Business

Intelligence artificielle.
Valeur réelle.

Le dir-op de Sophie ne sait pas par où commencer. Mais Sophie, elle, dispose d'un plan d'action clair pour industrialiser sa PoC à l'échelle de l'entreprise. Découvrez ici ce que Sophie et d'autres clients d'Orange Business ont compris.

Votre feuille de route pour opérationnaliser l'IA :

transformer les PoC en services GenAI à l'échelle de l'entreprise

Business

Introduction

89 % des dirigeants d'entreprise estiment que l'IA transformera leur organisation[1]. Pourtant, 90 % d'entre eux attendent de la GenAI qu'elle dépasse le stade du simple battage médiatique ou de la preuve de concept (PoC). Et 66 % se déclarent mitigés ou insatisfaits des progrès réalisés par leur entreprise en matière d'IA[2]. Alors, qu'est-ce qui bloque ?

Nous savons que l'urgence liée à l'opérationnalisation des services GenAI peut parfois créer un environnement de travail sous pression. Mais, pour reprendre les mots de Rudyard Kipling, j'espère que les informations contenues dans ce document vous aideront à garder la tête froide, même si ceux qui vous entourent semblent la perdre.

Kristof Symons, *CEO International, Orange Business*

Aujourd'hui, la pression s'intensifie pour transformer les PoC fondées sur l'IA en services évolutifs à grande échelle, un processus que nous nommons « opérationnalisation ». Ceux qui en portent la responsabilité prennent rapidement conscience de l'ampleur des défis auxquels ils sont confrontés.

Lancer une PoC est relativement simple (et c'est précisément pour ça que de nombreuses entreprises ont déjà tenté l'expérience). Une PoC demande peu de coordination des équipes, ne remet pas en question les silos de données, n'impose pas de corriger des résultats de faible qualité ou entachés d'« hallucinations » (résultats erronés), ni de mettre en place une posture de cybersécurité rigoureuse, ou encore de faire monter en compétences d'importantes équipes.

Mais une fois la phase d'opérationnalisation de cette PoC engagée, chacun de ces sujets devient critique. On voit alors apparaître un écart de plus en plus marqué entre les attentes des directions, qui exigent des services robustes déployables à l'échelle de l'entreprise, et la capacité réelle des équipes techniques à les délivrer. Un rapport récent d'Economist Impact révèle que seuls 37 % des dirigeants estiment leurs applications GenAI prêtes pour une mise en production, un chiffre qui tombe à 29 % chez les utilisateurs[3]. Par ailleurs, comme le confirme une étude menée par Orange Business et GlobalData, les coûts cloud, jusque-là absorbés dans les budgets existants, connaissent une flambée soudaine.

Faire converger tous ces éléments pour créer des services d'IA évolutifs, qui apportent une vraie valeur, demande plus que des compétences techniques (même si elles sont essentielles) : cela exige une expérience concrète, un discernement fondé sur l'expertise et la capacité à prendre les bonnes décisions. Autrement dit : de la sagesse.

Cette sagesse s'appuie sur une connaissance approfondie des fondamentaux de l'IA – et notamment de la GenAI – sur lesquels les entreprises s'appuient désormais pour bâtir leur avenir. Cela inclut notamment la capacité à lever les silos entre les équipes cloud, cybersécurité et infrastructure. Elle requiert également une intelligence stratégique : non seulement savoir définir et appliquer des politiques de gouvernance et de sécurité, mais aussi pouvoir les adapter en continu, à mesure que le paysage de l'IA et des risques évolue.

Chez Orange Business, cette sagesse est bien réelle. Elle se traduit par la manière dont nous accompagnons nos clients dans l'opérationnalisation de leur IA et par l'intégration de l'IA au cœur de nos offres et services. Ce document en illustre les fondements à travers cinq piliers essentiels à l'opérationnalisation de l'IA :

1. **La qualité des données**
2. **L'utilisation adaptée des LLM (large language model)**
3. **La sécurité**
4. **L'infrastructure**
5. **La création de valeur**

Maîtriser la qualité des données

Quel que soit le cas d'usage envisagé, une règle fondamentale s'applique à tous les projets d'IA : si les données en entrée sont mauvaises, les résultats le seront aussi.

