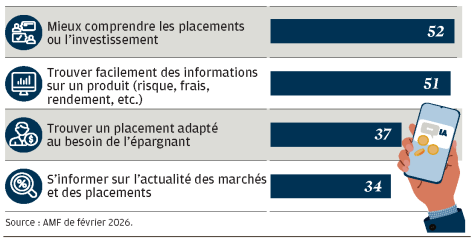
DAVID CHARLET,
PRÉSIDENT
DE L'ANACOFI

Révolution ou évolution naturelle ?

Depuis vingt-cinq ans se pose la question de la numérisation du monde de la gestion de patrimoine. En réalité, il y a deux interrogations en une : les professionnels sont-ils équipés ? Et leurs clients auront-ils encore besoin d'eux ou se débrouilleront-ils seuls avec des plateformes en ligne et des offres moins chères ?

La numérisation et le développement des outils technologiques ont indéniablement mené à une évolution du paysage.
Aujourd'hui, nombre des plus grandes banques françaises ont autant de clients ou presque dans leurs filiales en ligne que dans leurs réseaux d'agences. Presque 80 % de Français disposent d'un compte dans une banque en ligne ou dans une fintech, même si, dans la majorité des cas, il s'agit d'un compte complémentaire à celui de la banque traditionnelle.
L'usage du numérique est une réalité, et le placement via le portail ou l'application de notre banque est devenu accessible. Il n'y a dès lors aucune raison de ne pas considérer que l'intelligence artificielle (IA) va a minima remplacer du personnel dans ces entreprises.
Cependant, le cas de ceux que l'on appelle les CGP [*conseillers en gestion de patrimoine*] est assez différent. Ils ont toujours été à la pointe du progrès et utilisent beaucoup les outils numériques. La Covid-19 a d'ailleurs fait basculer les derniers réticents. Si certains ont déployé des plateformes en ligne – on parle du modèle dominant des « CGP amplifiés », ce phénomène s'est répandu jusque dans le monde du courtage. Si les grands acteurs (banques, assureurs) réduisent leur implantation sur le territoire, ceux du conseil et du courtage se multiplient et gagnent des parts de marché.
On compte 2.500 entreprises de courtage en assurances et 1.600 en conseil financier de plus en 2024 qu'en 2018. Elles se convertissent très rapidement à l'IA, comme auparavant aux simulateurs, agrégateurs et autres outils techs. Toutes les organisations professionnelles les accompagnent dans ce mouvement. Actuellement, ce ne sont donc pas tant les entreprises qui sont en danger, mais les emplois et les fournisseurs d'outils.
Quand il faut payer très cher pour un outil de comparaison de produits ou de rédaction de documents et de procédures de conformité, au résultat rarement impeccable, alors qu'avec une IA à quelques centaines d'euros pour un accès professionnel, on peut obtenir un résultat très convenable, les entreprises s'interrogent. La vraie question est celle du rapport du client à ces outils et à leur conseil ou intermédiaire. Des études de l'AMF ou d'Ipsos de 2025 nous éclairent assez bien. Si quatre Français sur dix et une majorité des moins de 35 ans utilisent les IA génératives, le taux chute très vite (jusqu'à moins de 20 %) pour les plus âgés ; or, ce sont eux qui détiennent le capital.

Qu'attendez-vous de l'IA ?
En %



Source : AMF de février 2026.

