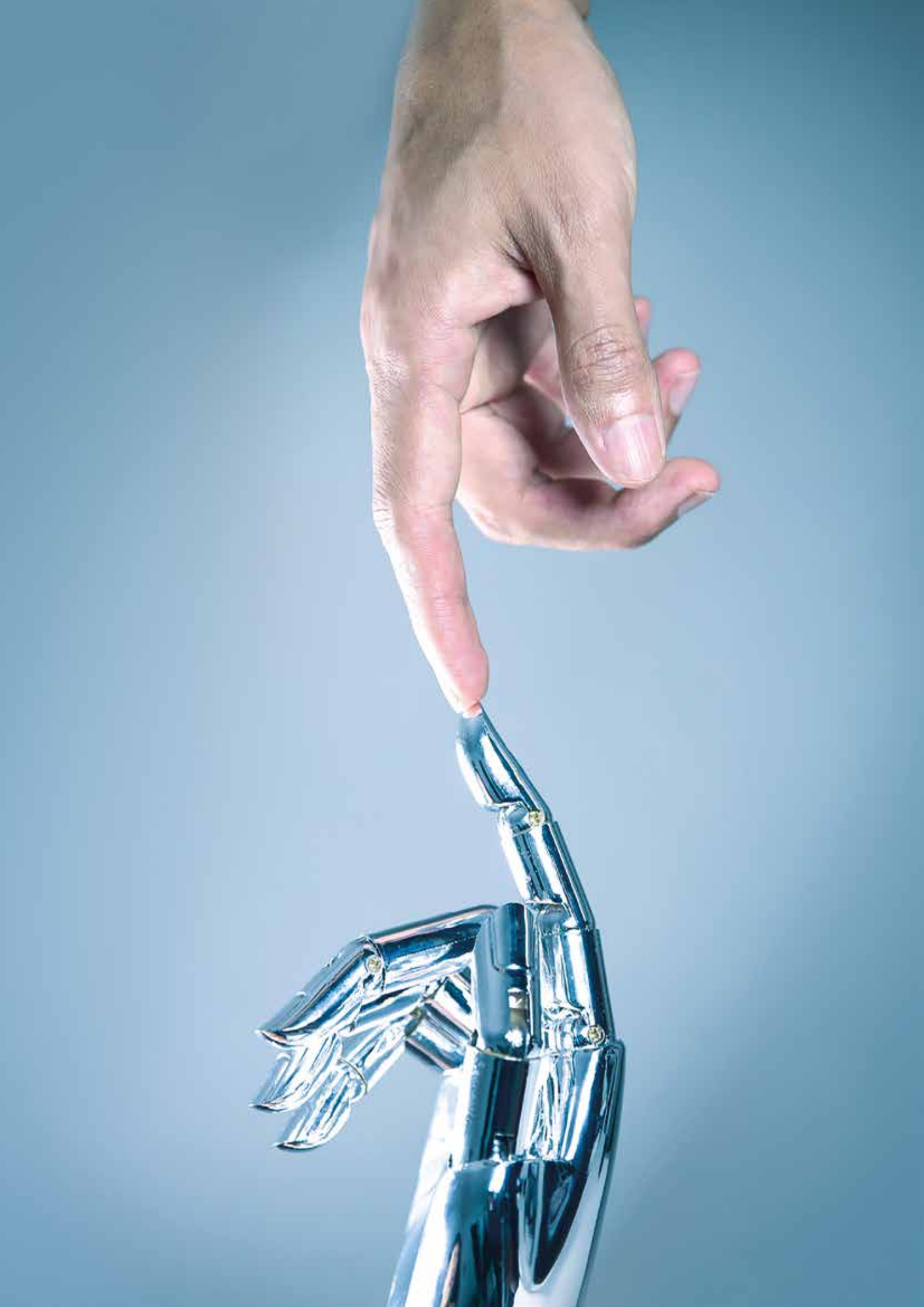
KPMG

AI in Control

Maîtriser les risques liés à l'intelligence artificielle

kpmg.fr



« Nous sommes à la veille d'une révolution technologique qui modifiera fondamentalement notre façon de vivre, de travailler et d'entretenir des relations les uns avec les autres. La transformation sera différente de tout ce que l'humanité a connu auparavant en matière d'ampleur, de portée et de complexité. »

Klaus Schwab
Fondateur et Président exécutif du Forum économique mondial Genève

Les nouveaux risques liés à l'intelligence artificielle (IA) exigent des approches nouvelles et intégrées pour être maîtrisés.
Notre publication a pour objectif de vous aider à comprendre les risques liés à l'IA et à les maîtriser.
Elle met l'accent sur les principaux risques liés à l'intelligence artificielle sans pour autant chercher à fournir une solution à l'ensemble des problématiques liées à cette technologie.
L'approche AI in control, développée par KPMG, constitue un cadre sur-mesure pour maîtriser les risques et les contrôles.
Cette approche par les risques vous donnera les clés pour construire une IA fiable, et ainsi renforcer la confiance de vos clients et de vos partenaires.

1

La révolution de l'intelligence artificielle

Qu'est-ce que l'Intelligence Artificielle ?

L'Intelligence Artificielle est un ensemble de techniques et de méthodes qui visent à simuler l'intelligence.

Les concepts d'IA visent à intégrer les aspects suivants :

