

DIGILLIA

conseil et ingénierie en
intelligence artificielle



**L'intelligence
artificielle expliquée
aux entreprises**

Pourquoi ne pouvez-vous plus ignorer l'intelligence artificielle ?

L'intelligence artificielle (IA) est un processus d'imitation de l'intelligence humaine qui repose sur l'apprentissage. La machine améliore ses capacités avec les exemples qui lui sont soumis pour son entraînement.

La grande majorité des algorithmes sur lesquels reposent l'intelligence

artificielle existe depuis des décennies mais l'accès à des grands volumes de données et le développement des capacités de calcul des processeurs graphiques ont récemment permis d'atteindre ou de dépasser les capacités humaines pour de nombreuses tâches.





● **1950**

Alan Turing propose un test de l'intelligence des machines

● **1955**

John McCarthy invente le terme «intelligence artificielle»

● **1957**

Frank Rosenblatt développe le perceptron, ancêtre des réseaux de neurones

● **1986**

Rumelhart, Hinton et Williams inventent la «backpropagation»

● **1979**

Kunihiko Fukushima invente le néocognitron, ancêtre des CNN

● **1964**

Joseph Weizenbaum développe Eliza, premier système de traitement du langage naturel

● **1994**

Chinook est le premier logiciel à gagner un championnat du monde

● **1997**

IBM DeepBlue bat Kasparov, champion du monde d'échecs

● **1998**

Yann LeCun développe LeNet-5, premier réseau de neurones convolutif (CNN)

● **2012**

AlexNet gagne le challenge ImageNet de classification d'images

● **2011**

IBM Watson gagne Jeopardy contre deux anciens champions

● **2008**

La reconnaissance vocale est intégrée aux téléphones mobiles (Google, Apple)

● **2014**

Le chatbot Eugene Goostman trompe le test de Turing

● **2014**

Ian Goodfellow développe les GAN pour générer des images

● **2015**

DeepMind AlphaGo bat Lee Segol, champion du monde de jeu de Go

● **2018**

Microsoft NMT produit des traductions de qualité professionnelle

● **2018**

L'IA bat les humains au test de compréhension de Stanford

● **2017**

Une équipe de Google développe les «transformers» à l'origine de GPT

● **2019**

La FDA a approuvé 39 algorithmes à usage médical

● **2021**

DeepMind AlphaFold2 résout le repliement des protéines

● **2022**

OpenAI lance ChatGPT

Qu'est-ce que l'intelligence artificielle?

Le concept le plus important à comprendre concernant l'apprentissage machine (machine learning) est l'approche fondamentalement différente de la création de logiciel. La machine infère le résultat à partir d'exemples, au lieu de suivre un jeu d'instructions (code) conçu spécifiquement pour ce résultat.

Cette approche est particulièrement intéressante pour modéliser les prédictions et les décisions dont le savoir est tacite, car chacun sait beaucoup plus qu'il ne le réalise et qu'il peut donc expliquer, après des années de pratique.

Il existe plusieurs modèles d'inférences en fonction du type

d'exemples et de résultats que l'on souhaite obtenir mais ceux-ci restent génériques. L'intelligence artificielle est une collection de modèles, aujourd'hui regroupés en 4 grandes familles.

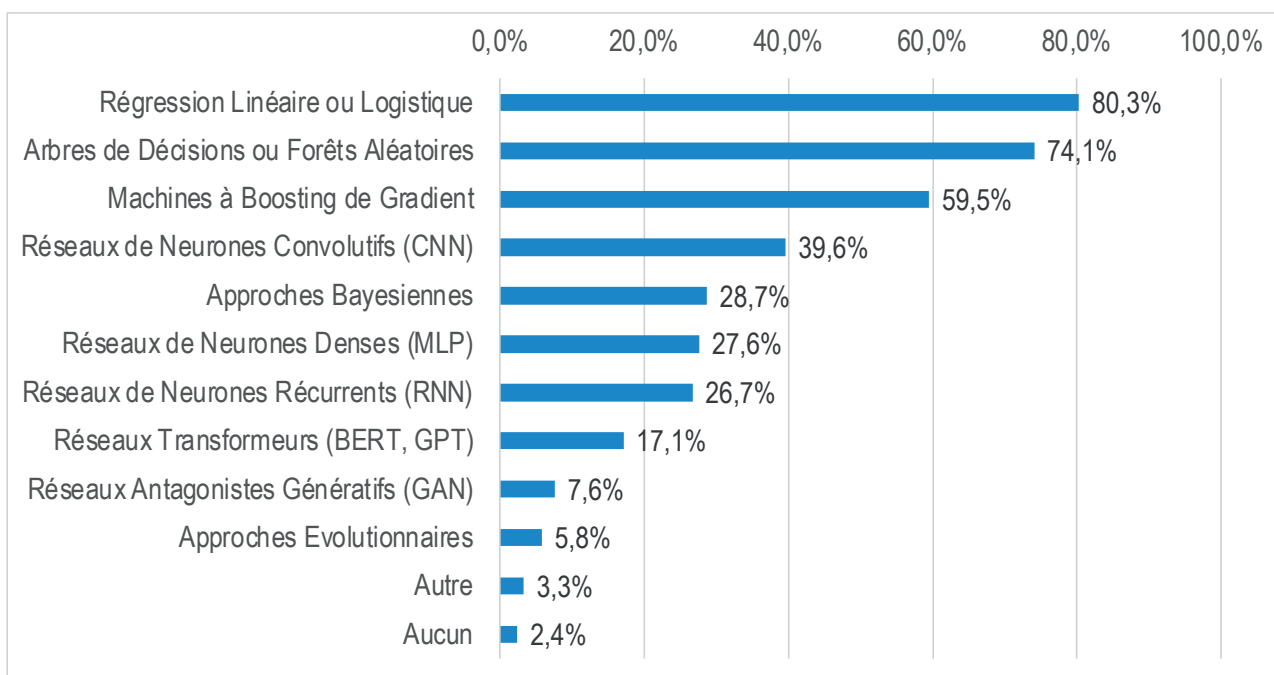
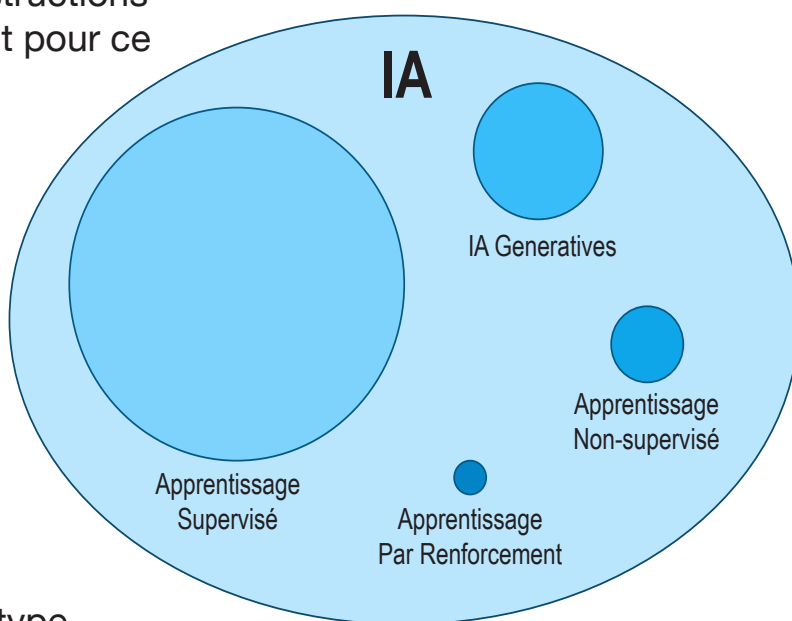