Ce qui détermine la performance d'un modèle ? Les données, et plus précisément leur qualité. Sans données, il n'y a pas d'IA. L'IA a besoin des données pour apprendre : que ce soit pour entraîner de nouveaux modèles ou pour permettre à ceux déjà en production de s'adapter à la réalité. Et inversement, les données prennent toute leur valeur grâce à l'IA, qui permet de les traiter, de les analyser et d'en tirer des enseignements à partir de volumes d'informations toujours plus importants.

La qualité des données est au cœur de la réussite des projets d'IA, et cela a toujours été le cas. Ce qui change aujourd'hui, c'est l'ampleur de l'adoption. Il y a quelques années encore, seuls les grands groupes pouvaient se permettre de déployer des outils d'IA. Avec la GenAI, cet accès s'est démocratisé.

Autrement dit, les technologies et les algorithmes ne sont plus des facteurs de différenciation. En revanche, vos données peuvent l'être.

Il est donc indispensable de garantir une qualité de données optimale pour limiter les risques. Problèmes de confidentialité, failles de sécurité, processus de saisie défaillants… si votre socle de données est imparfait, la GenAI ne fera qu'amplifier ces défauts. D'où l'importance de traiter ces sujets dès le départ. Corriger les erreurs de qualité des données une fois le modèle entraîné coûte bien plus cher que de s'assurer de leur fiabilité dès le début du projet. D'autant plus que, demain, certains modèles seront peut-être entraînés à partir de données générées par d'autres IA, au risque de figer les biais et les erreurs dans les couches profondes du système.

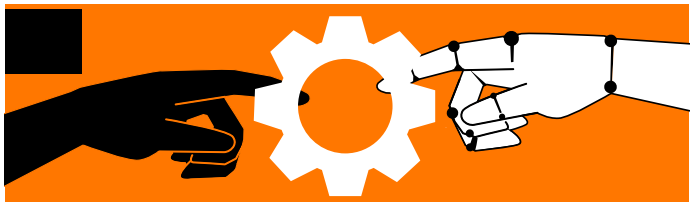
Les services d'IA donnent aussi accès à des sources d'information bien plus riches et diversifiées : documents texte, enregistrements audio ou vidéo, mails, fichiers scannés, relevés de capteurs… Évaluer la qualité des données non structurées est un défi que nous relevons déjà avec nos clients.

Mais comment les entreprises s'assurent de la qualité de leurs données lorsqu'elles sont aussi nombreuses ?
En agissant à trois niveaux :

Adopter une approche fondée sur la valeur

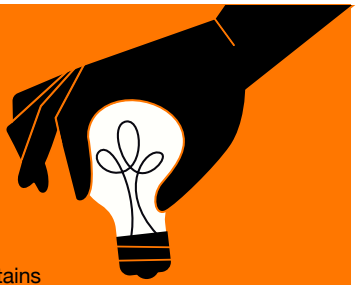
Tenter d'améliorer la qualité de l'ensemble de vos données revient souvent à risquer que rien ne soit accompli. Mieux vaut commencer par identifier les domaines où l'IA apportera une réelle valeur, cela vous aidera à évaluer les cas d'usage les plus prometteurs et à construire progressivement des bases de données conformes aux bonnes pratiques. Si vous partez d'un cas d'usage précis, vous pourrez déterminer les données nécessaires et concentrer vos efforts sur la garantie de leur qualité. Vous aurez ainsi confiance dans les données utilisées, et donc dans les résultats obtenus.

Cette logique s'applique également aux données non structurées, mails, présentations et autres documents, pour affiner les modèles et réussir une stratégie RAG (retrieval augmented generation) (voir section suivante). Il est donc indispensable d'établir une gouvernance, avec des critères précis définissant ce que l'on entend par « qualité documentaire ».



