LA CHRONIQUE

de François-Serge Lhabitant

La fin du conseiller ou du client?

Selon une étude publiée par Citigroup, les «robo advisors» ou robots-gérants auraient aujourd'hui près de 14 milliards de dollars sous gestion et devraient augmenter ce montant à près de 5000 milliards à l'horizon 2025. Venus des Etats-Unis, leur but est de démocratiser la gestion d'actifs, tellement chronophage si vous la faites vous-même, tellement coûteuse et réservée aux plus fortunés si elle est déléguée à un conseiller financier appartenant à l'espèce humaine.

Le principe de fonctionnement des robots-gérants est relativement simple. Tout d'abord, l'investisseur potentiel n'a plus besoin de se rendre dans sa banque ou chez son conseiller financier. Il se connecte à un site internet et répond à quelques questions en ligne. Un logiciel analyse ses réponses, puis détermine la stratégie de placement appropriée en fonction de ses intérêts, de son âge, de sa fortune, de ses objectifs de placement et de sa propension au risque. Le plus souvent, cette stratégie est un mélange de fonds de placements ou exchange traded funds. Le client n'a ensuite plus qu'à cliquer sur un bouton pour accepter cette stratégie, affirmant au passage qu'il a bien lu toutes les informations relatives. Ses avoirs sont immédiatement investis selon la stratégie suggérée par le robot, et ajustés ensuite à chaque fois que le robot le jugera nécessaire.

Initialement destinés aux investisseurs individuels, les robots-gérants s'attaquent maintenant aux tiers gérants et conseillers financiers. Ils mettent en avant la simplification des procédures de gestion de portefeuille, et le fait que le bipède conseillé par le robot peut se consacrer à d'autres aspects bien plus intéressants (la fiscalité, les successions, FACTA, l'échange automatique d'informations, etc.).Pas d'intervention humaine, pas de locaux coûteux, une standardisation à l'extrême puisque tous les portefeuilles suivant la même stratégie peuvent être gérés en même temps – l'utilisation de robots-gérants semble n'apporter que des bénéfices… en tout cas pour ceux qui les mettent en place ainsi que pour les fonds destinataires des allocations. Mais qu'en est-il de l'investisseur final? Certes, les robots-gérants ne prélèvent qu'une modeste commission de gestion de 0,30% par année, mais leur activité les vaut-elle véritablement? Au risque d'en décevoir certains, notre avis est que les robots-gérants sont un peu ce que les fast foods sont à la gastronomie. Le résultat est certes peu coûteux, rapide, pratique, sans surprise, mais il est produit dans une usine de manière industrielle et à long terme est loin d'être idéal pour notre santé.

Tout d'abord, la plupart des robots-gérants suivent des algorithmes simplistes, typiquement basés sur la théorie moderne du portefeuille et ses grands principes qui datent des années 1950. Ils favorisent donc souvent des fonds indiciels, voient les actions comme plus rémunératrices mais plus risquées que les obligations, et ont donc tendance à les surpondérer quand on est jeune et à les sous-pondérer en vieillissant. Pas sûr que tout ceci ne justifie un coût de 0,30% par année, d'autant plus qu'ils sont incapables de prendre en compte des spécificités, les passifs ou les désirs un peu trop particuliers. Ensuite, le choix des véhicules d'investissement est relativement limité. L'investisseur se retrouve donc restreint à une palette de produits financiers le plus souvent choisie plus pour des raisons commerciales que pour la véritable qualité de leurs gérants, et sortant rarement des actions, obligations, et marché monétaire. Oubliez donc l'idée de battre le marché. Enfin, les décisions des robots-gérants sont prévisibles et donnent lieu à de larges volumes d'achats et de ventes sur les marchés financiers. Avec l'augmentation des actifs sous gestion des robots, ces volumes devraient avoir une influence grandissante sur les cours. Et comme d'habitude, des investisseurs sophistiqués comme par exemple des hedge funds devraient commencer à les arbitrer – typiquement en mettant en place des robots arbitrageurs. Il est assez facile de voir dans quels sens les profits vont se diriger.

Tout ceci est bien joli, me direz-vous, mais quid des investisseurs ayant une assise financière petite à moyenne et sans aucune connaissance financière? Au départ, les robots-gérants visaient typiquement cette clientèle, si possible plutôt jeune et désireuse de tout faire via leur tablette ou leur smartphone.

A notre avis, ces investisseurs sont précisément ceux qui auraient le plus besoin de conseils et d'explications avant d'investir, afin de bien comprendre les conséquences possibles de leurs choix. Et ce d'autant plus que le jour où le marché commencera à corriger, il leur faudra composer un numéro surtaxé où une voix suave mais légèrement métallique leur demandera poliment de patienter en attendant qu'un bipède – qui ne connaîtra rien de leur situation – se libère. Alors et peut-être alors seulement ces clients devenus de simples jouets dans les mains d'automates regretteront-ils ces bons vieux conseillers! ■

François-Serge Lhabitant est Professeur de Finance à l'EDHEC Business School.
L'article ne reflète que les vues personnelles de l'auteur.