CAPACITÉ
à analyser des grands volumes d'informations complexes

CAPACITÉ
à apprendre

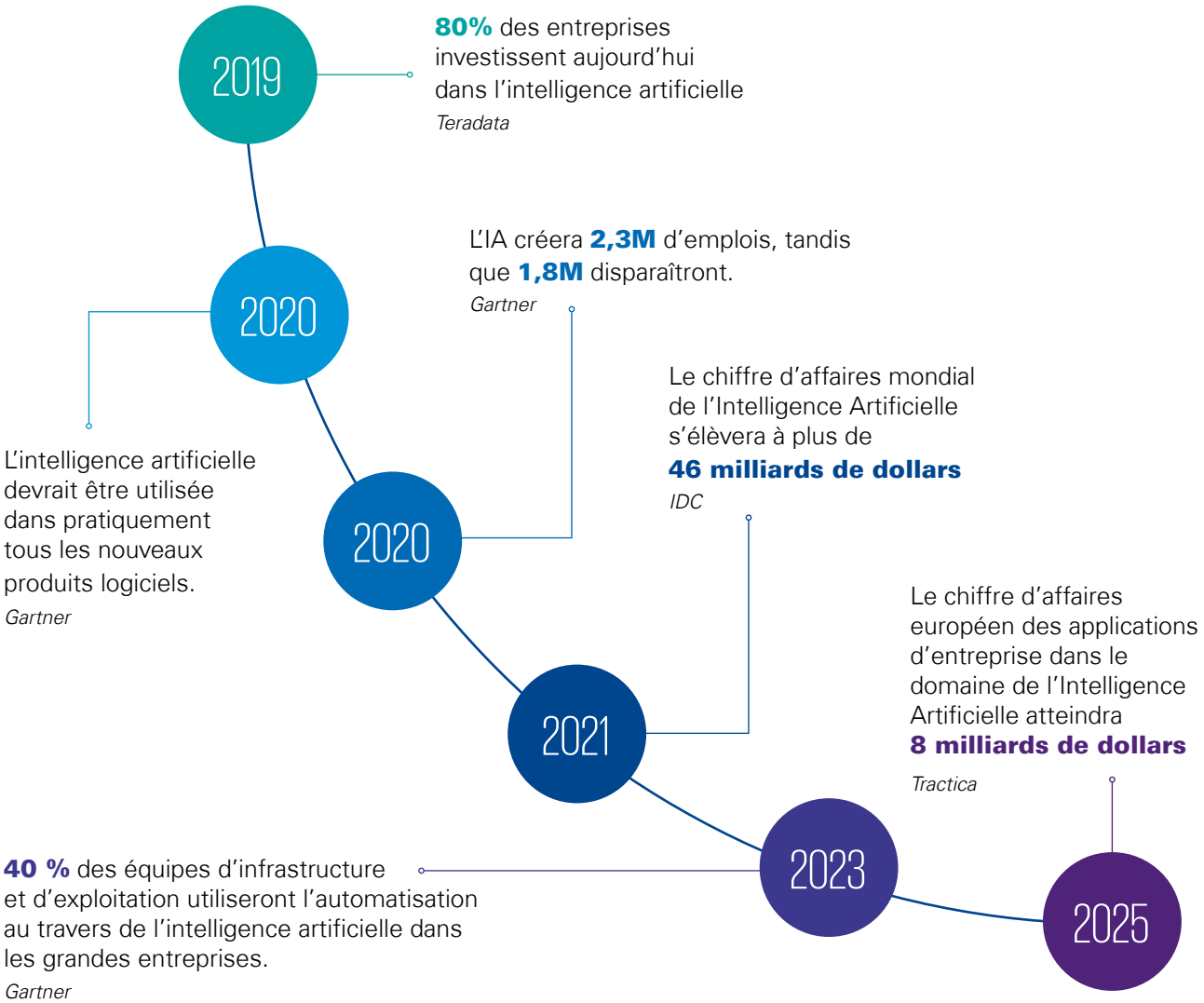
CAPACITÉ
à conclure

CAPACITÉ
à appréhender des données structurées ou non structurées (mot, image, son)

CAPACITÉ
à décider

Le début d'une nouvelle ère

Nous sommes à la veille d'un tournant technologique. Et, comme c'est le cas pour tout changement, les opportunités et les risques font l'objet de vifs débats. C'est ainsi que les choses doivent se passer. Un regard rétrospectif sur l'histoire montre que l'humanité s'est souvent trouvée au bord d'un tel tournant.
De l'invention de l'écriture au mouvement de protestation « Swing Riots » dans les années 1880, en passant par la montée de la mobilité pour tous, la technologie Internet et les derniers développements de l'Intelligence Artificielle, toutes les révolutions industrielles semblent suivre la même structure dramatique : il y a toujours une grande incertitude sur les impacts sur notre société.



L'Intelligence Artificielle, utilisée ici comme terme générique, a le potentiel de devenir l'innovation technologique la plus importante des prochaines décennies. Et les préoccupations la concernant ne sont pas nouvelles. Mais aujourd'hui, elles sont renforcées par une augmentation exponentielle des capacités de l'Intelligence Artificielle ainsi que par une adoption par tous les secteurs d'activité (Santé, Industrie, Automobile, Télécommunications, etc.), par tous les métiers (finance, marketing, R&D, etc.) et d'une interface quasi systématique avec les Hommes dans leur vie de tous les jours.

PAR EXEMPLE

Les entreprises de tous les secteurs investissent massivement dans les technologies d'IA pour proposer des services avancés et dynamiser leurs activités. Selon une étude KPMG, les dépenses globales devraient ainsi atteindre 232 milliards de dollars d'ici à 2025, contre environ 12,4 milliards de dollars aujourd'hui (Source : KPMG LLP, 2018).
On s'attend à ce que le niveau d'investissement augmente de plus en plus au cours des prochaines années, avec un potentiel énorme pour la création d'emplois, le revenu des entreprises et la croissance économique.

Des domaines d'application déjà variés

L'intelligence artificielle vise à imiter l'intelligence humaine. Même si c'est encore un voeu pieux à l'heure actuelle, l'IA dépasse déjà les capacités humaines dans certains domaines. Par définition, les aspects suivants sont adaptés à une imitation de l'intelligence humaine : perception de l'environnement, action ciblée et raisonnée, et apprentissage fondé sur l'information sous-jacente.
La combinaison de ces aspects conduit à un nombre pratiquement infini d'applications pour l'intelligence artificielle, interface utilisée pour chercher de la croissance, améliorer la performance et mieux gérer les risques.

Développement & innovation

- Analyse de structures moléculaires
- Brassage de bières adaptées aux goûts d'un individu
- Conception de modèles économiques liés aux matières premières

Achats

- Classification des données dans l'approvisionnement stratégique
- Support contractuel
- Chatbot d'achat

Production

- Bras robot autoapprenant
- Détection de défauts par ultrasons
- Exosquelette aidant les travailleurs pour le transport de charges lourdes

Distribution

- Choix de pneus adaptés
- Enregistrement et transcription des conversations en temps réel
- Chatbot d'assistance aux agents

Management

- Evaluation du potentiel des opportunités commerciales
- Automatisation de la gestion du marketing pour un site de vente
- Une IA en tant que Directeur Artistique

Services financiers

- Automatisation de la facturation
- Analyse en temps réel des marchés financiers
- Optimisation du processus de réception des factures lourdes

Supply Chain

- Logiciel auto-apprenant pour la logistique
- IA de gestion d'entrepôts
- Optimisation de la Supply Chain

Ressources humaines

- Assistance à la selection des candidats
- Création de documents de formation
- Chatbots RH

Organisation/ administration

- Visualisation des contenus de contrats
- Ordonnancement
- "Office in the car"

Service à la clientèle

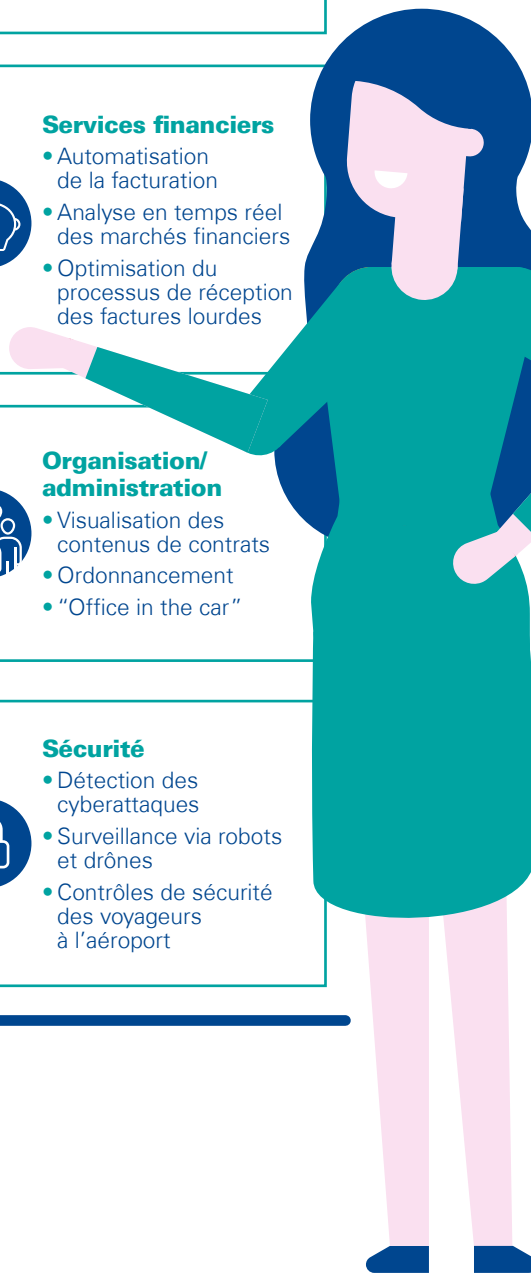
- Assistance à la réservation
- Réponses aux questions fréquemment posées
- Guidage des clients dans les magasins

