XAVIER BAYS
GAEL LEDERREY
JOSÉ LAMAS-VALVERDE

TOUR D'HORIZON DES RISQUES: LE MODÈLE DES QUATRE PILIERS DE L'IA POUR LES PME

Outil essentiel pour guider les dirigeants dans l'univers de l'intelligence artificielle

Dans leur modèle économique, la valorisation des données est un enjeu stratégique pour les entreprises. À la lumière de cet article, les PME doivent mettre en place ou affiner leur stratégie technologique dans un contexte de concurrence accrue, tout en restant vigilantes face aux enjeux des intelligences artificielles (IA), dont les investissements massifs attirent le crime organisé.

1. INTRODUCTION

La technologie comporte des opportunités et des risques; cette ambivalence est inhérente à son fonctionnement. Elle concerne autant les individus que la collectivité et les entreprises, dans un contexte de développement industriel et technologique où la question de la répartition des risques est centrale. Si les prédictions des Big-tech sur des progrès inédits et des bénéfices sans précédent pour l'économie en matière d'intelligence artificielle (IA) tardent parfois à se concrétiser, des avancées tangibles apparaissent néanmoins, notamment dans les domaines de la recherche scientifique et de la santé. L'IA accélère également l'automatisation des processus et la transformation des services.

Du côté des menaces, citons la dépendance structurelle des organisations à des systèmes d'IA, la centralisation des données qui augmente les risques de cyberattaques, les usages non maîtrisés favorisant les fuites de données et la non-protection de la vie privée des individus. Ces enjeux rappellent que la société doit se donner les moyens d'instaurer un cadre réglementaire efficace.

Est-il légitime de s'inquiéter des risques liés aux intelligences artificielles? Sans verser dans la paranoïa, il est pertinent de se former à l'IA, d'imaginer les différentes situations à risque, de les hiérarchiser et d'envisager les risques de manière plus approfondie afin de prendre de meilleures décisions. En effet, une organisation disposant d'un important ensemble de données peut légitimement se demander comment les utiliser. Toutefois, un mauvais choix initial peut entraîner la réalisation des risques abordés dans cet article. La *figure 1* illustre ce contexte: pour naviguer dans la mer des données, il faut se doter des moyens appropriés.

1.1 Objectif. Il est bien connu que, pour que les choses changent, il faut prendre des risques, mais il est également avisé de connaître ces risques pour se fixer des limites en toute connaissance de cause. Cet article a pour but de dresser un panorama pragmatique des risques liés à l'IA. L'objectif n'est pas d'en identifier un grand nombre mais d'éclairer les décideurs sur l'ensemble du spectre: du risque souvent sous-estimé de l'inaction (ne rien faire) aux menaces concrètes engendrées par une utilisation quotidienne des outils.

1.2 Définitions clés. Pour naviguer sereinement dans l'univers des IA, il convient de clarifier les termes. Selon les normes de référence ISO [1], le risque est défini comme «l'effet de l'incertitude sur les objectifs». L'incertitude désigne la possibilité de la survenance d'un phénomène dangereux ou d'un changement de circonstances dont les effets ont un impact sur la réalisation des objectifs d'une organisation. Toutefois, ces effets ne se limitent pas aux effets négatifs (concrétisation de menaces), ils englobent également les effets positifs (concrétisation d'opportunités perturbant l'ordre établi).

XAVIER BAYS,
INGÉNIEUR EN MATHÉMATIQUES APPLIQUÉES EPFL, COFONDATEUR ET HEAD OF SERVICES, SWISS STATISTICAL DESIGN & INNOVATION

GAEL LEDERREY,
PH.D DATA SCIENCE, SENIOR DATA SCIENTIST, SWISS STATISTICAL DESIGN & INNOVATION

Figure 1: **POUR APPRENDRE À NAVIGUER DANS LA MER DES DONNÉES, IL FAUT SE DONNER LES MOYENS**

Dans la pratique, il est crucial de distinguer deux états du risque:
→ le risque inhérent: c'est le risque dit brut, c'est-à-dire tel qu'il existe en l'absence de toute mesure de contrôle;
→ le risque résiduel: c'est la part du risque qui subsiste une fois que des mesures de traitement (options de modification du risque) ont été mises en œuvre.