L'IA BRIDE LA RÉFLEXION

Cependant, les cadres supérieurs sont plus de 60 % à les utiliser. Alors, le font-ils en matière d'épargne et d'investissement ?
Pour l'instant, ils ne s'en servent pas tant que ça, avec dans presque un cas sur deux une crainte quant à la qualité de l'information obtenue et, dans 40 % des cas, ils pensent que l'IA bride la réflexion, en plus de créer une dépendance non souhaitable.
Ils ne seraient donc que 11 % à utiliser l'IA avant de réaliser un placement, alors que 42 % vont vers un conseiller humain. Par ailleurs, 67 % d'entre eux craignent les erreurs du robot, et plus de 50 % ne s'en servent que pour mieux comprendre.
Ce que ces chiffres disent, c'est que les investisseurs veulent en majorité un accompagnement. Ce qui change, c'est sa forme.
Alors certes, ce conseil et cet accompagnement ne nécessiteront plus autant d'humains, ainsi un même professionnel pourra accompagner plus de clients.
Chacun s'est approprié la technologie et ses avantages, et finalement tous les schémas sont aujourd'hui utilisés. Les professionnels de l'investissement et de la gestion de patrimoine sont donc, encore une fois, à la croisée des chemins. Ils doivent améliorer l'expérience client, au moment où l'IA leur fait entrevoir une baisse des coûts de production qui n'ont fait que progresser depuis quinze ans, alors que leurs frais pris aux clients (leurs rémunérations par euro investi) baissaient.

> « Les investisseurs veulent un accompagnement. Ce qui change, c'est la forme de celui-ci »

NE PAS RATER LA NÉCESSAIRE MUTATION

Leurs interrogations du moment sont simples : comment ne pas rater la nécessaire mutation, afin de satisfaire des clients qui, soit se seront renseignés quant aux options et produits, soit attendront de leur conseiller qu'il sache faire ce qu'ils ne savent ou ne veulent pas faire, en tirant le meilleur de l'IA. Dès lors, les professionnels et les entreprises de l'investissement doivent définir quelle IA utiliser pour quelle tâche, apprendre à savoir bien prompter, gérer leur responsabilité (si l'IA, qui n'est qu'un outil, génère des erreurs) et se maintenir à jour, ce qui implique de se former.
Si les entreprises du conseil savent gérer cette transition, il semble que la clientèle qui souhaite leur aide restera constante. Elle risque cependant d'être plus exigeante et mieux informée.
Se pose la question de la génération des moins de 30-35 ans, qui ne connaîtra pas les effets de la transmission de capital avant une vingtaine d'années.
D'ici là, il peut se passer beaucoup de choses. Si, par exemple, en cas de succession, ces derniers ne ressentent plus le besoin d'un conseil humain, alors un changement majeur aura eu lieu, car aucune génération jusqu'ici ne s'est passée d'un conseil financier le moment venu, mais pour l'instant, l'IA n'arrive pas encore à supplanter l'humain…

ODILE DUTHIL,
PRÉSIDENTE DU CLUSIF
ET DIRECTRICE,
DE LA CYBERSÉCURITÉ
DU GROUPE CAISSE
DES DÉPÔTS

Cybersécurité : les entreprises dans une zone de turbulence

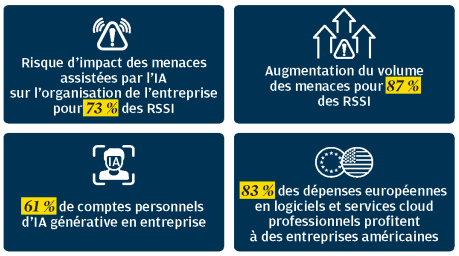
L'intelligence artificielle n'est plus une innovation émergente : elle est devenue un accélérateur de processus dans les entreprises, et, par conséquent, un accélérateur également pour les attaquants.

Dans ce contexte, il est important à la fois d'encadrer les risques liés à l'usage des intelligences artificielles (IA), la cybersécurité pour l'IA, et d'intégrer les IA dans le système de défense des entreprises.
Dans ce nouveau paysage où les risques liés aux ruptures technologiques augmentent, il est important pour chaque entreprise de bien définir sa politique en matière de continuité d'activité en cas de crise. La résilience opérationnelle n'est plus un objectif : elle devient une condition de survie.