Fig: Usage des algorithmes d'apprentissage machine par les utilisateurs de Kaggle



Apprentissage Supervisé

L'apprentissage supervisé enseigne au modèle à produire les résultats souhaités en lui fournissant des données d'entraînement comprenant des entrées X et des sorties y correctes. Une fois entraîné avec ces données, le modèle peut prédire les sorties y' correspondant à de nouveaux jeux d'entrées X' . L'apprentissage supervisé résout deux types de problèmes : la classification quand la prédiction est une catégorie discrète, et la régression quand la prédiction est une quantité continue.

Apprentissage Non-supervisé

L'apprentissage non-supervisé recherche les similarités ou les différences dans les données, et permet de découvrir des motifs cachés, des regroupements, des associations, et des corrélations.

Apprentissage Par Renforcement

L'apprentissage par renforcement d'un modèle d'IA recherche un comportement décisionnel optimal en fonction d'un état courant dans un environnement qui récompense de manière positive ou négative des expériences. Au fil des expériences, le modèle apprend à optimiser ses décisions, en maximisant la somme des récompenses au cours du temps. L'apprentissage par renforcement a permis de vaincre les meilleurs joueurs aux échecs et au jeu de Go.

Intelligence Artificielle Générative

L'intelligence artificielle générative est capable de générer du texte, des images, des sons, du code, et d'autres données à l'aide de modèles génératifs, comme les transformers, sur lesquels sont fondés les modèles de langage larges. Les modèles d'IA générative utilisent de vastes quantités de données pour apprendre à générer de nouvelles données présentant des caractéristiques similaires. Dans leur version Chat, ces modèles répondent de manière probabiliste à des invitations, notamment des questions.

Optimisation Mathématique

Il est important de mentionner aussi l'optimisation mathématique (linéaire, combinatoire, etc.), d'abord parce que l'entraînement des modèles d'IA utilise des algorithmes d'optimisation comme la méthode du gradient, et surtout parce que l'optimisation mathématique permet de résoudre toute une classe de problèmes d'optimisation avec contraintes mieux que les méthodes d'apprentissage de l'IA. Il est donc important de distinguer les problèmes d'IA, des problèmes d'optimisation, afin de choisir les bons outils.

Comment détecter les opportunités IA ?

Dans le cadre d'une culture digitale orientée IA, il y a trois questions essentielles auxquelles tout employé doit savoir répondre pour dénicher les opportunités de création d'efficacité et/ou de valeur par l'usage de l'intelligence artificielle.

Quand l'IA excelle-t-elle ?

Dans toutes les situations où il y a une prédiction à faire et où il existe une masse d'exemples sous forme de données digitalisées, l'intelligence artificielle doit être considérée pour rendre l'entreprise plus compétitive sur le terrain des prix, de l'excellence opérationnelle, et/ou de la supériorité des produits, par exemple :

- L'entreprise dispose d'un historique des ventes sur 10 ans pour prédire ses ventes futures et opti-

miser ses stocks.

- L'hôpital dispose de milliers de radios diagnostiquées pour assister les médecins avec une interprétation automatique.
- Le fabricant dispose d'un historique des pannes pour prévoir les opérations de maintenance afin de minimiser les temps d'arrêt et les coûts de réparation.

L'IA excelle quand la fonction de prédiction est simple et qu'il y a suffisamment de données pour la modéliser.

Quand faut-il éviter ou limiter l'IA ?

Inversement l'IA est inapte quand la fonction de prédiction est complexe et qu'il y a insuffisamment de don-

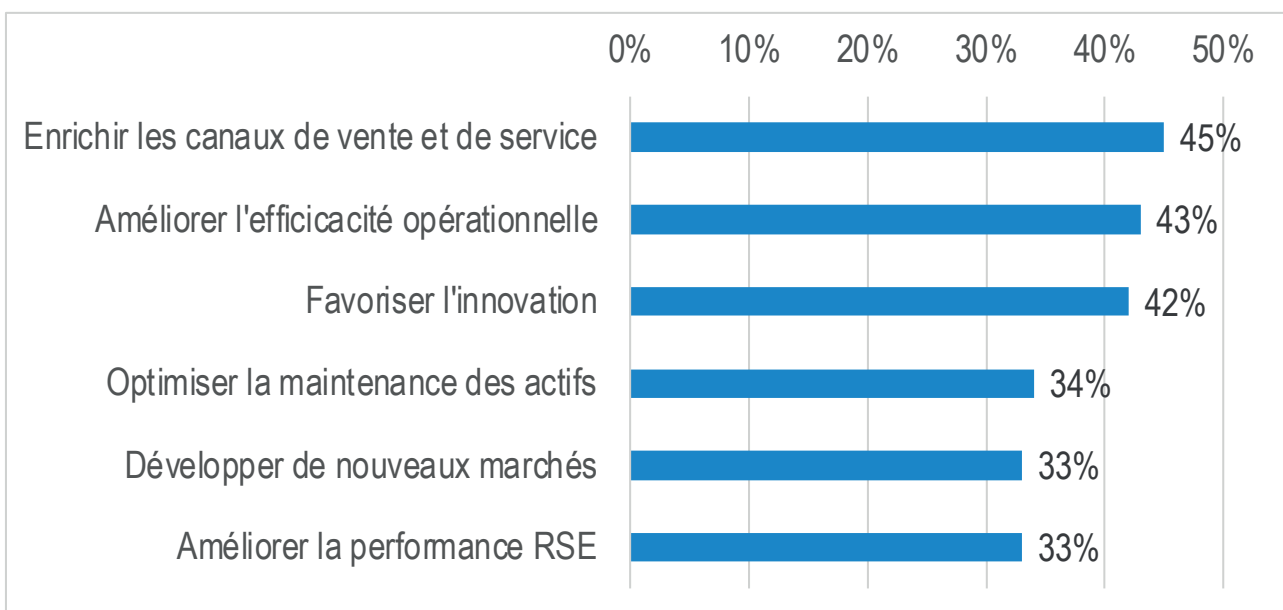


Fig: Objectifs entrepreneuriaux des projets d'IA d'après MIT Technology Review

nées pour la modéliser.