Monter en puissance progressivement

Une approche centrée sur la valeur offre la possibilité d'une évolution progressive. À chaque étape, vous vérifiez que les données mobilisées répondent aux exigences définies. Cela vous permet de constituer un portefeuille de cas d'usage aux résultats mesurables, tout en gardant la maîtrise des processus de gouvernance associés. Plutôt que de chercher à vous conformer à l'ensemble des réglementations possibles, vous vous concentrez uniquement sur les lois qui s'appliquent à vos cas d'usage.



Apprendre et itérer

Dans un domaine aussi dynamique que l'IA, la réussite dépend de votre capacité à apprendre et à itérer à la même vitesse. Lorsque certains cas d'usage se révèlent probants, les processus mis en place peuvent servir de base pour les déploiements futurs, notamment pour affiner et améliorer les jeux de données utilisés. Les enseignements tirés pourront être intégrés aux étapes suivantes, tandis que l'architecture, la gouvernance, la sécurité et la stratégie resteront pilotées par les cas d'usage identifiés.

Les grands modèles de langage (LLM) sont des réseaux neuronaux complexes, composés de milliards de paramètres. Au fil de leur développement et de leur entraînement, ils apprennent à raisonner, à inventer ou à générer, d'où le nom d'intelligence artificielle générative.

Exploiter les modèles de langage de manière appropriée

Les LLM sont devenus l'un des usages les plus visibles de l'IA, grâce à la large diffusion de services comme Bard, ChatGPT ou Copilot. En 2023, le nombre de nouveaux LLM lancés dans le monde a doublé par rapport à l'année précédente[4].

En partie en raison de cette forte exposition peut-être, les entreprises pensent qu'un unique modèle, utilisé via une application comme Bard ou ChatGPT, peut résoudre tous leurs problèmes. Or, cette idée repose sur une confusion : par nature, les LLM sont très larges, donc très génériques. Ils ne sont pas conçus spécifiquement pour répondre à des cas d'usage métier. Comme évoqué plus tôt, la réussite d'un projet d'IA repose sur l'alignement avec des cas d'usage précis. Par conséquent, les LLM doivent être adaptés et entraînés pour répondre aux objectifs d'une organisation.

Cela implique d'y consacrer du temps et des ressources, pour entraîner les modèles, apprendre à concevoir des prompts adaptés et définir des garde-fous afin de garantir que les réponses fournies soient bien conformes aux attentes métier. Plus concrètement, pour exploiter efficacement les LLM, les entreprises doivent :

1. Identifier et maîtriser les hallucinations

Les LLM sont des réseaux de neurones complexes, composés de milliards de paramètres. Grâce à leur entraînement, ils apprennent à raisonner, à inférer et à générer, d'où l'expression « IA générative ». Leur objectif n'est pas d'atteindre la vérité, mais de produire du contenu. Ce qui signifie que, lorsqu'ils ne connaissent pas la réponse à un prompt, ils peuvent en inventer une : c'est ce que l'on appelle une « hallucination ». Dans un contexte professionnel, cela peut avoir des conséquences importantes. Les entreprises doivent donc rester vigilantes face à ces hallucinations et mettre en place les garde-fous nécessaires. Cela passe par la mise en place de politiques et de procédures qui garantissent que les utilisateurs savent comment formuler des prompts correctement, en orientant le modèle dans le contexte approprié et en fournissant des informations contextuelles pour l'étayer par la bonne réponse.

2. Opter pour le fine-tuning ou la RAG

Il est bon de rappeler que même les LLM les plus performants sont des modèles génériques. Pour les adapter à des besoins

spécifiques, il faut trancher entre deux approches : les affiner (fine-tuning) ou recourir à la génération augmentée de récupération (RAG).

L'approche fine-tuning consiste à réentraîner le modèle sur les données propres à l'entreprise. Cela ne doit être fait qu'une fois et peut produire des résultats très pertinents pour un cas d'usage donné et pour l'ensemble de votre entreprise. En revanche, il s'agit d'une méthode coûteuse, chronophage et sujette aux hallucinations, en particulier lorsque le modèle est confronté à des prompts qui ne relèvent pas de son champ d'apprentissage.

