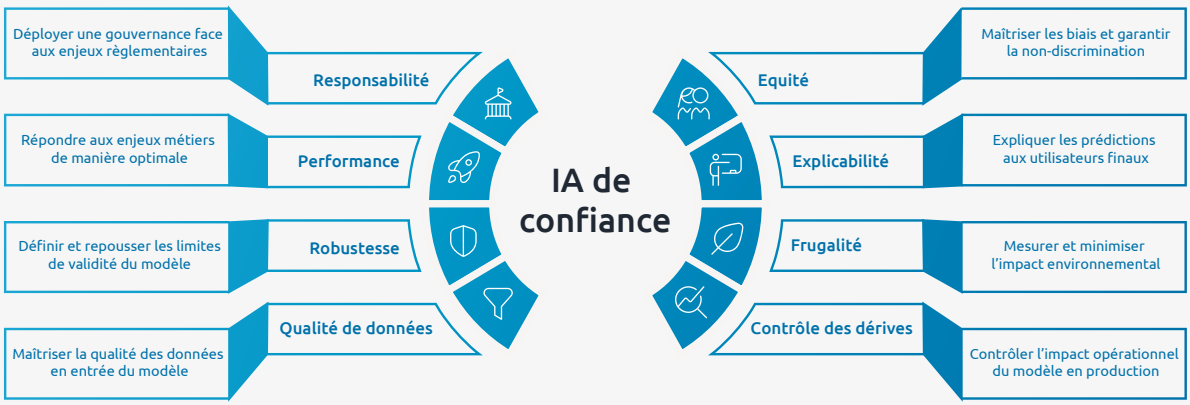


Fig. 2 – Les 8 dimensions de l'IA de confiance

De manière générale, pour se conformer à l'AI Act, il faut que l'organisation :

- *Identifie tous les systèmes d'IA qu'elle produit et/ou utilise, et les cas d'usage associés ;*
- *Les classifie en fonction des risques engendrés (y compris ceux découlant d'usages détournés, malveillants ou maladroits) ;*
- *Identifie son rôle dans la chaîne de valeur et les obligations associées ;*
- *Prenne en conséquence les mesures appropriées et en particulier fasse certifier les IA à haut risque ;*
- *Documente ces mesures et puisse les communiquer ;*
- *Maintienne un processus de gouvernance et de veille pour réévaluer régulièrement les risques (y compris de nouveaux risques auxquels l'organisation ou le législateur n'aurait pas songé initialement) et s'y adapte si nécessaire.*

LE CAS PARTICULIER DES IA A USAGE GENERAL

Pour conserver sa pertinence en dépit d'une innovation constante, l'AI Act se focalise sur les risques liés aux usages des technologies plutôt que sur les technologies elles-mêmes. Le législateur a toutefois créé une caté-gorie particulière, les modèles d'IA à usage général (ou GPAI pour General Purpose AI), dont l'accessibilité, la diffusion et l'étendue quasi-infinies des possibilités nécessitent qu'ils soient encadrés pour eux-mêmes, en amont de leur mise sur le marché.

Une IA à usage général est définie comme un modèle d'IA entraîné sur un très grand nombre de données via un apprentissage auto-supervisé, présentant une généralité significative, capable d'exécuter de manière com-pétente un large éventail de tâches distinctes, et susceptible d'être intégré à une variété importante de sys-tèmes et d'applications. ChatGPT et Midjourney en sont deux exemples parmi les plus connus. Les fournis-seurs de GPAI devront notamment faire preuve d'une transparence renforcée sur le fonctionnement et la com-position du modèle afin d'éviter autant que possible de présenter des résultats dont l'utilisateur ignorera tota-lement comment et sur quelles bases ils ont été obtenus (effet « boîte noire »).

En outre, lorsque leur création a nécessité une puissance de calcul supérieure à 10^{25} FLOPS[1] les GPAI sont considérés comme porteurs d'un « risque systémique », c'est-à-dire « un risque spécifique aux capacités à fort impact des modèles d'IA à usage général, ayant une incidence significative sur le marché de l'Union en raison de leur portée ou d'effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sûre-té, la sécurité publique, les droits fondamentaux ou la société dans son ensemble, pouvant être propagé à grande échelle tout au long de la chaîne de valeur ». Les fournisseurs de ces très grands modèles devront notamment informer la Commission européenne du risque encouru, réaliser des tests contradictoires pour identifier les risques et prendre des mesures significatives pour les juguler.

[1] FLOPS (Floating Point Operations per Second) : unité de mesure de la puissance de calcul d'un système informatique.

Le calendrier

Voté par le Parlement européen le 13 mars 2024 , l'AI Act va connaître une entrée en application progressive jusqu'en 2030 (Fig. 2). En particulier, les IA interdites devront avoir disparu dès la fin 2024. Le régime de sanctions débutera quant à lui mi-2025. L'essentiel des obligations devra être respecté mi-2026, avec diverses exceptions jusqu'en 2030 selon le type de produit IA et le type d'acteur.