CYBERSÉCURITÉ

SOLANGE GHERNAOUTI
Professeure, directrice du Swiss Cybersecurity Advisory & Research Group, HEC – Unil (www.scarg.org)

La manipulation pire que le vol des données

Cette nouvelle forme de cyberattaque ne vise pas à la prise de contrôle de systèmes informatiques mais à celle du cerveau humain.

Jusqu'à présent, la majorité des problématiques de cybersécurité était centrée autour des questions de disponibilité et de confidentialité des données et des moyens à mettre en œuvre pour lutter contre des attaques en déni de service, contre l'espionnage ou encore le vol ou la destruction de données. Désormais, c'est la manipulation de l'information visant son intégrité, sa fiabilité et sa véracité qui semble devenir une préoccupation majeure des experts sécurité, comme le souligne en particulier l'article paru le 10 septembre dernier sur le site américain Defense One «La nouvelle vague de cyberattaque ne volera pas des données mais les modifiera».

En ébranlant la confiance dans l'information accédée, en affectant ainsi la perception de la réalité et son analyse, «l'ennemi» est paralysé et n'est plus en mesure de décider correctement.

Ce brouillage de l'information, le fait de ne jamais savoir avec certitude si elle est juste ou non, relève des mêmes mécanismes que ceux utilisés par des personnalités perverses pour rendre l'autre fou et le manipuler à son avantage. Il s'agit d'une véritable guerre psychologique et sémantique, une guerre d'influence où les manipulations à des fins tactiques et stratégiques peuvent être d'envergure et concerner la population comme également des décideurs civils et militaires. Ce type de cyberattaque ne vise pas à la prise de contrôle de systèmes informatiques mais à celle du cerveau humain.

C'est le pouvoir de l'information comme le soulignait, il y a plusieurs décennies déjà, le slogan du magazine *Paris Match* «Le poids des mots, le choc des photos», plus que jamais d'actualité, Internet offrant une caisse de résonnance sans précèdent à ce phénomène préexistant à l'ère digitale. Il suffit pour s'en convaincre de se rappeler la manière dont les photos de personnes décapitées ou d'un enfant mort sur une plage impactent le comportement des individus et influencent les décisions politiques qui affectent la vie de chacun.

Selon une des dernières études du groupe Allianz concernant les cyberrisques, l'augmentation de la connectivité et de la commercialisation des outils de la cybercriminalité accroissent le nombre, la gravité et le coût des incidents, constitue une des menaces les plus importantes auxquelles nous sommes confrontés. En outre, la performance économique de nos organisations est de plus en plus dépendante de l'impact des contraintes réglementaires liées au monde numérique et aux conséquences financières relatives à leur non respect ou consécutives à des vols de données. A cela s'ajoute, toujours selon Allianz, les coûts liés aux interruptions des affaires, aux vols de propriétés intellectuelles ainsi qu'aux chantages rendus possibles par des cyberattaques.

Bien que les cyberrisques soient complexes et multiformes, nous disposons pour les maîtriser de quelques fondamentaux qui doivent être pris en considération au niveau stratégique et instanciés en mesures opérationnelles efficaces. Cela passe entre autres par:

- **une gestion continue des risques pour les éviter, les accepter, les contrôler ou éventuellement les transférer;**
- **l'identification des valeurs critiques de l'entreprise et des risques associés (cela ne concerne pas uniquement les risques d'origine technologique mais aussi ceux liés à l'humain, ou à une trop forte dépendance à des entités tierces, ou encore à des situations conjoncturelles de fusion, acquisition par exemple);**
- **une culture de la cybersécurité et une hygiène informatique appropriées;**
- **des plans de gestion de crise et de continuité des affaires.**

Ainsi, pour une organisation, quels que soient sa taille et son secteur d'activité, toute infrastructure connectée est attaquable, augmentant notamment son risque de réputation et d'image. Dès lors, comprendre son exposition aux cyberattaques et ses nouvelles vulnérabilités afin d'être prêts à gérer les cyberincidents est devenu primordial.

Cette inévitable phase de sensibilisation aux cyberrisques est fondamentale, car elle permet de définir sa posture vis-à-vis des risques et d'agir en toute connaissance de cause mais aussi de renforcer le pouvoir de chacun à produire de la sécurité en adoptant des comportements cohérents, en réduisant sa fenêtre d'exposition et devenant un vecteur privilégié de la détection des risques et non de leur propagation.

Se connaître soi, avoir les pieds sur terre, rechercher l'authenticité ne constituent pas une autre idée du bonheur mais est devenu un invariant du développement personnel et économique et nous renvoie à la nécessité de pouvoir disposer des bonnes informations, aux bons moments, aux bons endroits, et donc à l'urgence de pouvoir contrer ou pallier les dispositifs visant à en modifier le sens et à les manipuler. ■