Marketing

- Optimisation de l'utilisation des panneaux d'affichage numériques
- Incitation à l'achat
- Création de contenus textuels de haute qualité

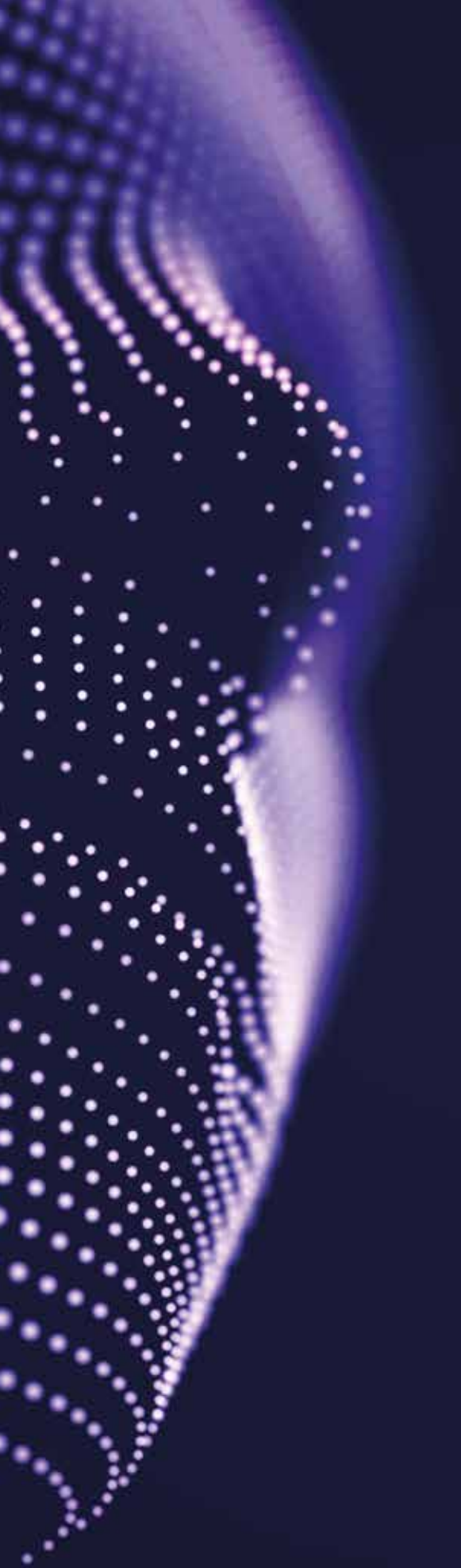
Sécurité

- Détection des cyberattaques
- Surveillance via robots et drônes
- Contrôles de sécurité des voyageurs à l'aéroport



2

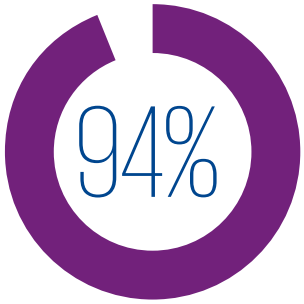
Nouvelles technologies : nouveaux risques



Nous croyons que l'organisation de demain ne sera pas en mesure de maîtriser ses risques sans contrôler l'IA. L'intelligence artificielle occupera ainsi une place prépondérante dans les processus d'affaires et sera donc étroitement liée aux risques de l'organisation. Ces risques seront changeants, nouveaux, complexes et à multiples facettes, et pourront avoir de fortes répercussions financières, réglementaires, opérationnelles, ou sur la réputation de l'organisation.

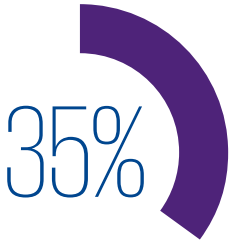
Dans le cadre de notre quatrième édition annuelle du Global CEO Outlook, nous avons interrogé 1300 dirigeants de grandes entreprises du monde entier afin de connaître leur point de vue sur les principales opportunités et les défis auxquels leur entreprise est confrontée.

Leurs réponses, combinées à d'autres enquêtes (réalisées par des experts d'IBM, IDC, MIT et KPMG), ont mis en évidence l'accélération de l'IA et les opportunités formidables qu'elle offre en tant qu'avantage concurrentiel, mais également en tant que véritable défi mêlant des enjeux liés à la règlementation, la confiance et la réputation.



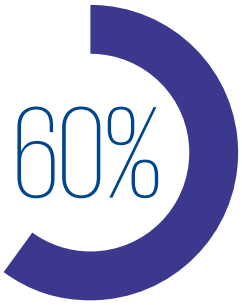
des entreprises considèrent que **l'IA est une clé** pour leur avantage concurentiel.

- IDC -



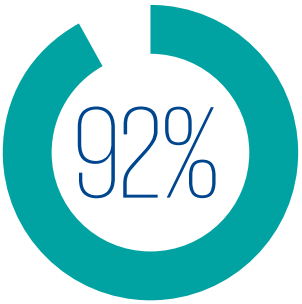
seulement ont un haut niveau de **confiance** dans leur solution d'analyse de données

- KPMG's recent Guardians of Trust report -



considèrent les **contraintes règlementaires** comme un obstacle à la mise en œuvre de l'IA

- IBM IBV AI 2018 -



s'interrogent sur la **fiabilité** des données, des analyses... et s'inquiètent de l'impact sur la **réputation.**

- KPMG's recent Guardians of Trust report -

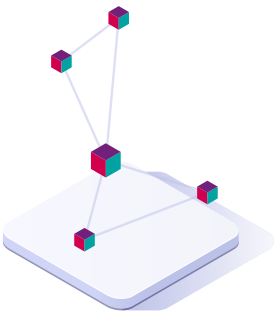
1 entreprise sur 20 **a intégré l'IA** dans ses offres ou processus.

- MIT Sloan Management Review -

> "Les chefs d'entreprise doivent outiller leurs équipes pour une nouvelle ère de l'intelligence artificielle et de l'automatisation croissante."

Duncan Tait SEVP, Head of Americas and EMEIA Fujitsu

- KPMG's 2018 Global CEO Outlook -



Ces enquêtes confirment que le développement d'une solution d'intelligence artificielle s'accompagne d'un niveau de risque accru. Bien que les référentiels traditionnels de risque et de contrôle ainsi que les modèles de processus informatiques puissent toujours être utiles, nous avons identifié les 7 catégories suivantes de risques critiques qui pourraient avoir un impact significatif sur la fiabilité de la solution d'IA :

Risques liés à la stratégie et à la gouvernance

Étant donné l'ampleur des changements que l'IA apportera, il existe des risques pour les organisations qui ne seront pas en mesure de s'adapter au changement. Les programmes d'IA doivent donc être alignés sur la stratégie de l'organisation et l'appuyer en prenant en compte son appétence au risque.
Une vision collective forte, initiée au plus haut niveau de l'organisation, peut contribuer à la gestion de ces risques stratégiques, si elle est correctement partagée par les différentes instances de gouvernance concernées par l'IA.