Les prédictions faites par l'intelligence artificielle sont généralement assorties d'un score probabiliste qui n'assure jamais une certitude de 100%. En plus, l'intelligence artificielle, en particulier les réseaux de neurones, souffrent d'un manque d'interprétabilité. En d'autres termes, le processus de décision des modèles est difficile à comprendre et fait donc peser 3 risques : (i) un risque de partialité, (ii) des prédictions inattendues dans certains cas, (iii) une

complexité algorithmique qui obscurcit l'identification et la correction des erreurs. Pour ces raisons, certaines décisions ne peuvent pas être confiées à l'IA qui doit être limitée à un rôle d'assistance, comme l'aide au diagnostic médical.

Comment envisager l'IA ?

Beaucoup pensent que l'intelligence artificielle pourrait automatiser leur métier et les remplacer comme la voiture motorisée a mis fin au métier de cocher.

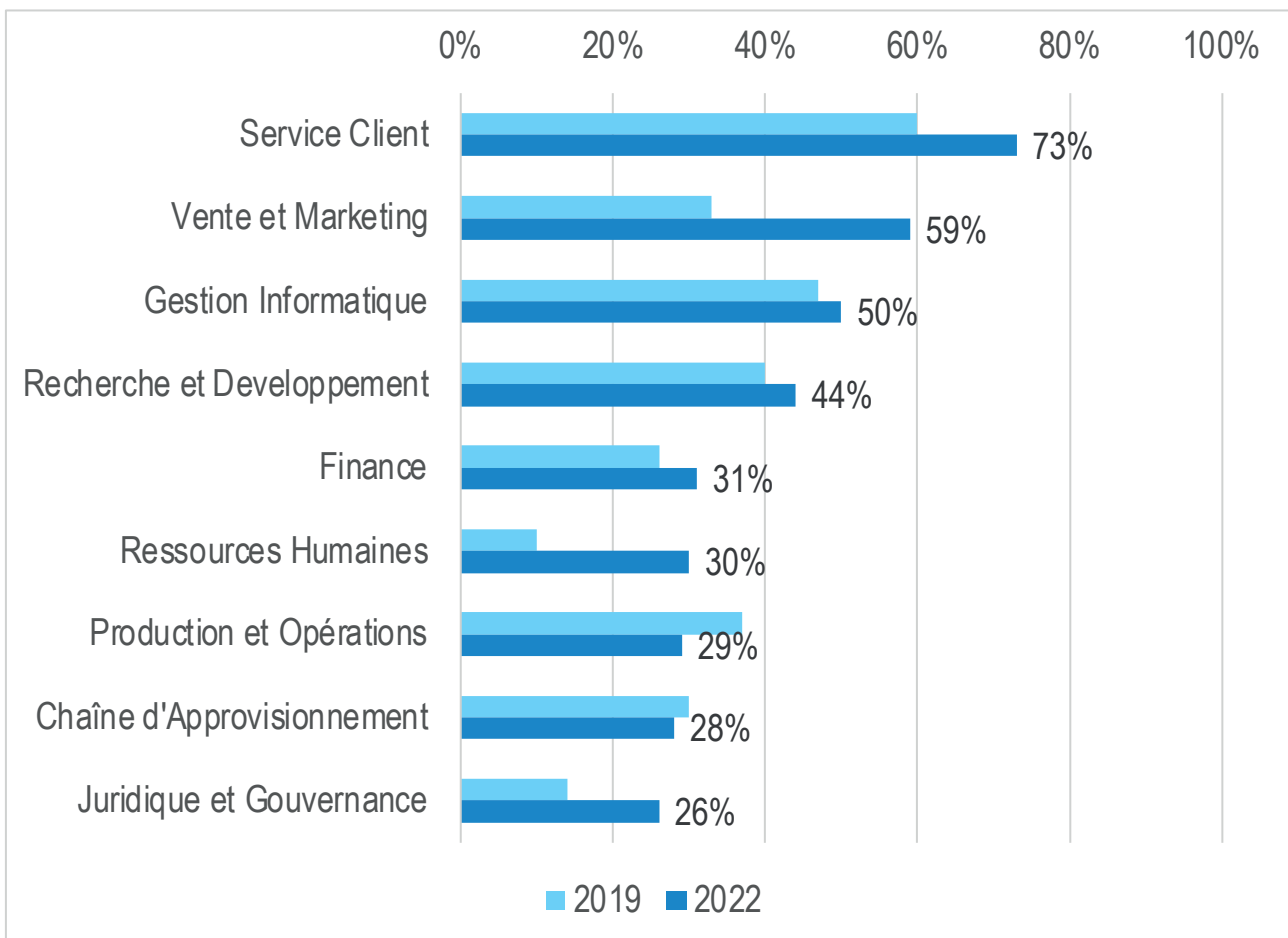


Fig: Usage de l'IA dans les départements d'entreprises d'après MIT Technology Review



Les travaux de Erik Brynjolfsson, Tom Mitchell, et Daniel Rock sur la base O*Net liant 966 métiers à 19.612 tâches montrent que quasiment aucun métier n'est fait que de tâches automatisables par l'IA, que presque tous les métiers comportent au moins une tâche susceptible d'être automatisée ou améliorée par l'IA, et qu'il y a une grande variabilité dans l'exposition des métiers à l'IA. La grande majorité des métiers va perdurer, mais les travailleurs qui savent utiliser efficacement l'IA remplaceront ceux qui ne le savent pas, car l'IA réduit le niveau de compétence nécessaire pour atteindre les meilleures performances.

En fait, un métier est un ensemble de tâches. Ces tâches sont spécialisées (requièrent de l'expertise), banales (pas d'expertise), automatisables ou améliorables par les technologies.

L'IA amène à repenser les ensembles de tâches qui forment les métiers. Par voie de conséquence, repenser les métiers amène à repenser les processus, et donc à transformer la manière dont les entreprises opèrent.

Afin de déterminer où appliquer l'IA dans l'entreprise :

1. Considérez les métiers des employés et des sous-traitants de l'entreprise et divisez-les en tâches.
2. Examinez chaque tâche pour voir si elle peut faire l'objet d'une assistance (augmentation) ou d'une automatisation à l'aide d'outils d'IA tels que l'apprentissage supervisé ou l'IA générative.
3. Évaluez le retour sur investissement, les bénéfices non quantifiables, et les risques, pour fixer vos priorités.