La RAG, à l'inverse, consiste à concevoir des prompts avec vos connaissances spécifiques pour apporter du contexte. Cette approche peut se décliner à différents niveaux : simple (vous fournissez au modèle toutes les informations nécessaires directement dans un prompt) ou avec des approches plus avancées (le prompt est divisé afin d'amener le modèle à se concentrer sur des sections spécifiques). La RAG ne nécessite pas de réentraîner le modèle sur des données privées. En revanche, des experts du domaine doivent concevoir les prompts et évaluer la qualité des réponses générées.

3. La durabilité dans votre usage des LLM

Les LLM consomment d'importantes ressources de calcul. À mesure que les modèles deviennent capables de traiter des prompts plus longs et de produire des réponses plus développées, leur consommation énergétique augmente aussi. Il est donc essentiel d'évaluer si vous avez réellement besoin de toute cette capacité et de bien comprendre les implications liées à l'utilisation de prompts complexes générant de longues réponses. Il est également utile de réfléchir à la répétitivité des prompts : votre organisation posera-t-elle au modèle différentes variantes d'une même question de façon récurrente ? Dans ce cas, stocker les réponses et les rendre accessibles peut permettre de limiter le recours à ces prompts lourds et ainsi de réduire la demande en ressources de calcul.

4. Les implications sur la confidentialité des données

Si vous personnalisez un LLM pour votre cas d'usage, vous utiliserez nécessairement des données de l'entreprise. Cela implique de bien connaître les exigences réglementaires en matière de protection des données, d'autant plus que les modèles utilisés sont fournis par des tiers.

Selon les cas, vous devrez peut-être anonymiser les données, par exemple si vous utilisez un modèle pour analyser des contrats. Mais attention : cette anonymisation peut aussi réduire la pertinence des réponses.

5. Évaluer

Tout ce qui précède suppose un dispositif de retours d'expérience rigoureux. Il faut évaluer les réponses, revoir et affiner les prompts pour s'assurer que les modèles fonctionnent comme attendu. Mettre en place un cadre d'évaluation dès le début permet de suivre la qualité des réponses et de détecter la fréquence d'hallucination d'un modèle, autant d'enseignements qui permettent d'orienter les ajustements et réentraînements futurs.

Garantir la sécurité

La cybersécurité reste une préoccupation majeure pour les organisations. En s'engageant dans l'innovation numérique et en adoptant des technologies puissantes comme l'IA, elles introduisent également de nouvelles vulnérabilités, augmentant leur exposition aux attaques. D'autant que l'IA est aussi accessible aux attaquants qu'aux entreprises qui l'exploitent de manière éthique. Des failles connues peuvent désormais être exploitées plus rapidement, à moindre coût et à grande échelle.

C'est tout le paradoxe de la transformation numérique à l'échelle mondiale : les technologies conçues pour stimuler la croissance sont aussi susceptibles d'accélérer la prolifération d'actifs toxiques. Ces actifs, ce sont les personnes, les processus et les technologies qui mobilisent inutilement les ressources, génèrent de l'insatisfaction chez les collaborateurs et laissent persister des failles dans les systèmes des entreprises.

Selon les experts du secteur et les entreprises de cybersécurité, plus de 80 % des organisations présentent des vulnérabilités dans leur environnement IT. En moyenne, cela représenterait une faille par application. Si l'on considère le nombre d'applications utilisées par une entreprise numérique type, on commence à prendre la mesure du problème.

Autrefois, ce type de menace aurait été particulièrement inquiétant, mais restait sous contrôle : les cyberattaquants devaient disposer de compétences techniques avancées pour exploiter les failles. Ce n'est plus le cas aujourd'hui. La maturité croissante de l'intelligence artificielle a un impact majeur sur la cybersécurité, à deux niveaux :

D'abord, l'IA abaisse les barrières à l'entrée et permet à chacun d'en faire davantage, beaucoup plus rapidement. Ce gain de productivité est évidemment positif lorsqu'il concerne les employés, mais devient redoutable entre les mains des cybercriminels : il suffit de peu pour transformer une menace isolée en offensive massive. Une attaque qui nécessitait autrefois des semaines de préparation peut aujourd'hui être exécutée en quelques minutes, sur plusieurs cibles en parallèle. Si votre organisation utilise plusieurs centaines d'applications vulnérables, leur grand nombre ne constitue plus une protection : même un attaquant peu expérimenté peut les cibler simultanément.