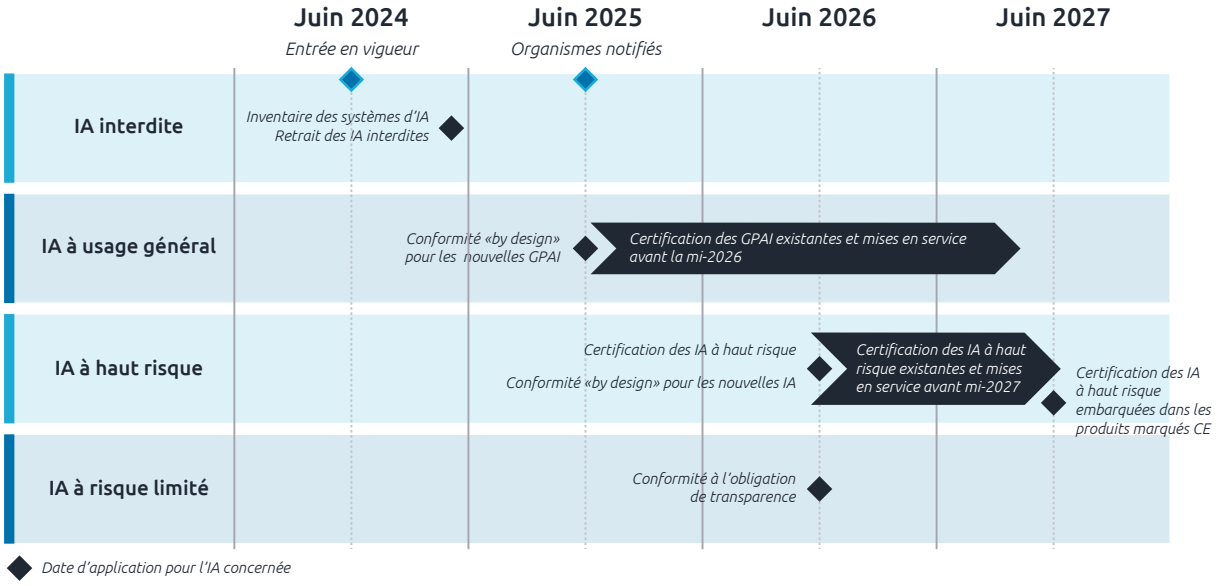


Fig. 3 – Le calendrier de l'entrée en application de l'AI Act

» *Les entreprises n'ont que quelques mois pour, au minimum, recenser les solutions algorithmiques qu'elles utilisent et s'assurer qu'aucun de leur service ne met en œuvre une IA prohibée.*

Les sanctions

À l'instar du RGPD, le législateur a retenu un système d'amendes basé, selon les cas, sur une somme forfaitaire ou sur une part du chiffre d'affaires mondial (CA). Pour les grands groupes, ce sera le montant le plus élevé qui sera retenu ; pour les PME, le plus faible. Le tableau ci-dessous résume les niveaux de pénalités encourues selon les cas de figure :

	Grands groupes et ETI	PME et Start-ups
Mise en oeuvre d'**IA prohibées**	**Jusqu'à 7% du CA mondial consolidé**	**Jusqu'à 35 millions d'euros**
Non-respect des obligations de déclaration et de certification des **IA à haut risques**	Jusqu'à 3% du CA mondial consolidé	Jusqu'à 15 millions d'euros
Manquement aux obligations d'information	Jusqu'à 1% du CA mondial consolidé	Jusqu'à 7 millions d'euros

» *Même si, comme ce fut le cas pour le RGPD, les autorités pourraient se montrer tolérantes dans les premiers temps, l'ampleur des sanctions doit inciter les entreprises à ne pas retarder leur mise en conformité.*

Les institutions, leurs missions et leurs pouvoirs

L'entrée en vigueur de l'AI Act s'accompagne de la mise en place d'un écosystème institutionnel pour aider à son application, pour la contrôler et pour adapter le texte à l'évolution des technologies, des usages, et donc des risques. Si un certain flou demeure encore sur la désignation de quelques organismes, ainsi que sur la répartition des rôles, nous dressons dans la figure 3 un panorama des institutions clés aux échelons français, européen et international :