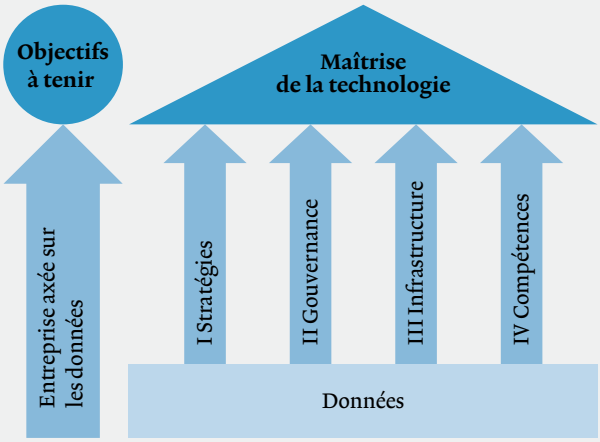
Le management des risques est une approche permettant de passer de l'un à l'autre. Il s'articule autour d'un processus cyclique qui consiste, dans un premier temps, à identifier, analyser et évaluer les risques (c'est ce qu'on appelle l'appréciation des risques), puis à les traiter et à les surveiller, tout en assurant une communication et une documentation adéquates à leur sujet. Cet article se concentre spécifiquement sur la première étape: l'identification des risques liés à l'IA. Nous proposons toutefois quelques clés méthodologiques pour l'analyse du risque en conclusion.

1.3 Méthode. Pour structurer cette analyse et couvrir un spectre aussi large que possible, deux approches ont été croisées. D'une part, le «modèle des quatre piliers de l'IA pour les PME», présenté au chapitre 2, sert de grille de lecture principale. D'autre part, une démarche ascendante est adoptée: l'identification commence par les risques opérationnels rencontrés au quotidien par les utilisateurs, pour remonter progressivement vers les enjeux plus structurants de gouvernance et de stratégie.

Les risques relatifs aux quatre piliers sont abordés dans les chapitres 3, 4, 5 et 6. Chaque risque est numéroté et défini en une seule phrase. Son contexte est brièvement expliqué, un exemple l'illustre et une piste de réflexion est proposée pour une analyse ultérieure.

JOSÉ LAMAS-VALVERDE, PH.D. PHYSIQUE, EXPERT EN ANALYSE DES RISQUES, FONDATEUR-DIRECTEUR, GESTRISK, JOSE.LAMAS@GESTIONDESRISQUES.CH

Figure 2: **MODÈLE DES QUATRE PILIERS DE L'IA POUR LES PME**



Le modèle des quatre piliers de l'IA pour les PME

2. LES QUATRE PILIERS DE LA MISE EN PLACE DE L'INTELLIGENCE ARTIFICIELLE

Le modèle des quatre piliers de l'intelligence artificielle pour les PME, présenté à la *figure 2*, permet d'orienter la transformation numérique de l'organisation et sert également de cadre pour identifier les risques liés à l'IA. Il repose sur les compétences, l'infrastructure, la gouvernance et la stratégie technologique. Selon les auteurs, ce modèle couvre les aspects les plus importants de la transformation *data driven* afin de maximiser les chances de réussite.

2.1 Les compétences. Au-delà de la création d'une *data team*, les compétences requises concernent une culture orientée data au sein de l'entreprise, connue comme data *literacy*. Il ne s'agit pas seulement de savoir coder, mais de comprendre ce qu'est une donnée, comment elle est produite, comment l'interpréter, ainsi que de faire preuve d'un engagement éthique. Une équipe data interne devra posséder trois compétences clés: la gestion des flux de données *(data engineering)*, l'analyse *(data science)* et surtout le lien avec le métier *(business analysis)*, indispensable pour que la technique serve les objectifs réels de l'entreprise.