Ensuite, la capacité de l'IA à automatiser les tâches répétitives accélère son adoption dans de nombreux services : RH, IT, développement, marketing, juridique… Mais comment s'assurer de l'absence de failles avant le déploiement de ces nouveaux outils ? Chaque nouvelle application peut créer une brèche potentielle.

C’est là tout le paradoxe de la numérisation à l’échelle mondiale : les technologies qui permettent une croissance accélérée sont aussi celles qui amplifient les risques liés aux actifs numériques dangereux.

Comment l’éviter ? En se concentrant sur quatre axes :

1. Débarrassez-vous des actifs toxiques

Face à l’ampleur des vulnérabilités, la plupart des entreprises n’ont pas les ressources pour tout corriger. Il est donc essentiel d’identifier les plus grandes vulnérabilités et de se débarrasser de ces actifs.

2. Adaptez la sécurité à vos usages

Traditionnellement, la cybersécurité d’entreprise est pensée par des experts et appliquée dans toute l’organisation. Or, les équipes sécurité ne sont ni responsables RH, ni commerciaux, ni marketeurs. Chaque fonction a ses propres priorités et pressions. Cela engendre des situations qui peuvent contraindre et pousser les collaborateurs à contourner les règles et créer, sans le vouloir, de nouvelles failles. La sécurité doit donc s’adapter aux besoins de l’employé, proposer des défenses efficaces mais non contraignantes et offrir des formations ciblées, construites sur des scénarios réalistes qui reflètent la manière dont les équipes opèrent.

3. Revise your security strategy

La majorité des dispositifs actuels reposent sur des approches et politiques traditionnelles, peu adaptées aux attaques automatisées et évolutives d’aujourd’hui. Elles ne sont pas conçues pour faire face à des attaques surpuissantes. Il faut réexaminer, réviser et élaborer une stratégie qui reflète la nature en constante évolution du paysage cybernétique actuel et des besoins des entreprises. Il faut s’ajuster et s’adapter, considérer la conformité comme un socle minimum, non comme un objectif en soi. La sécurité n’est plus un chantier ponctuel, mais un processus continu.

4. Ayez conscience de vos limites

Aucune entreprise ne peut tout faire seule, et aucun fournisseur ne peut couvrir toutes les éventualités. La cybersécurité moderne repose sur des écosystèmes de partenaires capables de comprendre les réalités du terrain et vos besoins spécifiques. Cela peut impliquer de mobiliser différemment des partenaires existants ou d’en intégrer de nouveaux. Quoi qu’il en soit, il s’agit d’une véritable rupture avec les principes et pratiques traditionnels.

Concevoir une infrastructure adaptée à l'IA

Les services réseau ont toujours été influencés par des demandes technologiques plus globales. Dans les années 1990, c'était la généralisation de la téléphonie mondiale. Il y a une dizaine d'années, l'essor massif des services en cloud. Chacune de ces étapes a nécessité une redéfinition des modes d'acquisition, de déploiement et d'utilisation des infrastructures réseau.

Aujourd'hui, la majorité des entreprises reconnaissent l'importance, voire le caractère stratégique, d'une infrastructure numérique adaptée. À l'échelle mondiale, 80 % des décideurs estiment qu'elle est essentielle à l'atteinte de leurs objectifs commerciaux. Cela vaut aussi pour les réseaux.

Avec l'explosion de l'IA, la pression s'intensifie. On sait déjà que les besoins en infrastructure vont croître fortement : 52 % des investissements GenAI prévus dans les 18 mois à venir concernent des infrastructures cloud, qu'elles soient publiques ou dédiées. Mais quel sera l'impact sur le réseau ?