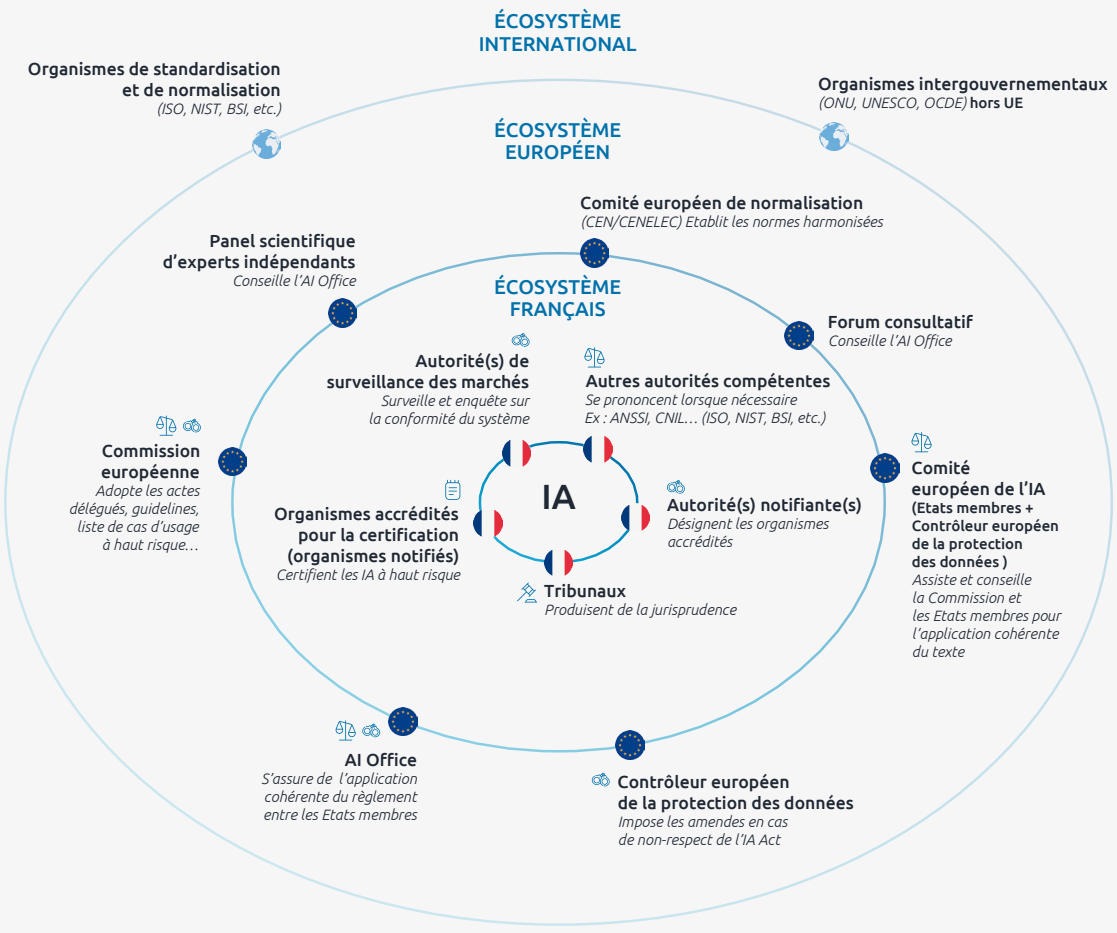


Fig. 4 – L'écosystème institutionnel de réglementation de l'IA

Fig. 5 – L'écosystème institutionnel de réglementation de l'IA

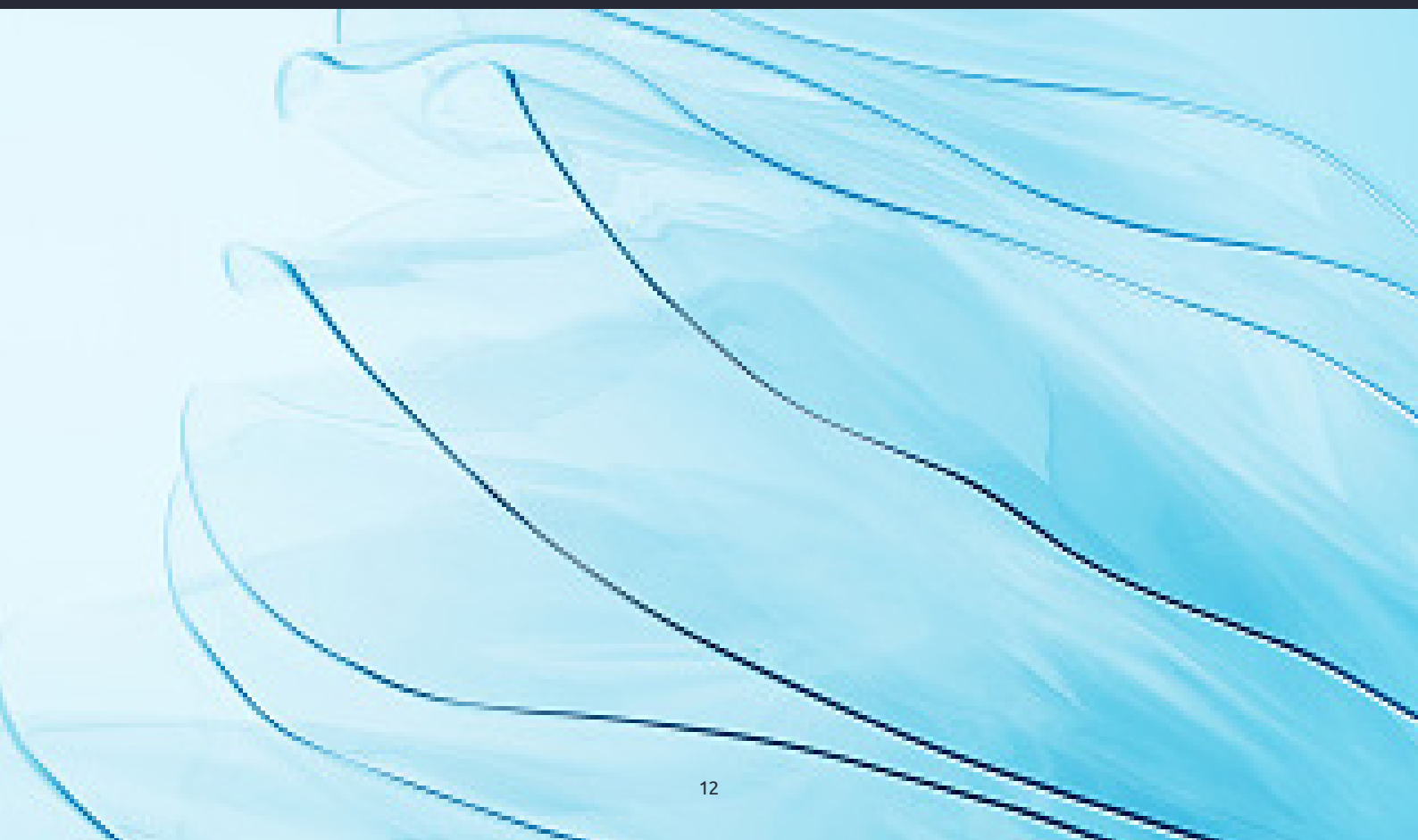
Il n'est pas nécessaire d'attendre la mise en place du cadre institutionnel pour débuter sa mise en conformité. En revanche, il faudra être attentif à ce processus, notamment au niveau national, car les différents organismes seront des interlocuteurs privilégiés.

LE ROLE DES INSTITUTIONS SECTORIELLES

Au sein de l'écosystème institutionnel mobilisé autour de l'AI Act, il nous semble probable que certaines institutions sectorielles se positionneront – ou seront au minimum consultées – autour de cas d'usage spécifiques et à risque. Ce devrait notamment être le cas dans des domaines très réglementés comme la finance et la santé.

Dans le secteur financier, la Banque centrale européenne (BCE), l'Autorité de contrôle prudentiel et de résolution (ACPR) et l'Autorité bancaire européenne (ABE) joueront certainement un rôle central dans la supervision et la régulation, car les exigences de l'AI Act devront s'articuler avec celles d'autres textes tels que la norme BCBS 239, la directive 6AMLD, le règlement DORA ou encore le règlement eIDAS. Nous sommes convaincus que le soutien de ces institutions sera essentiel, en particulier pour la mise en œuvre de cas d'usage à haut risque comme les modèles de détection LCB-FT (Lutte contre le blanchiment d'argent et le Financement du terrorisme), d'analyse KYC (Know Your Customer), d'octroi de crédit, de segmentation et de scoring des clients.

Dans le domaine de la santé, la Haute autorité de santé (HAS) et l'Agence nationale de sécurité du médicament (ANSM) en France, l'Agence européenne du médicament (EMA), ainsi que les organismes de recherche et de réglementation en matière de bioéthique, sont très attentifs au développement des applications de l'IA. La santé est en effet en pointe en la matière, qu'il s'agisse du développement de nouvelles molécules et de nouveaux médicaments, de système d'aide au diagnostic et au dépistage ou de personnalisation des traitements. Autant d'usages qui, au sens de l'AI Act, peuvent mettre en jeu la santé des patients et être donc catégorisés à haut risque.