Risques de biais

Le risque de biais fait référence à une erreur systématique ou à un écart par rapport à la vérité ou à l'éthique en raison d'une approche ou d'un processus qui entraîne des erreurs dans les résultats. Dans certains cas, les algorithmes peuvent avoir des biais intégrés en raison des préférences conscientes ou inconscientes du développeur et dans d'autres cas, les préjugés dans le monde réel peuvent s'infiltrer dans les systèmes d'IA grâce aux données utilisées dans le processus d'apprentissage automatique.

PAR EXEMPLE

En 2014, l'une des plus grandes entreprises mondiales a mis au point un programme informatique permettant de passer en revue les CV des candidats afin d'automatiser la recherche des meilleurs talents. Cependant, dès l'année suivante, l'entreprise a compris que son nouveau système était préjudiciable aux femmes. Les ingénieurs ont découvert que l'IA était défavorable aux candidates car le processus d'apprentissage avait été mené en utilisant des CV provenant majoritairement de profils masculins.

Risques éthiques

Pour mettre en œuvre de nouvelles technologies dans les processus interagissant avec des tiers externes ou internes, les organisations devront démontrer que les systèmes sont fiables et éthiques. La confiance et l'éthique sont des facteurs clés pour que les organisations atteignent leurs objectifs stratégiques car elles sont des conditions nécessaires à la réputation, à la satisfaction de la clientèle et à la fidélité des employés. Dans ce contexte, il convient d'aligner tous les nouveaux développements technologiques sur les lois, règlements, valeurs, politiques et procédures des organisations. Elles devront également rendre compte aux tiers et ce, de manière transparente, des processus numériques et des résultats connexes. Cette bonne pratique est désormais plus que nécessaire pour toutes les organisations.

Par conséquent, de la conception à l'élaboration, en passant par la mise à l'essai, la mise en oeuvre et l'exploitation de tout système d'IA, l'éthique doit être considérée comme un domaine d'intérêt majeur pour assurer que les données utilisées, le traitement et les résultats sont conformes aux règles et aux valeurs.

PAR EXEMPLE

COMPAS* est un logiciel s'appuyant sur des algorithmes permettant de calculer un indicateur de risque potentiel de récidive pour les accusés aux Etats-Unis. Ce score, dont l'utilisation pour la prise de décision légale a été autorisée en Juillet 2016, a toutefois tendance à estimer que le risque de récidive d'un homme de couleur est plus fort que celui d'un homme blanc, posant une question éthique qui est celle du biais raciste mais également un risque de stigmatisation : certaines études montrent que seulement 20% des personnes à risque récidivent effectivement.

* : Correctional Offender Management Profiling for Alternative Sanctions

Risques cyber

Les risques cyber peuvent être présents tout au long du cycle de vie de la construction et de l'exploitation de l'IA.
Les algorithmes d'IA s'appuient sur des systèmes sous-jacents tels que les ordinateurs, les serveurs, les appareils mobiles, les réseaux, les capteurs et le code logiciel. Ces infrastructures collectent et stockent de grandes quantités de données, hébergent et exécutent des algorithmes d'IA. Les données collectées et utilisées doivent être protégées de toute altération, de leur point de collecte à leur traitement et leur stockage. Les violations, les modifications de code ou de données pourraient en effet avoir des répercussions catastrophiques sur l'organisation.

Risques opérationnels

Les solutions d'Intelligence Artificielle s'appuient sur des systèmes d'information et des infrastructures sous-jacentes. Par conséquent, comme tous les systèmes informatiques, et afin d'assurer une maîtrise efficace de l'environnement informatique, les solutions d'IA sont également exposées aux risques habituels. En effet, plusieurs domaines de contrôle doivent être abordés, en raison de leur impact direct sur la performance des solutions IA : la stratégie et la gouvernance, la sécurité et l'infrastructure, la conformité, la gestion du changement et les processus informatiques.

Risques d'explicabilité

Le risque d'explicabilité fait référence à la capacité à expliquer comment une IA arrive à un résultat, que ce résultat soit valide ou non. Si la logique de la solution d'IA n'est pas bien comprise, elle pourrait nuire à la capacité de répondre aux questions légitimes des clients et des partenaires, ce qui aurait des répercussions sur les activités commerciales et entraînerait une perte financière ou une atteinte à la réputation.

PAR EXEMPLE

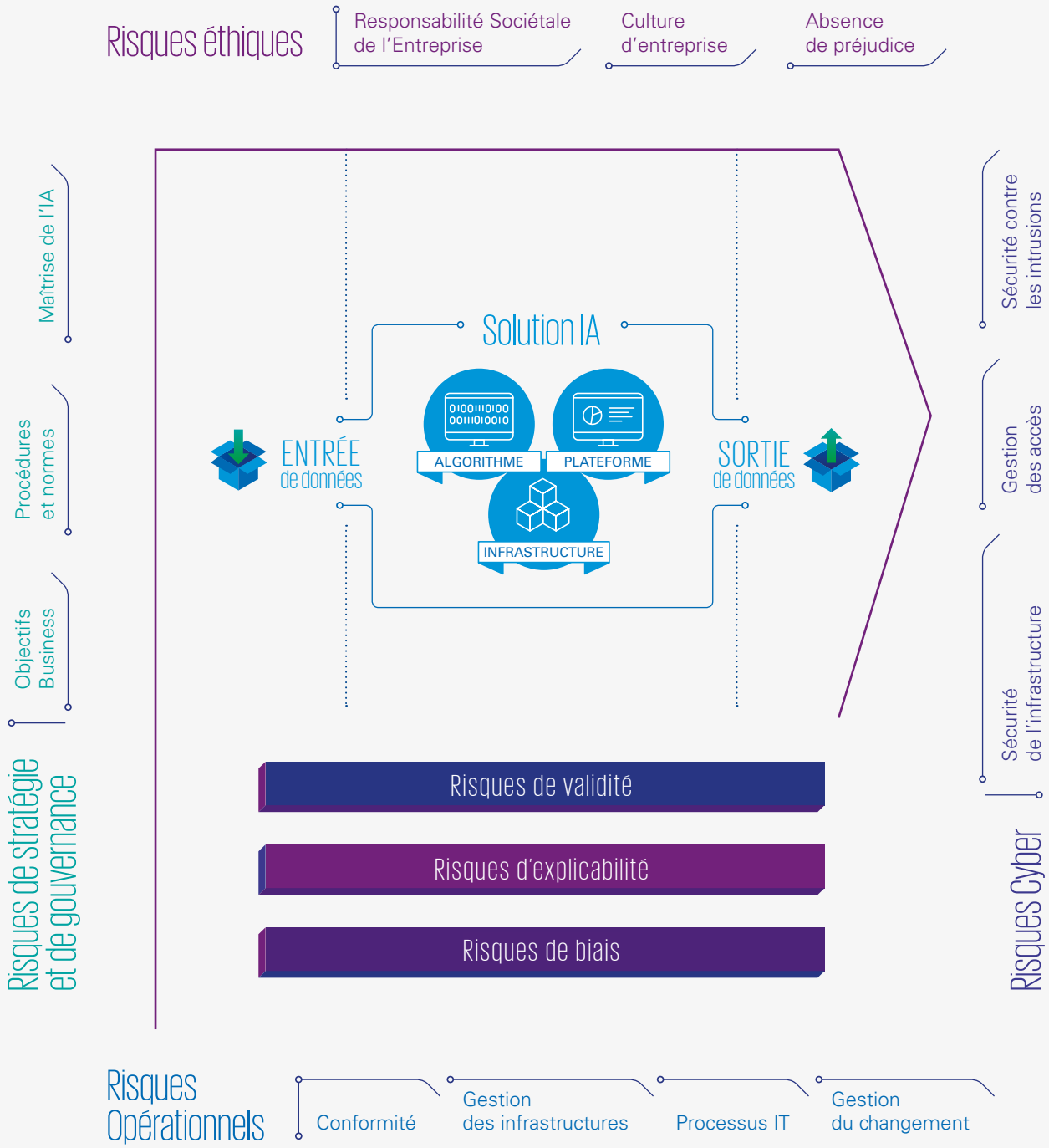
Dans le cas d'un traitement automatisé, une personne dispose d'un droit d'accès aux informations utiles concernant la logique sous-jacente, ainsi qu'à l'importance et aux conséquences prévues de ce traitement pour elle.