Comprendre le rôle des données au cœur de l'IA

Un critère pour qu'une tâche soit susceptible d'être automatisée ou améliorée par l'IA est que l'ensemble des entrées X et l'ensemble des sorties y de la tâche puissent être suffisamment bien mesurés pour qu'une machine puisse apprendre la correspondance f entre les deux ensembles grâce à un nombre suffisant d'exemples pour déterminer la relation $y=f(X)$.

Combien d'exemples faut-il ? La réponse simple est le plus le mieux, mais cela dépend de la complexité de la relation et de la qualité des données.

Dans le cas d'une tâche à une entrée et une sortie, dont la relation est linéaire, il peut suffire de deux exemples précis.

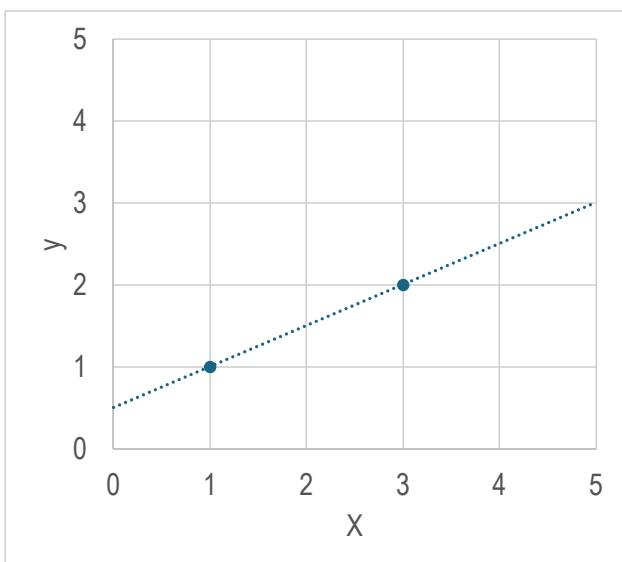


Fig: Relation simple.

Pour une relation plus complexe, le

nombre d'exemples nécessaires augmente.

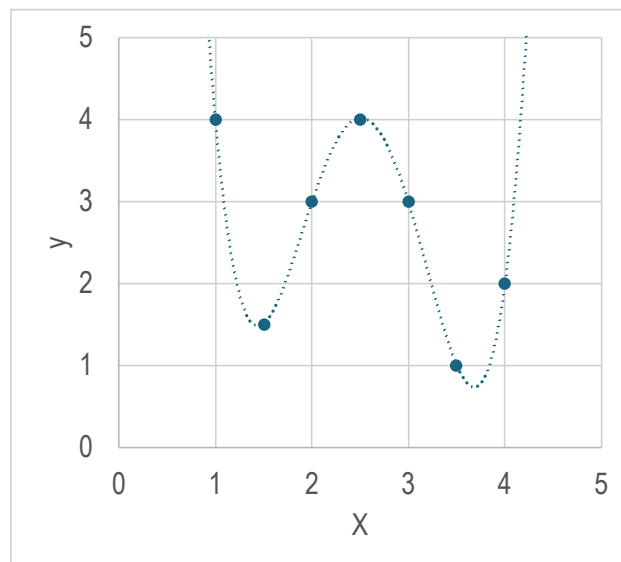


Fig: Relation complexe.

Maintenant, imaginons que la tâche ait N entrées ou caractéristiques x_1, x_2, \dots, x_N , dont la valeur est comprise dans un espace $[0, 1]$. L'espace des données est donc un hypercube de dimension N et de côtés 1. Imaginons que nous divisions cet hypercube en 10 sur chacun de ses côtés. De cette manière, l'hypercube de côtés 1 contient 10^N petits hypercubes de côtés 0,1. Si la complexité de la relation exige 1 exemple dans chacun des petits hypercubes pour la modéliser pour l'ensemble des valeurs possibles des caractéristiques, il faut 10^N exemples pour entraîner un modèle d'IA qui se substituera à la tâche.

Le besoin en données augmente exponentiellement avec le nombre



d'entrées de la tâche. C'est ce que l'on appelle la « malédiction de la dimensionnalité » en apprentissage machine.

D'une manière générale, on considère que le nombre d'exemples doit être au moins 10 fois le nombre de paramètres d'un réseau de neurones pour l'entraîner, mais la qualité affecte le besoin en données, en particulier les données manquantes, les données aberrantes, les données bruitées (mauvaise précision de la mesure), les données corrélées, nécessitent d'être compensées.

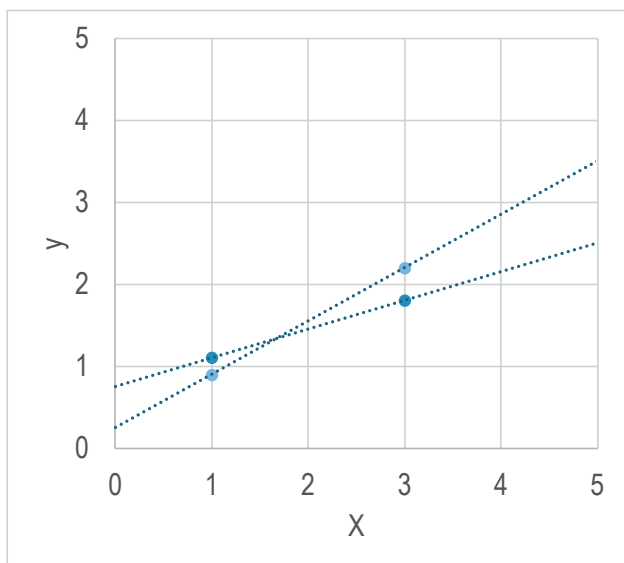


Fig: Impact d'une erreur de $\pm 10\%$ dans la mesure des exemples utilisés pour modéliser une relation linéaire, par exemple un capteur précis à $\pm 10\%$.

Il existe des techniques pour sélectionner les données non corrélées, réduire la dimensionnalité, et traiter le bruit, mais il est important de comprendre que l'entraînement des mo-

dèles d'IA nécessite des données de qualité, en quantité suffisante, car de mauvaises données engendrent de mauvaises prédictions.