Personne ne peut prédire avec certitude quels seront les usages de l'IA dans chaque entreprise ni les exigences que cela imposera aux réseaux pour les supporter.

Ce qui est certain, en revanche, c'est que le réseau devra s'adapter aux cas d'utilisation de l'IA. Il devra être capable d'absorber de grands volumes de données, avec une bande passante suffisante et une latence minimale, notamment pour les traitements en périphérie (Edge), rendus nécessaires par l'Internet des objets (IoT) et d'autres équipements connectés.

Il faudra aussi pouvoir répondre aux besoins de calcul massifs associés aux grands modèles de langage (LLM), que ce soit pour les entraîner ou pour garantir les performances des applications et services qui les exploitent.

Pour les responsables des infrastructures réseau, la difficulté réside dans l'incertitude : il est complexe d'anticiper précisément les besoins à venir. Mais l'attentisme n'est pas une option. L'adoption rapide de l'IA impose aux entreprises de mettre en place une stratégie résiliente, adaptable et évolutive.

À quoi doit ressembler cette stratégie ?
Elle repose sur plusieurs piliers :

1. **Un design orienté usage**
   Comme nous l'avons vu, c'est le cas d'usage qui détermine l'utilisation d'une IA. Il influencera l'architecture réseau : comme l'emplacement de l'IA (à la périphérie ou en cloud) ou le degré de décentralisation de l'entreprise (et de ses données). Dans tous les cas, il faudra garantir que le réseau supporte la puissance de calcul, une connectivité à haut débit et des données en mouvement.

2. **Confidentialité, sécurité et réglementation**
   Nous avons largement abordé les implications de l'IA en matière de confidentialité et de sécurité des données. Mais une autre question clé est celle de l'acheminement des données vers les applications concernées. À mesure que le stockage devient plus décentralisé, la sécurisation des réseaux entre les sources de données, le calcul et les applications devient essentielle au maintien de la confidentialité. Il faut également tenir compte des enjeux de souveraineté vis-à-vis de l'endroit où vos données sont stockées ainsi que des incohérences entre les zones géographiques pouvant entraîner une élasticité accrue. Or, ces exigences varient d'un pays à l'autre, ce qui impose aux réseaux une plus grande souplesse.

   Et s'il n'y a pas eu de grands changements récents en matière de régulation, cela devrait arriver. Tout déploiement de réseau doit donc pouvoir répondre aux changements induits par la législation.

3. **Gérer la congestion, le trafic et la disruption**
   La croissance du trafic est inévitable. Avec elle, le risque de congestion augmente, ce qui peut dégrader la vitesse de traitement et accroître la latence. Les applications commerciales de l'IA pourraient, à l'avenir, nécessiter un accès à une connectivité rapide, sécurisée et à faible latence pour fonctionner correctement et donner leur pleine mesure.
   En parallèle, les réseaux, qu'ils soient publics ou privés, restent exposés aux perturbations. Nous évoluons peut-être dans un monde virtuel basé sur les clouds, mais la connectivité qui en est le moteur repose sur des câbles très physiques. Comme l'actualité nous le rappelle régulièrement, ces infrastructures physiques peuvent être affectées par des événements environnementaux ou géopolitiques. Pour qu'une stratégie soit efficace, elle doit obligatoirement prévoir des mesures d'urgence, permettant de maintenir la qualité des services sans dégradation et d'intégrer pleinement la mise en réseau dans l'approche globale.

4. **Gouvernance de l'IA**
   Le réseau joue également un rôle central dans la gouvernance de l'IA. Ce point est fondamental : une mauvaise gouvernance peut entraîner des erreurs de déploiement, des violations et une exposition des données. Il est donc crucial dans le cadre d'une bonne gouvernance de savoir qui gère les données, d'en vérifier la fiabilité et de s'assurer que l'ensemble de l'infrastructure, y compris le réseau, offre la transparence et la sécurité nécessaires. On ne peut pas faire confiance à des données transmises par un réseau non sécurisé.