2 Les ressources, normes et standards pour préparer sans délai sa mise en conformité

Le rôle de la standardisation

Un ensemble de référentiels, de normes et de recommandations, actuellement en cours d'élaboration, aidera et guidera les organisations dans leurs démarches de mise en conformité avec l'AI Act.

Dans l'attente du processus de certification officiel, nous recommandons d'examiner dès à présent les certifications et les standards existants. Même s'il n'est pas encore possible de couvrir en totalité les exigences de l'AI Act, certaines combinaisons de certifications et de normes (ISO 42001 et LNE 2.0, notamment) permettent de s'en approcher, et donc d'anticiper le travail à venir.

Dans la même logique, il nous apparaît également judicieux d'adhérer à une démarche collective volontaire, comme l'AI Pact, à la fois pour commencer à mettre ses IA sous contrôle, pour développer en interne cette culture de la responsabilité, et pour donner dès à présent à ses parties prenantes des gages de confiance.

» *Comme ce fut le cas avec le RGPD, il est probable que les actes européens qui suivront le règlement, les lignes directrices, les normes et standards convergent à peu près vers un ensemble de bonnes pratiques permettant un usage maîtrisé de l'IA.*

L'AFNOR et le LNE, deux organismes français en pointe sur la certification de l'IA

L'AFNOR

L'association AFNOR conçoit des solutions fondées sur les normes volontaires, sources de progrès et de confiance depuis 1926. Sa vocation est d'accompagner les organisations et les personnes pour diffuser cette confiance. Animateur du système français de normalisation, AFNOR Normalisation accompagne et guide les professionnels pour élaborer les normes volontaires nationales et internationales, dont la norme ISO 42001 pour l'établissement et la mise en œuvre d'un système de management responsable de l'intelligence artificielle (SMIA).

LE LNE

Acteur reconnu en certification de produits, système de management et services, le LNE offre depuis trois ans, une certification des processus d'Intelligence Artificielle. Seules ou en synergie avec l'ISO 42001 récemment publiée, les certifications du LNE permettent aux entreprises de certifier la fiabilité et l'éthique de leurs systèmes d'IA par un tiers de confiance, leur offrant ainsi un avantage compétitif. En complément, le LNE propose des évaluations approfondies d'IA, renforçant ainsi la crédibilité et la qualité des solutions proposées.

3 Identifier sa place dans la chaîne de responsabilité

En contrepoint de son approche par les risques, l'AI Act différencie les responsabilités des différents acteurs en fonction de leur rôle dans la mise en œuvre du système d'IA considéré.

Un système d'IA peut être le produit d'une chaîne de valeur complexe, où les responsabilités n'apparaissent pas toujours de façon évidente. L'AI Act entend démêler les choses, d'une part, en définissant nettement les rôles (fournisseur, déployeur, mandataire, distributeur, opérateur…) et, d'autre part, en établissant un principe clair : chacun est responsable de ses actions.

» *Les responsabilités ne pèsent ni entièrement, ni automatiquement sur l'un ou l'autre des acteurs, mais se répartissent entre les différentes parties impliquées tout au long de la chaîne de valeur.*

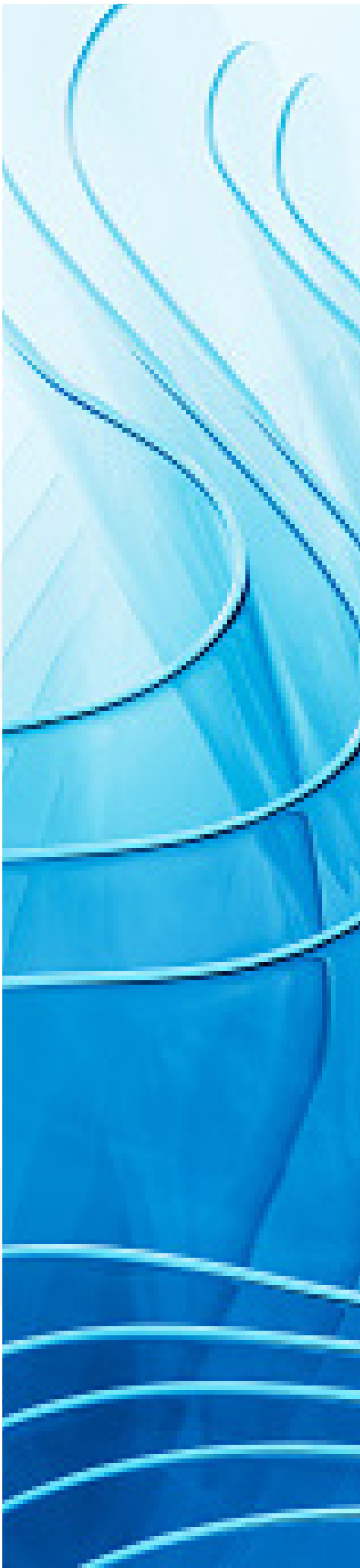
L'une des conséquences essentielles de cette approche est que la distribution des responsabilités sera différente pour chaque cas d'usage. Certains rôles peuvent ainsi ne pas exister, ou bien être portés par un même acteur. Par exemple, un distributeur qui aura modifié l'usage d'une IA sera alors considéré comme un fournisseur, et devra assumer les obligations qui en découlent.

Pour chaque produit d'IA, il conviendra donc d'établir la chaîne de responsabilité et de s'y situer pour déterminer ses obligations et celles de ses partenaires. Nous recommandons fortement de formaliser cette analyse par des documents écrits (contrats, licences…), ce qui constituera une sécurité juridique importante en cas de manquement.

Inversement, il faudra être très attentif à enregistrer et documenter ses actions afin de pouvoir les faire valoir en cas de mise en cause (la traçabilité technique est d'ailleurs l'une des exigences clés du texte).