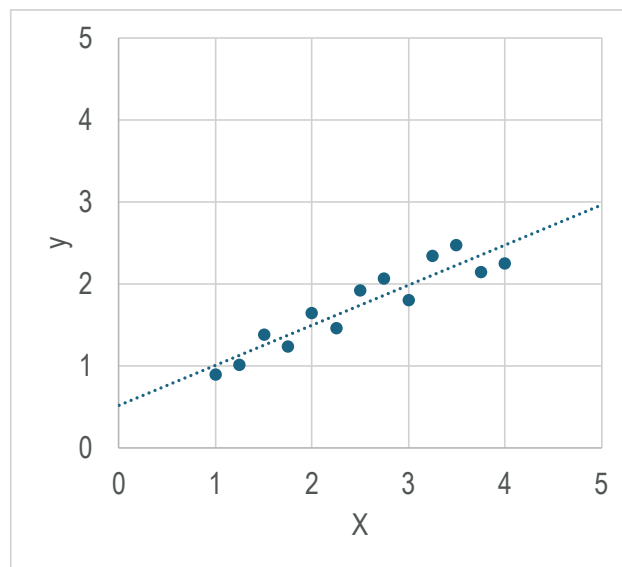


Fig: La multiplication des exemples peut permettre de compenser un bruit de $\pm 10\%$ par effet de moyenne.

Néanmoins, de nombreux exemples de projets réussis ont été réalisés en utilisant de petits ensembles de données. Selon une enquête menée par Kaggle en 2020, plus de la moitié des personnes interrogées ont déclaré avoir réalisé un projet d'apprentissage machine avec moins de 5 000 échantillons. Par exemple, une équipe de l'Université de Stanford a utilisé un ensemble de données de seulement 1 000 images pour créer un système d'IA capable de diagnostiquer avec précision le cancer de la peau.



Des données de qualité remplissent plusieurs critères. Elles doivent être:

- Pertinentes (avoir une relation directe avec la sortie),
- Complètes (pas de données manquantes),
- Cohérentes (pas de données aberrantes ou mal formatées),
- Actuelles (peut nécessiter une réactualisation périodique ou continue),
- Représentatives (couvrir l'ensemble de l'espace des données),
- Précises (précision forte, bruit faible).

Votre responsabilité	Notre responsabilité
Données de qualité Objectif clair et faisable avec ces données	Extraction des caractéristiques Sélection, configuration et entraînement du modèle
Responsabilité partagée	
Déploiement sur votre infrastructure	



Le danger d'ignorer ou de retarder l'adoption de l'IA

L'intelligence artificielle, en particulier l'apprentissage machine, est la nouvelle technologie à usage général la plus importante depuis l'Internet, car les modèles d'intelligence artificielle sont depuis peu supérieurs aux humains dans l'exécution de nombreuses tâches avec des gains de productivité énormes. Les entreprises qui continuent de diviser le travail entre humains et machines perdront de plus en plus leur avantage concurrentiel au profit de celles qui intégreront efficacement les capacités de l'IA aux capacités humaines.

Pourtant de nombreuses entreprises attendent que la technologie mûrisse avant de l'adopter, mais cette approche de « suiveur » pose plusieurs problèmes.

- La transformation des tâches assistées ou automatisées par l'IA, nécessitera de reconcevoir les métiers et les processus de l'entreprise. La résistance au change-

ment et les besoins de formation ne doivent pas être sous-estimés.

- Les mentalités sont longues à évoluer. Il faut des succès pour diffuser une culture data qui développe une adhésion étendue à toute l'entreprise.
- Les systèmes génériques ajouteront peu de valeur à l'entreprise car ils sont accessibles à tous. Il faut de l'expérience pour construire une infrastructure qui permette de les adapter, de les configurer, et de les déployer dans un cycle d'amélioration continue (MLOps).

Le temps qu'un suiveur ait effectué une transformation tardive, les premiers adoptants auront acquis des gains de productivité et conquis des parts de marché considérables. Les suiveurs pourraient ne jamais rattraper leur retard, à l'instar des entreprises qui ont trop tardé à adopter l'internet.



Comment démarrer ?

Il est recommandé de démarrer avec des séminaires ou des réunions de présentation pour sensibiliser les équipes aux capacités et aux incapacités de l'IA, car les cas d'utilisation viennent des gens du métier.

Ceci devrait permettre d'identifier rapidement un ou deux projets pilotes de nature à entraîner l'organisation sur la voie de la transformation par l'IA, en notant qu'un bon projet pilote doit :

- Résoudre un problème spécifique qui crée de la valeur pour l'entreprise,
- Avoir la bonne taille : ni trivial, ni trop complexe, pour être faisable,
- Permettre un succès rapide et probant.

Avant de lancer un projet pilote d'IA, les dirigeants doivent clairement

communiquer la valeur pour l'entreprise, exposer le calendrier et les résultats souhaités, allouer un budget raisonnable, et construire une petite équipe dédiée. A ce stade, il est recommandé de collaborer avec des experts externes pour accélérer le calendrier du projet.

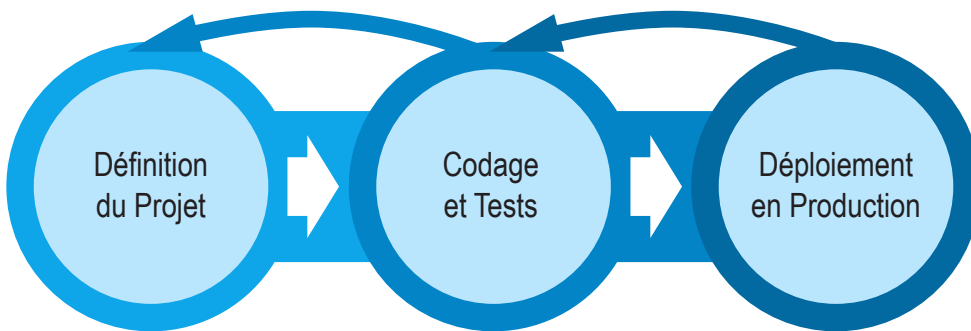
Lorsque le projet pilote atteint des étapes clés, et surtout lorsqu'il donne un résultat positif, l'équipe doit célébrer et communiquer le succès au sein de l'entreprise.

L'expérience doit alors être mise à profit pour établir la data et l'IA au cœur de la stratégie, conduire la transformation par l'IA, définir les profils à recruter, et construire une infrastructure pour le déploiement à échelle des projets d'IA, de façon à en faire un avantage compétitif durable.