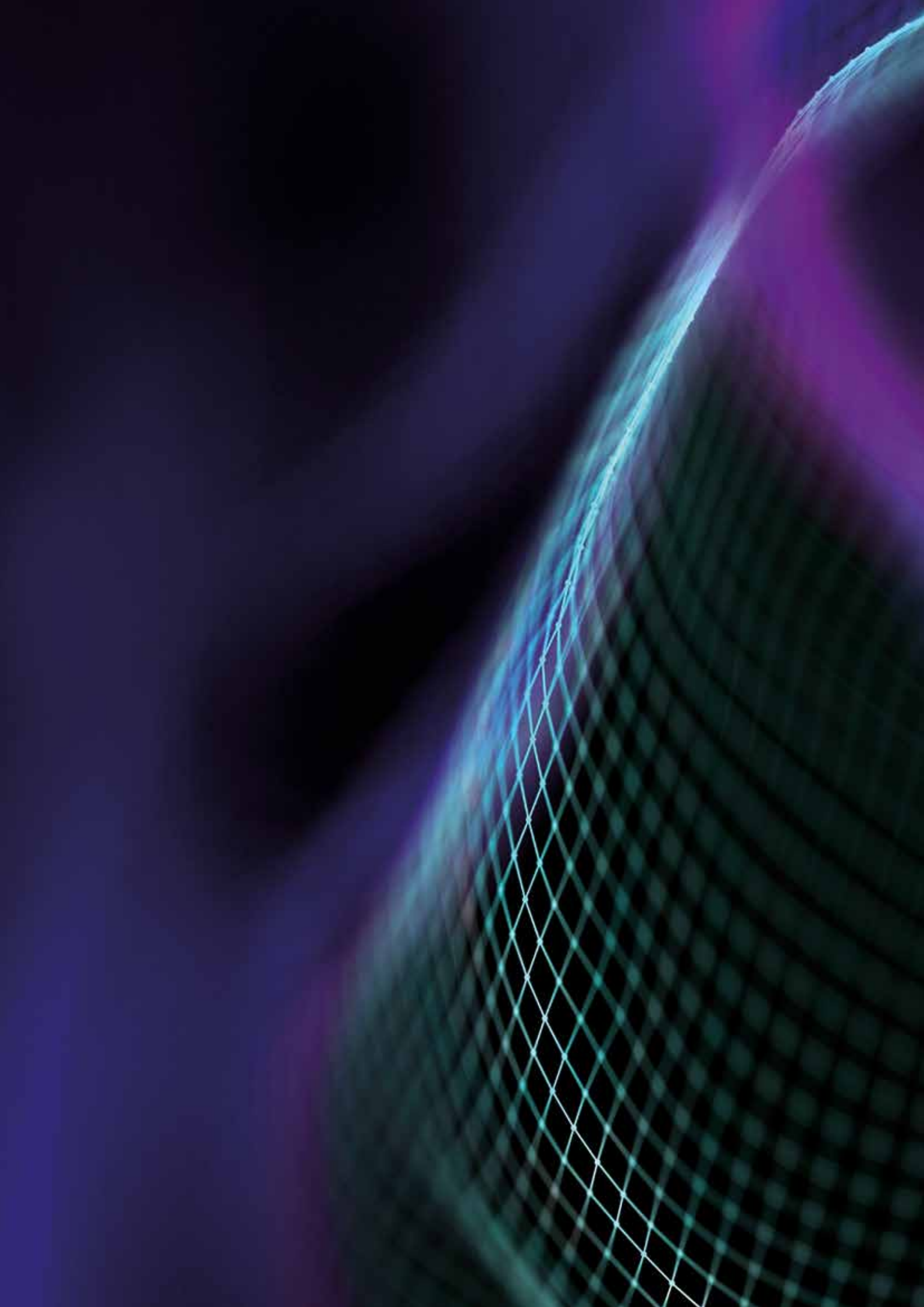
Risques de validité

Le risque de validité fait référence à un résultat inexact ne répondant pas aux attentes définies de la solution. La couverture des risques de validité permettra de s'assurer que le processus de construction de l'Intelligence Artificielle (périmètre de données, Algorithme, représentation des résultats, etc.) n'engendre pas de faux résultats.
Aussi, l'intelligence artificielle analyse des données provenant de sources diverses tels que des fichiers, des capteurs et des caméras. La modification de ces données par les hackers peut amener l'IA à les interpréter de manière erronée dans ce qu'on appelle des attaques dites « adversarial ».

PAR EXEMPLE

Des chercheurs ont montré qu'ils pouvaient tromper une voiture autonome en apposant simplement un autocollant sur un panneau de signalisation, conduisant la voiture à confondre un panneau d'arrêt avec un panneau de limitation de vitesse. D'autres chercheurs ont montré qu'ils étaient capables de faire en sorte qu'une IA confonde un panda et un singe gibbon, en modifiant légèrement l'image de manière imperceptible à l'œil humain. Ce même type de manipulation des données d'entrée peut aller plus loin en menant des attaques par injection de code causant des problèmes de sécurité sur le code de l'IA.