Création de valeur

L'intelligence artificielle offre aux entreprises des opportunités majeures pour transformer leur manière de travailler et faire évoluer leur modèle opérationnel. Elle peut devenir un socle fondamental de croissance et de performance durable, qu'il s'agisse d'offrir de nouvelles opportunités de partenariats ou de revenus.

Les entreprises en ont bien conscience. Dans le seul domaine de l'IA générative, Gartner prévoit que, d'ici 2026, plus de 80 % des entreprises auront utilisé des interfaces de programmation (API) ou des modèles d'IA et/ou déployé des applications basées sur l'IA dans des environnements de production, contre moins de 5 % en 2023. Autrement dit, la question de savoir si les entreprises vont adopter l'IA ne se pose plus. Les barrières à l'entrée sont tombées, avec une multitude d'outils et de services désormais accessibles, proposés aussi bien par les géants de la tech que par l'écosystème open source. Toute entreprise qui souhaite rester compétitive, et a fortiori prospérer, doit intégrer cette technologie. Elle doit donc comprendre comment la déployer avec succès au sein de son organisation.

L'un des pièges fréquents consiste à croire que, lorsque les prix baissent, il faut attendre que les coûts continuent de baisser. Or, dans un contexte où la capacité à entraîner les modèles et à en extraire de la valeur dépend étroitement du déploiement effectif de la technologie, il est bien plus pertinent de l'utiliser rapidement que de chercher à économiser quelques sous sur les dépenses d'investissement.

Il ne faut pas non plus négliger la mise en place d'indicateurs clés de performance (KPI) adaptés. Un client d'Orange Business considère qu'un seuil de 60 à 70 % de qualité des données suffit à générer de la valeur avec ses services d'IA. Pourtant, la plupart des organisations n'ont pas défini de métriques équivalentes. C'est un cas d'école : « Ne pas se préparer, c'est se préparer à échouer. » Si vous ne définissez pas clairement ce que vous attendez de votre projet IA, comment savoir s'il tient ses promesses ?

Il est également important de souligner que, à mesure que l'IA devient plus largement accessible, elle perd son avantage en tant que différentiateur concurrentiel. L'enjeu ne réside plus dans l'usage de l'IA en soi, mais dans la manière dont elle est utilisée. C'est ce qui fera la différence en termes de création de valeur.

De manière plus large, plusieurs questions doivent être abordées dans l'élaboration de votre business case :

À quelle distance de vos clients souhaitez-vous positionner vos outils ?

Il existe déjà des exemples d'IA interagissant directement avec les clients, les chatbots étant l'exemple le plus évident, mais cela ne devrait se faire que dans des déploiements très spécifiques et contrôlés. Par exemple, une mauvaise expérience, comme une hallucination, pourrait nuire à vos relations clients et à la réputation de votre marque. Utiliser des chatbots pour filtrer les demandes des clients est logique ; les situations plus complexes et ouvertes devraient être laissées aux agents humains.

Avez-vous évalué les biais de vos outils ?

Nous portons tous des préjugés, et chaque création, y compris les outils d'intelligence artificielle, en est inévitablement imprégnée. Pour en limiter l'impact, il est donc essentiel de sélectionner les modèles d'IA les plus pertinents pour vos besoins spécifiques, car leur efficacité varie considérablement.

Comment l'IA s'intègre-t-elle à votre environnement technologique actuel ?

Selon votre pile technologique actuelle, ajouter une brique IA peut revenir à faire cohabiter la science des fusées et l'âge de pierre. Il est donc fondamental d'anticiper cette intégration dès la phase de planification, sans quoi les gains espérés, qu'ils soient financiers, opérationnels ou commerciaux, risquent de ne jamais se concrétiser.

Quelles sont les implications en matière de confidentialité et de sécurité ?

Vous devez impérativement comprendre les aspects juridiques liés à vos usages. D'où proviennent les données qui entraînent votre IA ? Enfreignent-elles les droits d'auteur ? Exposent-elles votre système à des cyberattaques ? Enfreignez-vous les réglementations sur la protection de la vie privée en utilisant certains types de données pour entraîner et informer l'IA ? Ces questions doivent être résolues avant même de commencer.