» *Nous préconisons d'avoir sur cette question de la responsabilité une stratégie de prudence et de prendre soi-même un maximum de précautions, indépendamment des autres acteurs de la chaîne.*

Prenons un exemple, celle de l'entreprise A qui fournit une IA à faible risque à l'entreprise B, qui l'intègre dans une caméra pour outiller un cas d'usage à haut risque, mis en œuvre par l'entreprise C (Fig. 6).



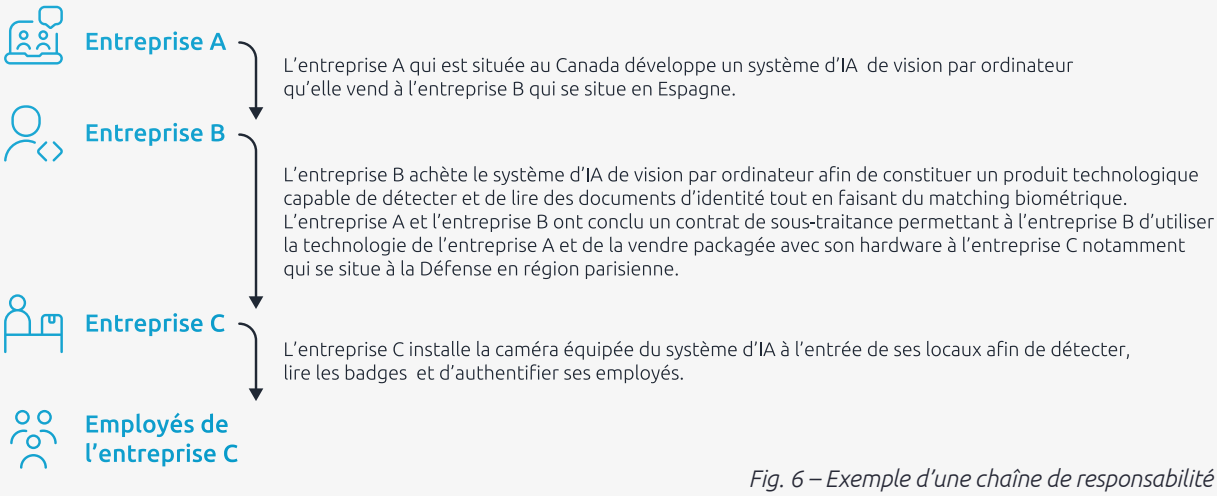


Fig. 6 – Exemple d'une chaîne de responsabilité

Dans ce cas, au regard des définitions données par l'AI Act, A peut être considéré comme le fournisseur en aval du système d'IA, B comme son fournisseur, et C comme son déployeur. Son IA étant à faible risque, A aurait la possibilité de ne pas la faire certifier et de laisser cette tâche à B qui, par son action, crée un système à haut risque. Cependant, il est selon nous plus pertinent de toujours adopter une démarche de conformité « by design », quel que soit le niveau de risque, car il en découlera trois bénéfices :

- Moins de travail au final, car il ne sera pas nécessaire d'aider chaque partenaire dans sa démarche de certification ;
- Plus de sécurité juridique car on se prémunit de problèmes que l'on n'aurait pas anticipés ou de recours qui, même illégitimes, seraient coûteux à régler ;
- Une proposition de valeur supérieure et différenciante car elle sécurise les distributeurs.

La responsabilité de l'entreprise varie et doit être déterminée pour chaque cas d'usage, en fonction du ou des rôle(s) qu'elle occupe dans la chaîne de valeur, mais il apparaît préférable de systématiser une approche de conformité by design.

LA PROPRIETE INTELLECTUELLE, UNE AUTRE RESPONSABILITE MAJEURE

En matière de responsabilités juridiques, l'AI Act aborde un autre sujet délicat, celui de la propriété intellectuelle. La première grande question que soulève l'IA en la matière concerne l'entraînement des modèles sur des données protégées. Les éditeurs d'IA arguent, aux États-Unis, d'un « fair use » et, en Europe, de l'exception prévue par la directive de 2019 sur le droit d'auteur concernant le data mining. Les titulaires des droits contestent de plus en plus cette interprétation car, selon eux, l'entraînement d'une IA constitue indubitablement une forme d'exploitation, qui nécessite donc une contrepartie. Aux États-Unis, le New York Times a intenté une action en justice contre Microsoft et OpenAI, dont le verdict est très attendu. En France, Le Monde a passé avec OpenAI un accord à double tranchant qui préserve les intérêts du journal mais affaiblit les partisans d'un système collectif. L'AI Act n'impose pour sa part qu'une transparence accrue sur les données d'entraînement, en rappelant qu'elles restent soumises aux règles de la propriété intellectuelle. L'équilibre sera délicat à trouver entre cette exigence de transparence et la nécessaire protection du secret des affaires, et il semblerait que l'on se dirige davantage vers un modèle basé principalement sur des contrats d'exploitation.

Une deuxième question majeure touche à la caractérisation des contenus générés par l'IA de manière à pouvoir les distinguer sans ambiguïté des créations humaines. L'objectif est double : d'une part, protéger chaque type de contenu comme il se doit ; d'autre part, lutter contre le parasitisme et les informations erronées ou trompeuses produites par l'IA, en particulier les deepfakes. L'AI Act impose ainsi de signaler les contenus générés synthétiquement (art. 50), ce que font d'ailleurs déjà certaines entreprises (Youtube, Meta).

4 Comment embarquer l'ensemble de son organisation

Étant donné la rapidité avec laquelle l'AI Act va entrer en application et, en parallèle, le développement accéléré des usages de l'IA par les métiers, l'organisation doit d'urgence se mettre en ordre de marche pour lancer le vaste programme de la mise en conformité.

Les acteurs internes d'une démarche éminemment transverse

Tout d'abord, sans même parler des possibles sanctions, l'ampleur des enjeux économiques, organisationnels et métiers liés à une adoption maîtrisée de l'IA imposent une implication directe du top management. Quant au programme de mise en conformité lui-même, sa conduite doit être menée par une direction bicéphale, technologique et réglementaire, qui saura en appréhender la dimension hybride. Selon les organisations, on pourra retrouver :

- **Côté technologie :** le CIO (Chief Information Officer), le CDO (Chief Data Officer) et/ou le CDSO (Chief Data Scientist Officer) ont commencé à implémenter l'IA. Ils en maîtrisent le fonctionnement, comprennent les implications technologiques et les impacts qu'aura l'implémentation des points de contrôle de la conformité, et savent mettre en place les garde-fous qui leur seront demandés ;
- **Côté réglementaire :** les responsabilités pourront se partager entre le Juridique, garant de l'interprétation du texte pour l'entreprise ; la Conformité, qui supervisera la mise en place opérationnelle des exigences ; et l'Éthique, pour éclairer les cas les plus délicats (finalité des cas d'usage, biais…).