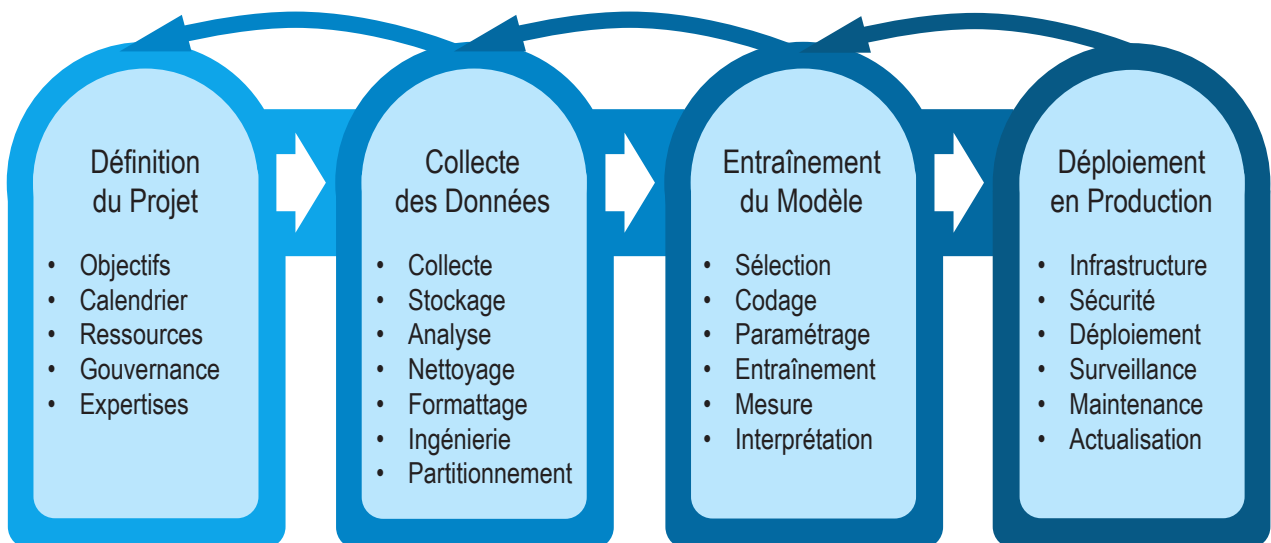


Conduite de projets d'IA

La conduite d'un projet de développement de logiciel suit le processus typique suivant. La différence principale entre un processus en cascade et un processus agile est la durée d'une itération (version ou sprint).

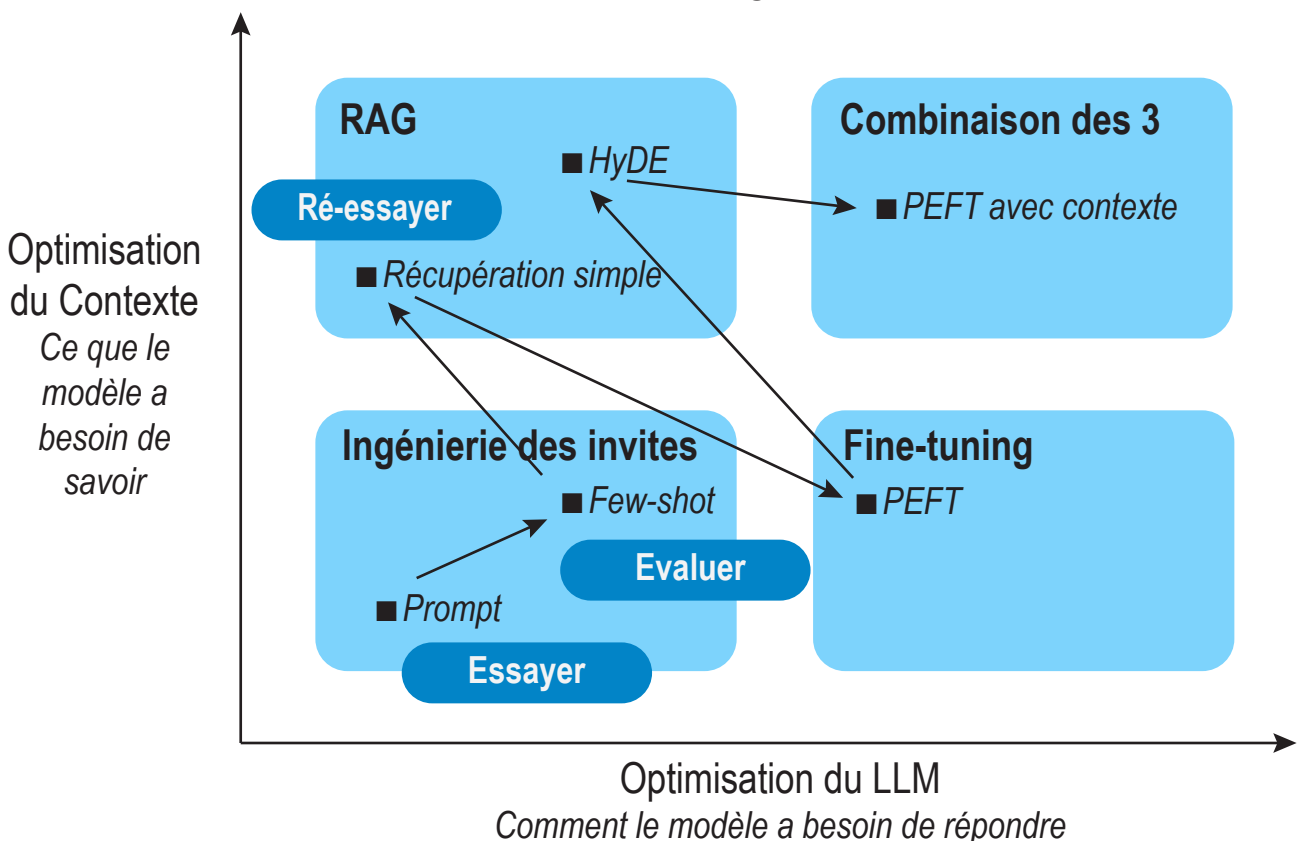


La conduite d'un projet d'IA implique une étape supplémentaire compte tenu du rôle des données (Système IA = Modèle + Données).



Les projets d'IA générative avec les LLMs nécessitent une approche plus expérimentale de type essai-erreur durant la phase d'entraînement du modèle :

- L'ingénierie des invites (prompt engineering) permet de raffiner les instructions notamment au moyen d'exemples (few-shot prompting) pour influencer les réponses.
- Si le modèle de langage large nécessite des données privilégiées et/ou récentes pour fournir une réponse pertinente, celles-ci peuvent lui être fournies par des techniques de génération augmentée de récupération (RAG).
- Finalement, si le modèle doit répondre dans un style ou dans un format systématique, celui-ci peut être ajusté (fine-tuning) à cet effet. De nombreux modèles ont une version Chat ajustée à partir d'un modèle de base pour des échanges conversationnels.
- Ultiment, il est possible de créer un LLM spécialisé (pre-training) pour mieux traiter le vocabulaire et la connaissance d'un domaine spécifique, en notant que l'entraînement de Bloomberg-GPT, un LLM dédié à l'information financière, a coûté plusieurs millions de dollars, de sorte que cette option est limitée aux grandes organisations.