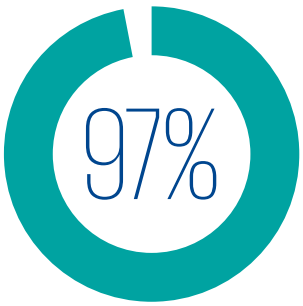

Risques éthiques
Responsabilité Sociétale de l'Entreprise
Culture d'entreprise
Absence de préjudice
Maîtrise de l'IA
Procédures et normes
Objectifs Business
Risques de stratégie et de gouvernance
Solution IA
ENTRÉE de données
ALGORITHME
PLATEFORME
INFRASTRUCTURE
SORTIE de données
Risques de validité
Risques d'explicabilité
Risques de biais
Sécurité contre les intrusions
Gestion des accès
Sécurité de l'infrastructure
Risques Cyber
Risques Opérationnels
Conformité
Gestion des infrastructures
Processus IT
Gestion du changement



3

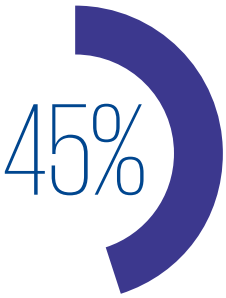
Nouveaux risques : nouvelles approches

Les nouveaux risques introduits par l'IA impliqueront de fait de nouvelles approches. Ces approches devront couvrir l'ensemble des risques existants dans le cas où les entreprises souhaitent surmonter le risque et tirer pleinement avantage de l'IA. Une enquête menée par KPMG auprès de 170 professionnels de la gestion du risque technologique a en effet souligné un manque de confiance envers l'Intelligence Artificielle. Cela révèle un impératif : établir un véritable cadre de confiance autour de cette technologie, bien que la démarche d'audit ne soit pas encore précisément définie pour 70% des professionnels interrogés.

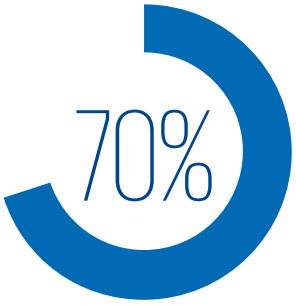


Pensent que l'IA est déjà utilisée ou est en passe de l'être

Manque de confiance dans la gouvernance actuelle de l'IA au sein de leur organisation



Ont prévu d'effectuer un audit de leurs solutions d'intelligence artificielle



Ne savent pas précisément quelle sera leur approche en matière d'audit de l'IA.

KPMG a développé une approche en deux volets offrant une méthodologie de bout en bout. Notre approche combine une analyse de l'environnement de contrôle basée sur les risques et une revue de l'algorithme visant à vérifier que les résultats de la solution d'IA sont impartiaux, valides et explicables.
Cette approche peut permettre aux entreprises d'évaluer et maîtriser les risques liés à l'IA. L'analyse de l'environnement de contrôle basée sur les risques et la revue de l'algorithme sont complémentaires et assurent le bon fonctionnement actuel et futur de la solution d'IA.

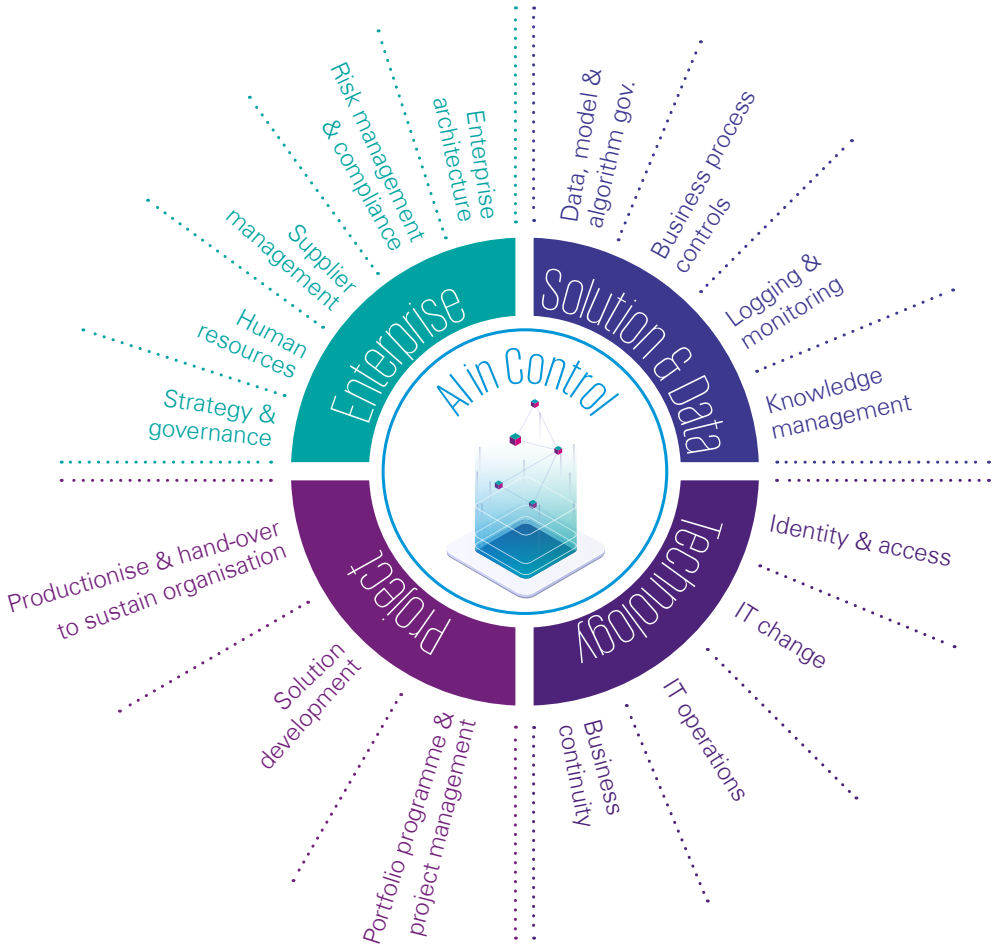
IA in control

Le cadre de risques et de contrôles que nous avons défini est conçu pour accompagner les professionnels dans la gestion de l'IA et à aider les entreprises au fil des différentes étapes de maturité des solutions d'IA, de la conception à la mise en œuvre, l'évaluation et la maintenance.

Ce cadre couvre 16 catégories de risques et de contrôles des solutions et des projets d'IA. Nous avons identifié 75 risques potentiels parmi 16 domaines différents et nous avons défini 106 contrôles types qui permettront de maîtriser ces risques.

Nous les avons également alignés aux 37 processus COBIT5.1 afin de respecter ce cadre de gouvernance et de contrôle couramment accepté comme cadre de référence.

Le référentiel de risques et de contrôles s'applique à différentes parties de l'écosystème d'une solution d'Intelligence Artificielle, telles que la stratégie, la gestion des risques et la conformité, le développement de solutions, la gouvernance des données et des modèles, l'enregistrement et la surveillance, ainsi que la gestion des connaissances. Notre approche peut être descendante ou ascendante en fonction des besoins de l'organisation.



Revue de l'algorithme

Outre le référentiel de risques et de contrôle, KPMG a mis en place une méthodologie de revue de solutions d'IA, afin d'en évaluer la fiabilité. Cette approche se décline en quatre points qui aident à instaurer la confiance dans leur utilisation. Ces contrôles sont effectués par des experts, Ingénieurs et Docteurs en Data Science.

01. Revue du code

La revue du code permet de s'assurer de sa cohérence avec les spécifications techniques et fonctionnelles de la solution déployée. La gestion des exceptions, les unit-tests, le versioning et la documentation font également partie de la revue technique : ces éléments limitent les risques de mauvaise utilisation ou de production de résultats erronés, et aident à garantir un bon niveau de maintenance.