Ce binôme devra s'adjoindre l'aide d'autres responsables de l'entreprise sur des questions spécifiques, comme les Risques, pour évaluer les conséquences des cas d'usage ; le DPO (Data Protection Officier), pour tout ce qui touche aux données personnelles ; le RSSI (Responsable de la sécurité des systèmes d'information), pour sécuriser les modèles d'IA et les données ; et le département Qualité, rompu aux procédures d'homologation et de certification nécessaires au marquage CE. L'importance de leurs rôles respectifs dépendra de l'organisation de l'entreprise, de son secteur d'activité et de la nature des cas d'usage.

Enfin, la mise en œuvre proprement dite impliquera de très nombreux acteurs, depuis les métiers, à l'origine des cas d'usage, jusqu'aux achats, qui auront à sélectionner des produits et des partenaires conformes, mais également les RH, qui accompagneront les programmes de sensibilisation et de formation.

» *La mise en conformité avec l'AI Act est une démarche qui, depuis la direction générale, va nécessiter l'implication et la collaboration d'un très grand nombre d'acteurs. Pour avancer rapidement dans un calendrier resserré, il faudra donc s'adapter aux spécificités de l'organisation et s'appuyer sur ses forces. L'expérience du RGPD pourra être une référence précieuse.*

Pas de conformité sans un Quality Management System

La mise en conformité passera obligatoirement par l'implémentation d'un système de management de la qualité (QMS), ou son adaptation s'il en existe déjà un.

Afin d'inscrire la conformité dans les pratiques et dans la durée, ce QMS s'appuiera sur :

- **Une organisation proche du terrain** pour que la conformité soit respectée au quotidien, une distribution claire des rôles et des responsabilités, une gestion des ressources ;
- **Une méthodologie pratique** d'évaluation des risques et des impacts ;
- **Des processus** qui permettront d'aborder en pratique tous les sujets (robustesse, explicabilité, biais, source et qualité de données, traçabilité, sécurité, propriété intellectuelle…), de cadrer les développements (équipes projet, sous-traitance…), de surveiller les modèles et leur évolution, de recevoir et traiter des alertes…
- **Des systèmes de contrôle et de pilotage.**

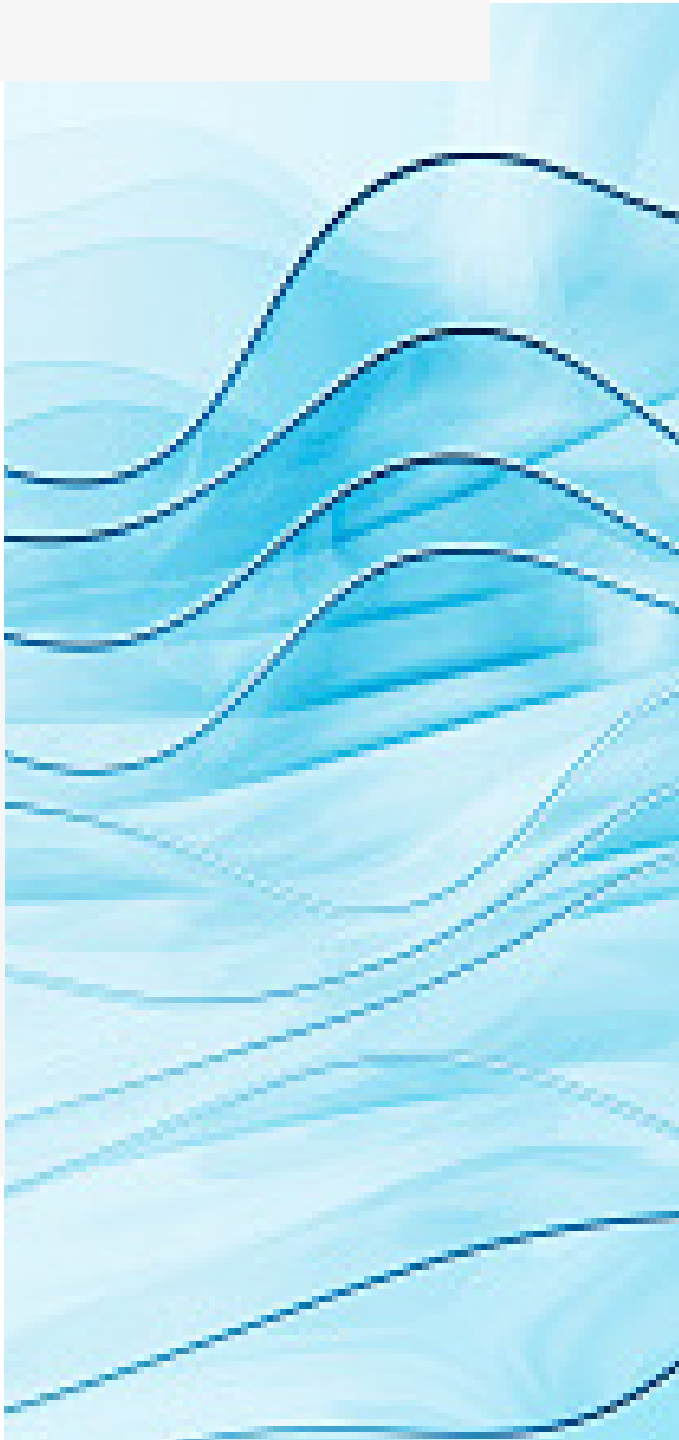
» *La mise en place du QMS sera la réalisation concrète qui va permettre à l'entreprise de se conformer dans les faits à l'AI Act.*

Un programme à part entière

Calendrier de l'entrée en application, portée de la réglementation, transversalité, maturité de l'organisation sur l'IA et nécessité de poursuivre ses développements : les très nombreux facteurs qui se télescopent exigent de bâtir un programme à part entière, structuré, avec son calendrier, son budget, son pilotage, sa gouvernance… Sans parler de la nécessité de savoir reprioriser les chantiers lorsque la règlementation évoluera ou que la jurisprudence aura donné des précisions sur certains points soumis à interprétation.