L'IA AMPLIFIE TOUT : LES USAGES, LES ATTAQUES, LES DÉPENDANCES

L'IA générative a déclenché une vague d'usages massifs, souvent non maîtrisés, en créant une appétence pour l'IA.
Parallèlement, l'IA offensive change d'échelle : les fuites de données par les prompts se multiplient, les modèles peuvent être manipulés, et les vulnérabilités spécifiques comme l'empoisonnement des données deviennent des vecteurs d'attaque à part entière.
L'arrivée du modèle Mythos, développé par la société Anthropic, a accentué cette pression : en réduisant le délai entre la publication d'une vulnérabilité et son exploitation, elle impose une surveillance accrue et un resserrement brutal des cycles de *patch management*.
Et, surtout, elle met en avant les potentielles faiblesses des entreprises dont les mécanismes de défense traditionnels sont mis à rude épreuve face à des attaquants plus agiles et plus rapides.
A cela s'ajoute un risque souvent sous-estimé : la dépendance technologique.
L'interdiction faite à Anthropic par le gouvernement des Etats-Unis de commercialiser Claude Fable 5 et Mythos 5 aux entreprises étrangères a rappelé qu'un fournisseur extra-européen peut rendre indisponible un service devenu critique et ce, sans préavis. Le *kill switch [arrêt d'urgence]* tant redouté n'est plus un scénario théorique.

Des RSSI inquiets et en surchauffe



Sources : Darktrace, Microsoft, Cigref, Asteres 2025.

GOUVERNER, ENCADRER, SÉCURISER : LES TROIS RÉFLEXES VITAUX

Face à cette accélération, les entreprises doivent structurer leur réponse autour de trois priorités :
– gouverner l'IA pour garder la maîtrise – comité IA, charte d'usage, cartographie des outils, des modèles et des données. Sans cadre de gouvernance, l'IA devient rapidement incontrôlable ;
– encadrer les usages pour contenir le *shadow IA [utilisation non autorisée de l'IA]* : les métiers adoptent l'IA à une vitesse inédite, souvent sans mesurer pleinement les risques associés (qualité des données, divulgation involontaire d'informations sensibles, dépendance à des modèles opaques ou non maîtrisés). Les solutions non validées doivent être identifiées, encadrées, bloquées ou remplacées. Laisser prospérer le *shadow IA*, revient à accepter une perte progressive de contrôle sur son patrimoine informationnel ;
– sécuriser les modèles et les flux critiques : tests de robustesse, audits, supervision continue… L'IA doit être traitée comme un système critique, mais elle constitue aussi un levier majeur de défense. Analyse des flux, détection d'anomalies, corrélation de signaux faibles, automatisation des tâches du centre des opérations de sécurité (SOC) : l'IA devient un allié indispensable pour absorber un volume d'alertes désormais impossible à traiter uniquement par des moyens humains.

AUTONOMIE STRATÉGIQUE : UN IMPÉRATIF, PLUS QU'UN SLOGAN

L'affaire Anthropic a rappelé que la souveraineté numérique n'est pas une question idéologique, c'est un enjeu de continuité d'activité. Les entreprises doivent diversifier leurs fournisseurs, renforcer leurs compétences internes, maîtriser leurs données et privilégier, lorsque cela est pertinent, des solutions européennes.
L'autonomie stratégique se mesure à la capacité de choisir ses dépendances et de continuer à opérer lorsqu'elle disparaît.

LA CONFIANCE NUMÉRIQUE : L'ACTIF IMMATÉRIEL LE PLUS PRÉCIEUX

Dans un monde où les ruptures technologiques se succèdent, la confiance numérique devient un actif immatériel déterminant. Elle conditionne la relation avec les clients, la crédibilité auprès des partenaires, l'attractivité auprès des investisseurs et la capacité à absorber les crises. C'est elle qui distingue les organisations robustes des organisations vulnérables.
Notre communauté travaille à cet égard au développement d'un indice de résilience numérique destiné à devenir un repère d'aide à la décision pour les dirigeants comme pour les investisseurs.

L'HEURE N'EST PLUS À L'OBSERVATION

L'IA accélère tout : les opportunités, les risques, les dépendances. Les entreprises doivent désormais réagir avec la même vitesse. Gouvernance, maîtrise des usages, sécurité technique, résilience opérationnelle et autonomie stratégique : tels sont les cinq piliers d'une cybersécurité adaptée à l'ère de l'IA.
Les organisations qui s'y engagent dès aujourd'hui ne se contenteront pas de mieux résister aux turbulences à venir, elles transformeront la confiance numérique en avantage compétitif durable.