Réputation et appropriation du produit par le public

L'intégration des IA génératives au cœur du développement logiciel est devenue presque indispensable aujourd'hui. Cependant, cette transition place les entreprises devant un défi de taille, à savoir exploiter ces outils sans compromettre la confiance de ses clients et sa crédibilité sur le marché. Si l'IA permet de produire beaucoup plus vite, elle crée aussi des vulnérabilités critiques. Ainsi le risque ne se limite pas qu'à une simple erreur de code, il touche désormais à l'image de l'entreprise. Mais comment profiter du gain de performance offert par l'IA tout en restant crédible auprès d'un public de plus en plus sceptique ?

Dans un premier temps nous allons étudier les risques de dégradation de l'image liés aux erreurs éthiques ou techniques. Dans un second temps nous verrons pourquoi l'IA peut faire baisser la valeur perçue d'un produit et créer un flou juridique qui freine l'appropriation par les clients.

La réputation d'une entreprise de développement repose sur sa capacité à sécuriser ses données et garantir la fiabilité de ce qu'elle livre même lorsqu'elle utilise des outils automatisés.

Tout d'abord, l'un des risques majeurs pour la réputation est celui de la fuite de données confidentielles. En avril 2023, le géant **Samsung** a subi une crise de sécurité majeure lorsque des ingénieurs ont utilisé ChatGPT pour optimiser du code source et retranscrire des réunions stratégiques. Comme le rapportent les articles de *CIO Dive* "Samsung employees leaked corporate data" et *Gizmodo* "Oops : Samsung Employees Leaked Confidential Data", ces données confidentielles sont devenues la propriété de l'algorithme d'OpenAI pour entraîner ses futurs modèles. Cet incident révèle un manque d'encadrement interne qui peut être perçu par les clients comme une forme de négligence.

Par conséquent, le journal *Le Monde* a rapporté que l'entreprise a dû interdire brutalement l'outil à ses employés "Samsung interdit l'utilisation de ChatGPT à une partie de ses employés", en mai 2023 pour limiter les dégâts. Pour le public, le message est catastrophique, si un géant technologique ne peut empêcher ses propres équipes de donner ses secrets, comment peut-il garantir à ses clients la sécurité de

leurs données ?

En plus de ce défaut de sécurité, une entreprise engage sa réputation sur la fiabilité des solutions livrées. Or, l'IA est sujette aux hallucinations, produisant des erreurs avec une assurance trompeuse qui peut même duper des professionnels. Ainsi, en février 2024, la justice canadienne a rendu une décision historique contre **Air Canada** après que son chatbot a inventé une règle de remboursement inexistante. Selon les analyses de *CBC News* "Air Canada found liable for chatbot's bad advice" et du cabinet *McCarthy Tétrault* via *The Guardian* "Moffatt v. Air Canada", le tribunal a statué que l'entreprise est l'unique responsable des propos de sa machine. Dès lors, l'argument du bug technique ou de l'autonomie de l'IA devient juridiquement et moralement irrecevable. Pour une société de développement, si une IA suggère une faille de sécurité que l'entreprise déploie sans vérification minutieuse, l'image d'expert rigoureux s'efface derrière celle d'un prestataire négligent qui a abandonné son rôle de superviseur au profit de la rentabilité.

Au-delà de ces enjeux de réputation, l'usage de l'IA transforme la perception qu'a le marché du produit final. L'appropriation d'un logiciel par le public n'est pas automatique, c'est un processus où l'utilisateur doit reconnaître l'utilité, la rareté et la légitimité d'une solution pour y adhérer.

D'un côté, on observe une dévaluation systématique du travail lorsqu'il est perçu comme ayant été effectué par une IA. Si le public a l'impression que le produit est généré à la chaîne, son envie de se l'approprier s'effondre car il devient banal. L'analyse de *ByteIota* "Stack Overflow Traffic Collapses 75% as AI Tools Win" et les réflexions du blog de *Stack Overflow* "Disrupting yourself in the age of AI" montrent que l'IA fragilise les communautés d'experts au profit de réponses automatisées. De fait, si une entreprise ne peut plus prouver la valeur ajoutée de ses développeurs, son produit n'est plus perçu comme une création unique ou innovante. L'appropriation par le client devient alors impossible car il n'y a plus de lien émotionnel ou technique fort avec l'outil. On ne se sent pas lié à un code produit en un clic, et le logiciel devient un simple consommable remplaçable par n'importe quelle autre IA concurrente, faisant chuter le pouvoir de négociation de l'entreprise.

De l'autre côté, l'appropriation est freinée par un flou juridique qui crée une barrière à l'achat. En effet, le recours collectif contre **GitHub Copilot** (Microsoft/OpenAI), détaillé par *The Register* et le cabinet *BakerHostetler* ("Doe v. GitHub, Inc. - The Copilot Litigation"), ainsi que par *Finnegan*, met en lumière le risque de parasitisme logiciel. L'IA peut reproduire des parties de code protégés par des licences sans citer les auteurs originaux. Donc, si un client achète un logiciel

contenant du code potentiellement plagié, il s'expose à des poursuites. Cette crainte juridique agit comme un véritable frein, le public refuse de s'approprier une technologie qui pourrait être accusée d'illégalité à tout moment. La propriété intellectuelle devient alors une zone d'ombre, et le client finit par se détourner d'une innovation qu'il juge trop "toxique" légalement.

En conclusion, l'IA générative apporte un gain de performance indéniable, mais elle amplifie aussi les risques pour une entreprise. Comme l'ont montré les cas de Samsung et d'Air Canada, la responsabilité ne se délègue pas, l'entreprise reste seule juge et coupable aux yeux du monde quel que soit l'outil utilisé. L'appropriation par le public, qui garantit le succès commercial à long terme, ne peut survivre que si la société garantit une valeur ajoutée humaine visible et une sécurité juridique irréprochable.