02. Données d'apprentissage, tests et validation

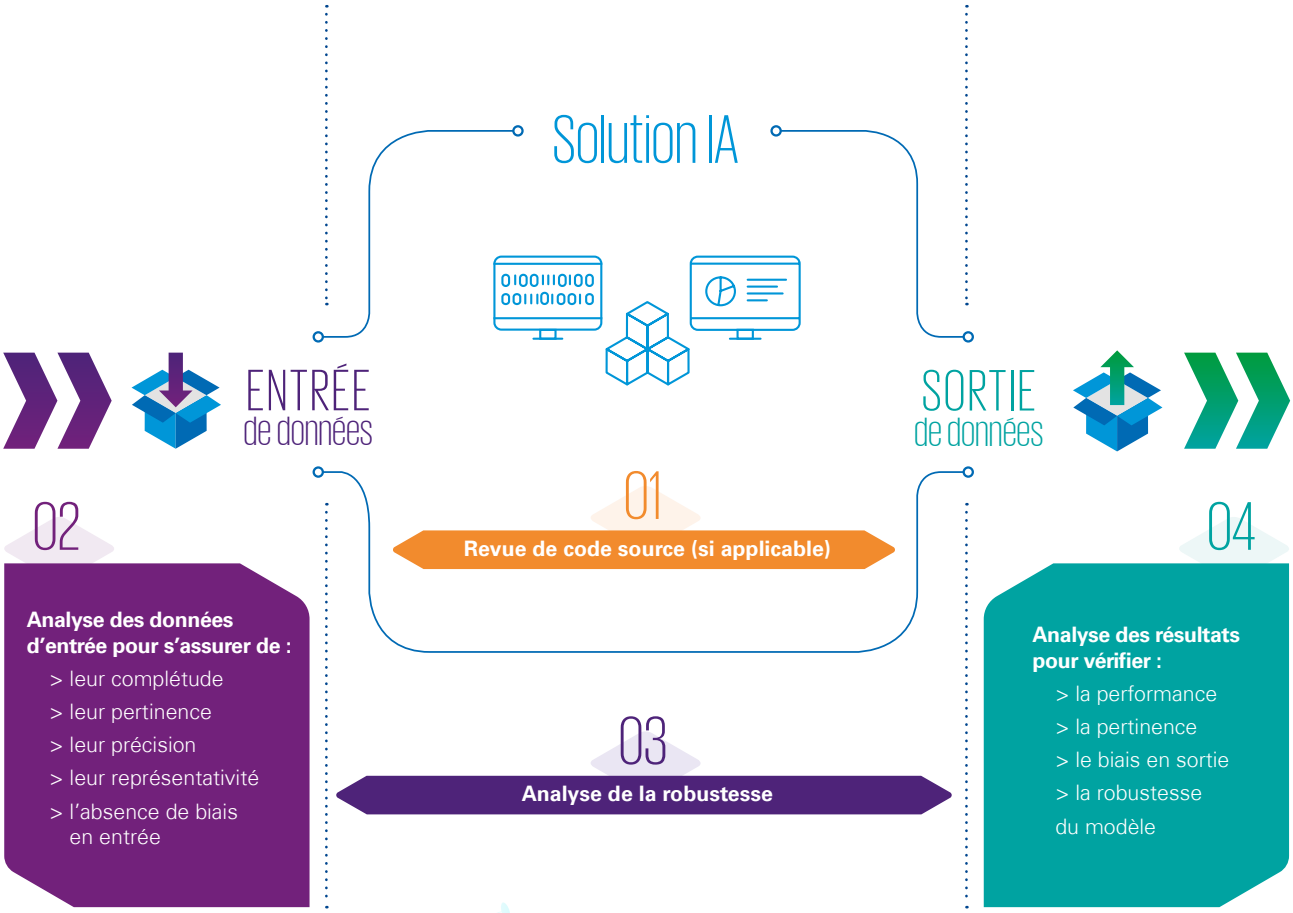
Un modèle est un algorithme ayant été entrainé à effectuer une tâche particulière. Le but de cet apprentissage est de produire une solution capable d'effectuer des prédictions (voire de prendre des décisions) sur la base d'informations entrantes. Les phases d'apprentissage, de test et de validation sont, par conséquent, des étapes essentielles à la construction d'une solution d'IA. Il est essentiel de s'assurer de la pertinence et de la représentativité des données utilisées lors de la phase d'apprentissage, et de vérifier que les mesures de performance du modèle sont effectuées selon des métriques appropriées, et sur des données indépendantes. Ces vérifications sont des procédures indispensables à l'assurance d'une solution pertinente et fiable.

03. Robustesse

Tout au long de son cycle de vie, un modèle va évoluer et être exposé à des données aberrantes, susceptibles de perturber son fonctionnement et de conduire à des résultats inattendus. Les tests continus de performance, de robustesse et de sensibilité aux perturbations permettent de limiter les risques de déviation, et de réduire le risque de production de résultats erronés. Ces tests aident à identifier des points de faiblesse et permettent d'apporter des mesures correctives efficaces.

04. Modèle explicable et résultats interprétables

Au regard du RGPD, la logique sous-jacente à un algorithme doit pouvoir être expliquée, tout comme les résultats produits et leurs conséquences (article 13.2.f). Au-delà de ces importants aspects réglementaires, il est aussi essentiel de pouvoir développer et déployer des solutions en toute confiance et de pouvoir en expliquer les résultats, en particulier lorsque ceux-ci semblent contre-intuitifs. Utiliser des algorithmes maitrisés et assurer une traçabilité documentée des développements et tests, tout au long du cycle de vie d'une solution d'IA, permettent de réduire les risques réglementaires et d'évoluer dans ces nouveaux environnements techniques en toute confiance.


Solution IA
ENTRÉE de données
SORTIE de données
01
Revue de code source (si applicable)
02
Analyse des données d'entrée pour s'assurer de :
> leur complétude
> leur pertinence
> leur précision
> leur représentativité
> l'absence de biais en entrée
03
Analyse de la robustesse
04
Analyse des résultats pour vérifier :
> la performance
> la pertinence
> le biais en sortie
> la robustesse du modèle

KPMG, leader reconnu en Innovation

Bien que l'IA puisse améliorer grandement l'efficacité des opérations et les résultats ainsi que stimuler la croissance de l'entreprise, les organisations doivent régulièrement revoir le profil des risques émergents liés à l'IA et identifier les tendances tout en restant à la pointe des performances.

Depuis plus de 100 ans, des entreprises du monde entier nous font confiance. Nous avons bâti notre réputation sur la compréhension des facteurs qui régissent votre entreprise :

Du conseil d'administration à l'ensemble de votre entreprise, telles que le service de finance, l'audit IT et le contrôle interne, nos équipes de conseil en gestion du risque ont de l'expérience dans la gestion des risques divers et émergents.

KPMG est un pionnier des solutions d'Intelligence Artificielle et possède un portefeuille de connaissance à ce sujet qui aide à améliorer et à accélérer les décisions favorisant la croissance et la rentabilité.

KPMG peut tirer parti de son expérience en matière d'Intelligence Artificielle et de risk consulting pour aider les organisations à intégrer les considérations de gouvernance, de risque et de conformité dans leur programme d'Intelligence Artificielle.

Les initiatives KPMG relatives à l'IA incluent notamment Ignite, KPMG Lighthouse et KPMG Insights Centers.