» *Pour initier son programme de mise en conformité, les premières actions à lancer dès à présent sont :*

- *Mettre en place le groupe pluridisciplinaire qui va piloter la mise en conformité ;*
- *Évaluer sa maturité et lancer l'inventaire de ses IA ;*
- *Définir ses priorités de mise en conformité ;*
- *Engager la sensibilisation des divers acteurs de son écosystème sur les risques liés à l'IA et sur leur part de responsabilité pour les maîtriser.*



5 S’outiller pour piloter sa conformité

Entre des exigences complexes, des cas d’usage qui vont vite se multiplier et des risques amenés à évoluer, l’implémentation et le suivi des règles imposées par l’AI Act ne pourra se faire sans un outil qui apportera de la visibilité et facilitera la collaboration entre tous les acteurs.

Loin d’une solution générique, cet outil doit être le reflet de la façon dont l’entreprise implémente sa mise en conformité : méthodologie d’évaluation des risques, audit des IA, définition des plans de remédiation, consolidation de la documentation, gestion de la qualité via le QMS… Il devra aussi pouvoir gérer les deux cas de figure possibles : soit les cas d’usage préexistants, qu’il faudra évaluer et ramener si besoin dans la conformité, soit les cas d’usage nouveaux, dont il faut encadrer le développement (conformité by design). Enfin, il faudra pouvoir suivre l’évolution de conformité dans la durée, avec plusieurs niveaux de granularité.

Nous avons réalisé au sein du Lab de Capgemini, et avec le soutien de Bpifrance, un important travail de R&D pour implémenter les obligations du texte dans une plateforme personnalisable qui permet d’identifier les cas d’usage et de gérer leur conformité. L’objectif de cet outil pionnier est de traduire les exigences de l’AI Act, parfois vagues dans leur formulation, en critères de validation actionnables, mesurables et, pour les cas d’usage à haut risque, aptes à alimenter le dossier de certification. Ces critères peuvent se baser soit sur les normes et les standards (en cours d’élaboration), soit sur une méthodologie propre, nourrie par notre expertise.

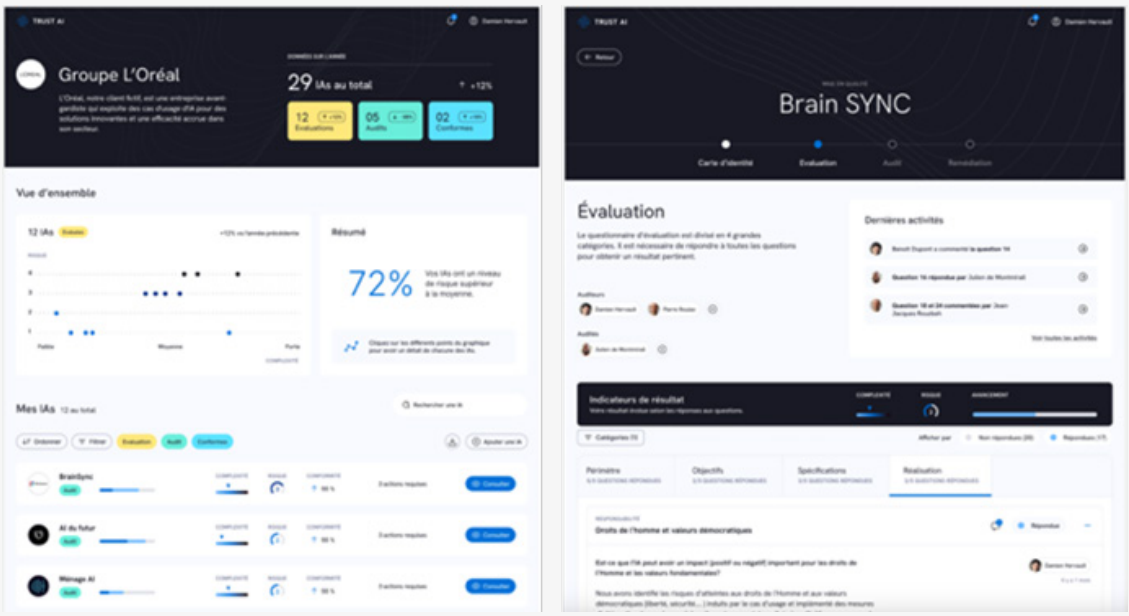


Fig.7 – La plateforme Capgemini de gestion de mise en conformité à l’AI Act

Pour illustrer notre méthode, prenons par exemple l'article 15 de l'AI Act, intitulé « Exactitude, robustesse et cybersécurité ». Cet article stipule que « la conception et le développement des systèmes d'IA à haut risque sont tels qu'ils leur permettent d'atteindre un niveau approprié d'exactitude, de robustesse et de cybersécurité, et de fonctionner de façon constante à cet égard tout au long de leur cycle de vie. » Ici, c'est l'expertise technique qui va permettre de déterminer ce que doit être ce « niveau approprié d'exactitude, de robustesse et de cybersécurité » et s'il est atteint.