Infrastructure MLOps pour IA à grande échelle

Dans tous les domaines, la qualité est assurée par deux fondements :

1. Des mesures (et un jeu de test), car on ne peut pas améliorer ce que l'on ne sait pas mesurer, et
2. Une parfaite traçabilité, car il faut pouvoir comparer les contextes (configuration, paramètres) des mesures pour identifier et restaurer les conditions optimales.

Dans le cas du développement logiciel traditionnel, l'objectif recherché est un taux d'erreur nul, éventuellement assorti d'une précision. Par exemple, le total d'une facture doit être exact avec une précision de deux décimales (au centime près) en toutes circonstances.

Une infrastructure DevOps a pour objectif de permettre le développement et l'intégration continues en automatisant le test, le versionnement, et le déploiement de façon à maintenir une progression itérative, rapide et de qualité constante, vers les objectifs mesurés. A cet effet, plusieurs métriques comme le degré d'avancement (burndown chart), le nombre de défauts et le temps moyen de résolution sont essentiels. Une telle infrastructure est basée sur le cloud, la modularité (dont APIs) et les outils suivants :

- La gestion d'environnement (conda, npm),
- Le contrôle de version (Git),

- L'automatisation des tests (unitaires, e2e),
- La containerisation sur le cloud (Docker),
- Le déploiement automatique (terraform, aws cdk).

Dans le contexte des projets d'intelligence artificielle, l'objectif est généralement de dépasser l'humain (human parity) dont le taux d'erreur se situe dans la plupart des domaines et selon les individus entre 5% et 15% (exact dans 85% à 95% des cas).

- A partir d'une matrice de confusion comparant les prédictions aux observations des données de test, l'exactitude (accuracy), la précision, le rappel (recall), et le score F1 permettent de mesurer la performance des algorithmes de **classification** en apprentissage machine.
- Un calcul de distance (Manhattan, Euclidienne, Minkowski) permet de mesurer la magnitude de l'erreur entre les prédictions et les observations et donc la performance des algorithmes de **régression** en apprentissage machine.
- Si la mesure de similarité cosinus est largement utilisée dans les projets de **traitement du langage naturel**, les différents cas d'utilisation des modèles de langage larges (LLMs) évoluent et nécessitent un consensus sur des me-

sures adaptées, comme le score BLEU pour les traductions, et les scores ROUGE pour les résumés.

- Si la partialité (bias) est un problème partagé par un grand nombre de modèles d'IA, les IA **génératives** ont introduit une nouvelle catégorie de dangers y compris leurs hallucinations. Il faut donc s'assurer de produire et de maintenir des modèles d'IA qui soient serviables, honnêtes et inoffensifs (Helpful, Honest, and Harmless).

Contrairement à un développement logiciel traditionnel fait de code, une solution d'intelligence artificielle comporte aussi des données d'entraînement, de test et de validation. En plus des objectifs d'une infrastructure DevOps, une infrastructure MLOps doit permettre d'optimiser la qualité et la performance des données dans toutes les phases des projets d'intelligence artificielle, notamment pour alerter des dérives du modèle et/ou des données (model/data drift) dans le temps.

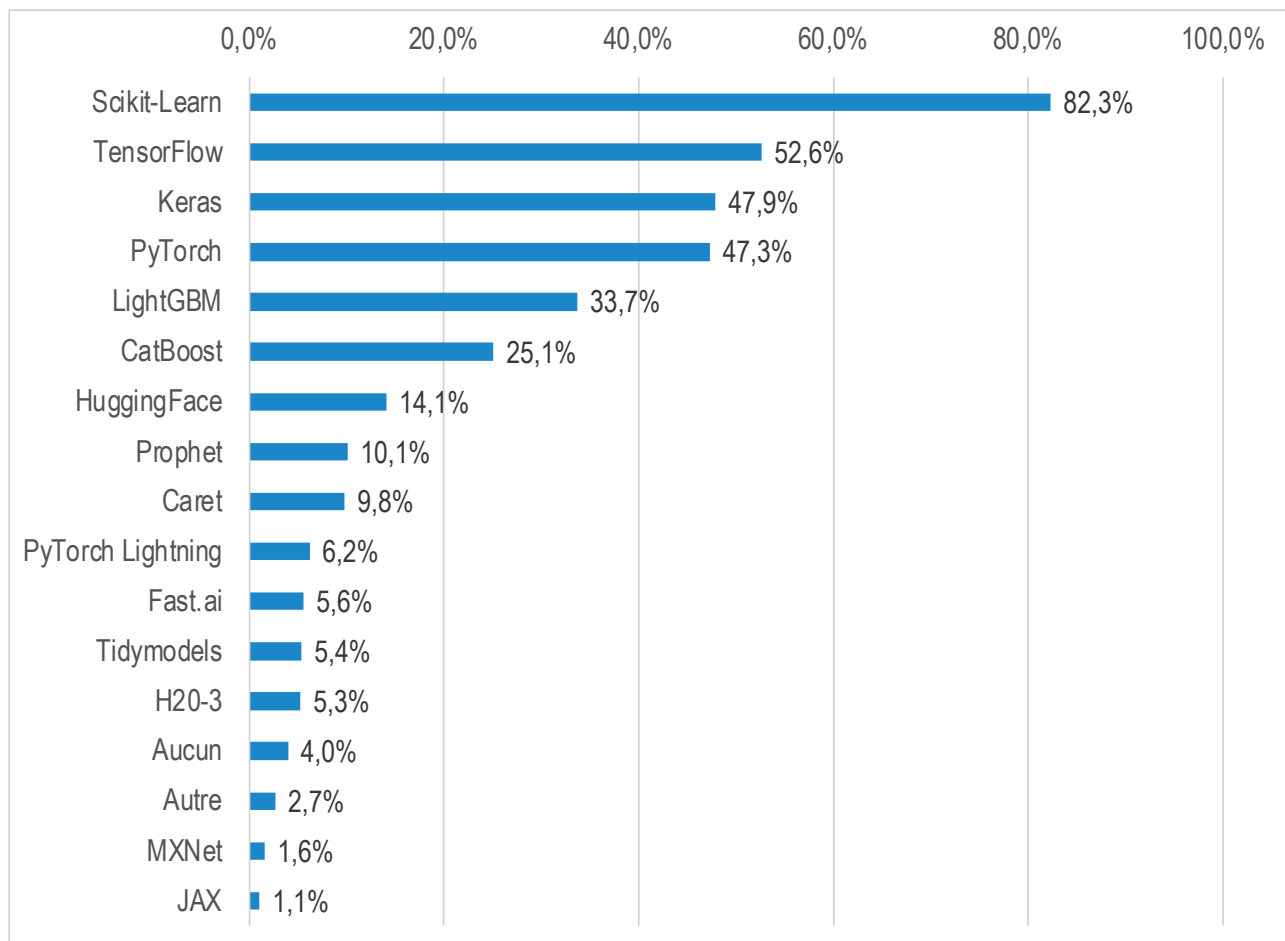


Fig: Usage des bibliothèques d'apprentissage machine par les utilisateurs de Kaggle

La transformation digitale par l'IA

Près de trois décennies de digitalisation et de dématérialisation des flux ont respectivement permis l'optimisation des processus, l'augmentation de la productivité, et la diminution des coûts par l'adoption des ERP (gestion intégrée), du CRM (relation clients) et du SRM (achats).