Ignite

KPMG Ignite est une plateforme regroupant tout le savoir faire de KPMG en matière de NLP (Natural Language Processing). Nos experts travaillent sur des technologies open source et développent des solutions d'IA spécialisées dans l'analyse de texte.

KPMG Lighthouse

Centre d'excellence Data Driven Tech : ce centre permet d'offrir des capacités d'analyse de façon transparente entre les régions et les entreprises membres du réseau KPMG afin d'offrir les meilleurs services et talents à nos clients. Aujourd'hui, le Lighthouse regroupe plus de 2000 experts à l'international et plus de 160 en France. Plus de 150 solutions d'IA ont été développées pour les besoins de nos clients.

KPMG Insights Centers

Ces environnements de travail collaboratifs de nouvelle génération permettent à nos collaborateurs d'aider les clients à interagir avec leurs données comme ils ne l'avaient jamais imaginé, en anticipant et en planifiant les perturbations. En explorant de nouvelles possibilités et solutions pour faire face aux risques critiques, aux défis de performance et de croissance, les Insights Centers à travers le monde aident à promouvoir des solutions nouvelles et innovantes aux défis commerciaux.

Nos expériences

Voici quelques exemples de l'utilisation par KPMG du cadre IA In Control pour aider les entreprises à gérer les risques liés à l'IA :

Leader des biens de consommation (France)

Une grande entreprise française du secteur des biens de consommation a développé un algorithme qui pose des questions ouvertes aux candidats qui ont effectué l'interaction initiale avec un chatbot. L'algorithme génère des scores d'adéquation culturelle en comparant les réponses données par les candidats avec les réponses données par un pool d'employés de l'entreprise.

Notre approche

KPMG a établi un cadre pour recueillir les données disponibles au sein de l'organisation et a proposé de nouvelles données variables et hypothèses à recueillir. Nous avons également déterminé des approches spécifiques pour auditer la solution d'IA, afin d'assurer sa neutralité, sa robustesse et sa performance.

Bénéfices

L'entreprise sera en mesure d'obtenir une assurance sur son algorithme de recrutement, réduisant ainsi le risque de discrimination et d'inefficacité, qui pourrait nuire à sa réputation et à ses finances.

Grande société émettrice de cartes de crédit (USA)

Le machine learning jouant un rôle de plus en plus important dans leurs décisions business, comprenant le risque de crédit, la détection des fraudes et les fonctions commerciales de marketing, l'équipe d'audit interne souhaitait préciser leur approche d'audit des modèles de machine learning. KPMG a été missionné pour aider à évaluer ses capacités, ses compétences et ses procédures de vérification de l'IA en comparaison avec les bonnes pratiques.

Notre approche

En collaboration avec de nombreuses équipes du cabinet, KPMG a mis au point une solution qui aide à évaluer les capacités, les compétences et les procédures d'audit interne par rapport à notre référentiel AI In Control, en plus d'offrir une formation aux équipes d'Audit interne sur l'évaluation des risques et des contrôles relatifs au machine learning.

Bénéfices

La société a vu son niveau d'assurance au regard de ses modèles d'IA fortement augmenter, et réduit le risque de défaillance de ces modèles, qui pourrait entraîner des dommages à la réputation de l'entreprise et des pertes financières.

Métropole Européenne (Pays-Bas)

Cette capitale européenne utilise un algorithme pour identifier, enregistrer, allouer et hiérarchiser les plaintes émanant de ses citoyens. La Ville veut s'assurer que l'attribution et la priorisation des plaintes sont impartiales et cherche donc à mettre en place un système de gestion des risques pour surmonter ces biais.

Notre approche

KPMG utilise sa méthode AI In Control pour guider la mise en place d'un système de contrôle sur la conception, la mise en œuvre et le fonctionnement de l'algorithme.

Bénéfices

La Ville sera en mesure d'assurer à ses citoyens que l'algorithme est contrôlé et examiné par une partie indépendante qui certifie sa conception, sa mise en oeuvre et son fonctionnement.

Grande institution financière (UK)

Une grande institution financière a mis en place un système de surveillance des transactions afin d'identifier les fraudes potentielles. Le système est fondé sur des modèles (complexes) et des règles métier. L'institution cherche à obtenir un examen indépendant des modèles utilisés afin de valider si le système de détection des fraudes a été mis en oeuvre tel qu'il a été pensé.

Notre approche

KPMG effectue un examen indépendant de la gouvernance, de la solidité, des données et des critères de rendement du système. Avec une approche sur mesure, KPMG valide l'exactitude des modèles utilisés et du système managérial qui les entoure.

Bénéfices

L'institution obtient une évaluation de la mise en oeuvre du système de suivi des transactions, comprenant des points d'amélioration potentiels. En outre, l'institution sera préparée à d'éventuelles vérifications des organismes de réglementation et des sociétés de surveillance.

Conclusion

L'intelligence artificielle est en train de révolutionner le monde des affaires et tout évolue rapidement. Ce n'est pas le moment d'être sceptique, d'hésiter ou d'attendre de voir. Pour réussir dans cet environnement disruptif, les dirigeants doivent rapidement prendre à leur compte les aspects pertinents de l'intelligence artificielle. Une prise de conscience, ainsi qu'un œil attentif aux opportunités émergentes, sont des conditions essentielles pour la viabilité de toute entreprise. Mais en même temps, il faut penser à maîtriser les nouveaux risques qui viennent avec l'Intelligence artificielle.

C'est pour répondre à cet objectif que nous avons construit notre approche IA In Control, qui vise à fournir des conseils et un cadre global pour gérer les risques liés à l'utilisation de l'IA.
Ce cadre est destiné à être continuellement amélioré au fur et à mesure que nous réalisons nos missions et adaptons notre méthodologie.

Nous vous invitons à nous contacter pour de plus amples informations et pour découvrir comment cette approche peut vous être utile !

Vos contacts

Julie Caredda
Partner Intelligence Artificielle, Lighthouse
Tél. : +33 (0)1 55 68 73 27
Port. : +33 (0)6 28 56 39 78
E-mail : jcaredda@kpmg.fr

Mariem Gamdou
Senior Manager, IT Risk Consulting
Tél. : +33 (0)1 55 68 25 71
Port. : +33 (0)6 19 24 76 38
E-mail : mgamdou@kpmg.fr

Laurent Gobbi
Partner, Responsable des activités Risk Consulting
Tél. : +33 (0)1 55 68 74 41
Port. : +33 (0)6 14 58 91 00
E-mail : lgobbi@kpmg.fr

Grégoire Levis
Partner, IT Financial Services
Tél. : +33 (0)1 55 68 88 58
Port. : +33 (0)6 18 40 84 36
E-mail : glevis@kpmg.fr

Vincent Maret
Partner, Privacy & Cyber
Tél. : +33 (0)1 55 68 26 64
Port. : +33 (0)6 17 12 22 13
E-mail : vmaret@kpmg.fr

Yohann Vermeren
Partner, Risk Consulting
Tél. : +33 (0)1 55 68 66 86
Port. : +33 (0)6 23 25 69 87
E-mail : yvermeren@kpmg.fr

kpmg.fr

Conception - Réalisation : Marketing & Communication - OLIVER - Juin 2019.

Crédit photos : DR.