Ainsi, si l'on se concentre sur la robustesse, qui constitue l'un des huit piliers de notre grille d'analyse des exigences de l'AI Act (Fig. 1), elle peut se découper en trois axes techniques :

- **Le contrôle du domaine de validité :** Le jeu de données sur lequel est entraîné le modèle d'IA définit son domaine de validité. S'il est utilisé sur des données qui en sont éloignées, la pertinence des résultats n'est pas garantie. Pour chaque modèle, il faut donc toujours contrôler au préalable l'adhérence des nouvelles données à son domaine de validité.
- **La maîtrise de l'incertitude des prédictions :** Même lorsqu'il est confronté à des données qui ne correspondent pas à celles sur lesquelles il a été entraîné, un modèle d'IA propose toujours une prédiction. Il est cependant possible d'apporter une nuance à ce résultat en donnant au modèle la capacité de lui adjoindre un degré d'incertitude, c'est-à-dire qu'il peut préciser dans quelle mesure il est sûr ou non de sa réponse.
- **Le contrôle de la stabilité du modèle :** Afin de garantir la cohérence métier, il est essentiel que les réponses du modèle ne soient pas altérées par des variations minimes des données en entrée. Par exemple, un modèle d'octroi de crédit ne doit pas donner une réponse différente si l'âge du demandeur change d'un mois ou son salaire de 10 euros. Une campagne de tests permet de s'en assurer.

En procédant de la sorte sur la totalité des piliers de notre grille d'analyse, notre plateforme permet ainsi d'objectiver la conformité du modèle aux exigences de l'AI Act, d'identifier le cas échéant les points à corriger, et de suivre, piloter et documenter l'ensemble de ce processus d'évaluation et d'ajustement. Nous accompagnons cet outil de notre expertise pour qu'il reflète la politique et la stratégie de l'organisation en matière d'IA et qu'il s'inscrive efficacement dans ses processus.

» *Avec la multiplication des usages de l'IA dans toute l'organisation, recourir à un outil spécialisé dans l'analyse, l'ajustement et le suivi des systèmes d'IA sera indispensable pour gérer efficacement le respect des règles de l'AI Act.*

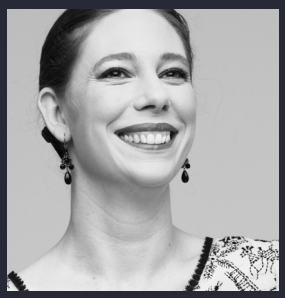
Conclusion

À débuter sans plus tarder, le chantier de mise en conformité avec l'AI Act va nécessiter :

- ☐ La compréhension approfondie d'un texte dense et complexe, et de ses implications ;
- ☐ Le besoin d'alignement et de sponsorship de plusieurs parties prenantes comme le Règlementaire, les Risques, l'IT, dont le département Data & IA, etc ;
- ☐ Des connexions avec l'écosystème institutionnel ;
- ☐ Une maîtrise des normes, standards, référentiels et processus de certification ;
- ☐ Une expertise scientifique et technologique des modèles d'IA, de leurs réglages et des méthodes d'explicabilité associées ;
- ☐ La capacité d'intégrer ces modèles à des applications métiers ergonomiques et sécurisées ;
- ☐ La définition et la conduite d'un programme de transformation transverse à l'échelle de l'organisation ;
- ☐ Une approche pluridisciplinaire pour comprendre la finalité des IA et prendre en compte les questions des risques, d'éthique, de conformité, de sécurité… ;
- ☐ La mise en place d'un outillage dédié ;
- ☐ L'acculturation des dirigeants, des équipes de développement et des utilisateurs métiers aux enjeux et aux spécificités de l'IA.

Réunissant l'ensemble de ces compétences, Capgemini Invent est en mesure d'accompagner ses clients pour faire de la mise en conformité à l'AI Act un tremplin pour accélérer une utilisation maîtrisée, sécurisée, responsable et créatrice de valeur de l'IA à grande échelle.

Signataires et contributeurs



Isabelle Budor
Vice President, CSR & Ethics for Trusted companies
isabelle.budor@capgemini.com

Spécialisée depuis plus de 10 ans dans l'accompagnement des transformations d'entreprise à la croisée du réglementaire, de la data/IA, et du bon équilibre entre sécurité et libertés & droits fondamentaux (RGPD, AI Act, ...), Isabelle intervient de façon pragmatique auprès d'organisations françaises et internationales, de toute taille et tous secteurs.

Raphaël Viné
Senior Director, Trusted AI, Next Frontier AI
raphael.vine@capgemini.com

Passionné par les nouvelles technologies du numérique et ayant effectué une grande partie de ses 20 ans de carrière dans le conseil auprès de différents secteurs d'activité, Raphaël a fait partie de l'aventure Quantmetry autour du développement d'IA avant de rejoindre Capgemini Invent France, pour lequel il est désormais en charge de l'offre Trusted AI et mise en conformité avec l'AI Act. Il accompagne au quotidien des clients soucieux de prendre la mesure du sujet et de définir les bonnes priorités, puis mettre en place des programmes réalistes et opérationnels.

Avec la contribution de notre équipe d'experts dans les domaines du juridique et de la data science : Inès Bedar, Asma Derbale, Anthony Duong, Damien Hervault, Gauthier Le Courtois du Manoir.

À propos de Capgemini Invent

Capgemini Invent est la marque d'innovation digitale, de design et de transformation du groupe Capgemini, qui permet aux dirigeants de façonner l'avenir de leurs entreprises. Etablie dans plus de 30 studios et plus de 60 bureaux dans le monde, elle comprend une équipe de plus de 12 500 collaborateurs, composée d'experts en stratégie, de data scientists, de concepteurs de produits et d'expériences, d'experts en marques et en technologie qui développent de nouveaux services digitaux, produits, expériences et modèles d'affaire pour une croissance durable.

Capgemini Invent fait partie du groupe Capgemini, partenaire de la transformation business et technologique de ses clients, les accompagne dans leur transition vers un monde plus digital et durable, tout en créant un impact positif pour la société. Le Groupe, responsable et multiculturel, rassemble 340 000 collaborateurs dans plus de 50 pays. Depuis plus de 55 ans, ses clients lui font confiance pour répondre à l'ensemble de leurs besoins grâce à la technologie. Capgemini propose des services et solutions de bout en bout, allant de la stratégie et du design jusqu'à l'ingénierie, en tirant parti de ses compétences de pointe en intelligence artificielle, en cloud, et en data, ainsi que de son expertise sectorielle et de son écosystème de partenaires. Le Groupe a réalisé un chiffre d'affaires de 22,5 milliards d'euros en 2023.

Get the future you want*

Plus d'informations sur www.capgemini.com

**Réalisez le futur que vous voulez*

Capgemini invent