Votre avenir fondé sur l'IA, plus difficile à concrétiser que vous ne le pensiez

Vous allez rencontrer des obstacles : la clé sera de savoir comment les surmonter.

L'IA n'est pas parfaite. Ceux qui s'y intéressent en connaissent déjà les limites actuelles. Pourtant, elle est déjà utilisée dans de nombreux secteurs, de l'industrie à la santé. Les entreprises s'engagent dans des phases d'expérimentation, de projets pilotes ou de tests de concepts. L'enjeu majeur est de discerner ce qui est véritablement efficace et ce qui peut être industrialisé. Celles qui parviendront à opérationnaliser leurs déploiements de manière fluide acquerront un avantage concurrentiel significatif.

Nous avons partagé ici des recommandations concrètes qui, nous l'espérons, vous aideront à bâtir votre avenir fondé sur l'IA. Si nous ne devions retenir qu'un seul message, ce serait celui-ci : ne sous-estimez pas les défis liés au passage d'une PoC à un service d'IA opérationnel à l'échelle. L'enquête menée par GlobalData l'a confirmé : les projets d'IA prennent plus de temps et nécessitent plus de ressources que prévu, car les défis liés à leur opérationnalisation sont largement sous-estimés.

Comme le disait Henry Ford, « les obstacles sont ces choses effrayantes que vous apercevez quand vous perdez de vue votre objectif ». Pour rester concentré sur vos priorités, assurez-vous que votre réseau peut soutenir les cas d'usage pertinents pour votre activité, soyez intransigeant par la qualité de vos données maintenez vos politiques de gouvernance et de sécurité à jour, et, surtout, entourez-vous des bons partenaires pour faire face aux défis que vous ne manquerez pas de rencontrer.

Comment Orange vous accompagne

Nous sommes un fournisseur de services numériques « network-native », reconnu depuis plusieurs décennies pour la protection des données critiques de nos clients. Orange Cyberdefense fait également partie des leaders mondiaux des services de cybersécurité. Et nous utilisons l'IA dans nos propres activités depuis plusieurs années : nos outils d'IA interviennent dans l'ensemble de notre réseau, nos collaborateurs s'appuient sur l'IA générative pour créer du contenu ou piloter leurs projets, et nos services sont eux-mêmes assistés par des capacités d'intelligence artificielle. L'intelligence des menaces est au cœur de notre approche basée sur les risques en cybersécurité. L'expertise accumulée par cette combinaison unique d'expériences, enrichie par un écosystème de partenaires de référence, nous permet de co-construire avec nos clients des services IA créateurs de valeur, durables et adaptés à leurs enjeux.

Nous disposons des compétences et de l'expérience nécessaires pour vous aider à :

- Garantir la qualité des données indispensables à vos déploiements IA.
- Tirer pleinement parti des LLM.
- Développer et fournir une posture de sécurité adaptée aux exigences actuelles et futures de l'IA.
- Déployer un réseau performant à haute vitesse et faible latence, capable de soutenir vos services IA, où qu'ils soient.
- Maximiser la valeur de vos services IA en comprenant les KPI et les risques associés.

Contactez-nous dès aujourd'hui pour mener avec succès l'opérationnalisation de l'IA au sein de votre organisation

1. https://www.dataiq.global/articles/2025-ai-and-data-leadership/#:~:text=Most%20organizations%20believe%20that%20AI,2024%20to%2089%25%20in%202025.
2. https://www.bcg.com/press/12january2024-ceos-genai-hype-or-experimenting#:~:text=According%20to%20a%20new%20report,and%20GenAI%20roadmap%20and%20investment
3. https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf
4. https://blogs.idc.com/2022/12/09/idc-futurescape-worldwide-future-of-digital-infrastructure-2023-predictions/
5. https://www.idc.com/getdoc.jsp?containerId=US51313423
6. https://www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-ofenterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026