Ont suivi deux décennies de transformation digitale portées d'abord par le e-commerce sur Internet, puis par les technologies mobiles. Contrairement à la digitalisation motivée par l'optimisation et la réduction des coûts, la transformation digitale crée de la valeur en favorisant l'innovation, et le développement de nouvelles offres (produits, services) et de nouvelles interactions (réseaux sociaux, réalité augmentée).

Nous pensons que la troisième vague de transformation digitale commence et qu'elle sera portée par l'intelligence artificielle, dont les progrès ont récemment été accélérés par l'atteinte d'un seuil critique dans l'accès aux puissances de calcul nécessaires (GPUs).

Une transformation digitale effective repose sur les 3*C : culture, cloud et changement :

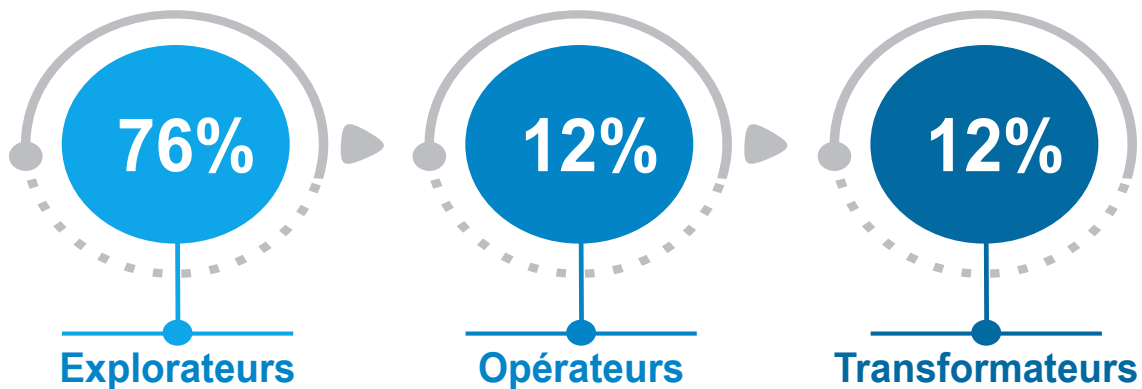
1. Une culture d'innovation au service du client : Les équipes internes sont les acteurs de la transformation digitale. La propagation d'une vision client et d'une culture

d'innovation, fondée sur l'expérimentation et l'empathie, et pilotée par les données en toute transparence, dirige la créativité pour la création de valeur.

2. Une infrastructure DevOps/MLOps afin de partager une vue à 360 degrés sur le cloud : Les îlots d'information, la multiplication des pipelines, et les traitements ad hoc sont un obstacle à la transformation digitale. Dans un monde digital, les données sont au cœur du pilotage car on ne peut pas améliorer ce que l'on ne sait pas mesurer. Le cloud et les technologies DevOps/MLOps permettent le partage d'une vue à 360 degrés et l'expérimentation agile.

3. Les méthodes agiles pour la conduite du changement : Les méthodes agiles (design thinking, lean thinking, customer journey mapping, agile development, etc.) permettent d'expérimenter, de pivoter ou de persévérer, pour valider progressivement les hypothèses de la transformation digitale dans un environnement incertain en constante mutation.

Conclusion : le chemin de la maturité en IA

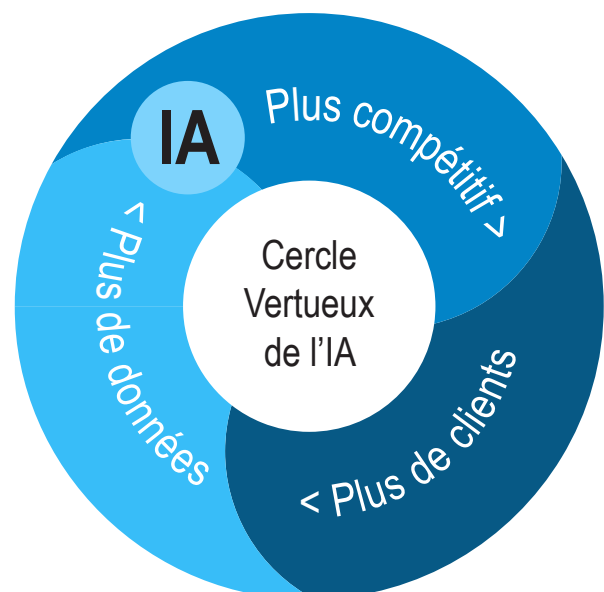


Certains modèles de maturité ont 5 niveaux et plus, mais nous aimons la simplicité.

Les **explorateurs** ont développé un intérêt pour l'intelligence artificielle qui les motive à expérimenter avec de petits projets ciblés (preuves de concept) utilisant des modèles d'intelligence artificielle développés par des tiers pour résoudre des problèmes ponctuels souvent de manière ad hoc (pas de processus qualité).

Les **opérateurs** ont formé des équipes et déployé une infrastructure Cloud et des méthodes MLOps pour développer, déployer et maintenir des modèles d'intelligence artificielle selon les règles de l'art. Ils analysent les métiers et les tâches qui les composent pour intégrer l'intelligence artificielle de manière systématique, améliorent la qualité de leurs données, et forment leurs équipes à collaborer avec l'IA afin de réaliser des gains de productivité et des réductions de coûts.

Les **transformateurs** ont développé une culture data + IA qui leur a permis de capitaliser sur les bénéfices immédiats de l'intelligence artificielle. Ils intègrent l'intelligence artificielle dans leur stratégie et dans leur gouvernance afin de se transformer pour innover, créer de la valeur, gagner d'autres avantages compétitifs, comme la supériorité des produits ou l'excellence opérationnelle, et bénéficier du cercle vertueux de l'IA.



Digillia vous souhaite bonne route sur le chemin de la maturité en IA.



Digillia SAS

Bureau 326
59 rue de Ponthieu
75008 Paris
France

 www.digillia.com
 contact@digillia.com