

Analyse individuelle d'un risque IA

L'arrivée massive d'outils permettant de coder plus vite comme ChatGPT, Claude ou Gemini au sein d'une équipe de développement peut créer un problème juridique que les sociétés doivent combler d'urgence à l'avenir. Pourquoi ? Tout simplement parce que le risque légal d'un outil IA puissant peut avoir de grandes conséquences pour la survie de la propriété intellectuelle de la société. Et c'est pour cela que pour y voir plus claire je vais analyser d'abord la conformité légale (RGPD, droit d'auteur) puis la responsabilité en cas de litige.

1. Le cadre de la Légalité

Tout d'abord je vais commencer par la propriété intellectuelle. En sachant que lorsque demandé à l'IA de nous fournir du code ou de nous aider à faire un projet, la chose importante à savoir est d'où vient ses code car les IA sont entrainer soit parce que les gens envoie comme la version gratuite de Chatgpt pûur entraîner le modèle ou par des morceaux de codes qui viennent de projets sous Licence GPL (licence qui oblige partager son code). En sachant cela il est important de se poser la question dans le cadre d'un projet dans une équipe, a qui appartient le code générer ? car actuellement, une œuvre sans auteur humain n'est pas protégée par le droit d'auteur et le risque pour une entreprise est qu'elle ne pourrait ne pas être propriétaire légale du logiciel qu'elle veut vendre ce qui peut porter préjudice pour celui qui a fait fait générer le code et aussi l'employeur. Et le plus gros risque pour l'entreprise, en prenant en compte que l'IA a été entraînée sur des codes sous licence GPL, si elle donne un morceau de code protégé sans citer la source, l'entreprise devient alors contrefactrice. Le terme juridique, je ne l'invente pas, il vient directement du Code de la propriété intellectuelle (CPI). Et l'un des dangers les plus gros liés à l'usage des IA génératives est qu'une société risque de devenir une société contrefactrice. Du coup, ces outils peuvent produire des morceaux de code protégés par le droit d'auteur ou par des licences Open Source. Si l'entreprise intègre et commercialise ce code sans respecter les obligations de l'auteur original, elle s'expose à des poursuites pour contrefaçon.

Sur le plan de la légalité, cet incident pose la question de la souveraineté des données : une fois le code injecté dans l'interface de l'IA, la société perd la maîtrise juridique de ses données. Le risque est que ce savoir-faire unique à chaque société tel que par exemple de Samsung qui est l'une des plus grandes entreprises du monde dans le secteur de la haute technologie, soit intégré au modèle d'apprentissage de l'intelligence artificielle et profite indirectement à la concurrence. Cet événement a d'ailleurs conduit Samsung à interdire temporairement l'usage de ces outils pour protéger leur propriété intellectuelle et éviter des sanctions liées à la négligence de la protection des données internes. Et dernièrement l'Europe a voté une loi l'AI Act qui impose des règles de transparence plus précisément dans l'article 50 où il impose des obligations de transparence strictes obligeant à marquer tout contenu généré par une intelligence artificielle.

2. Responsabilité

Maintenant passons à la partie responsabilité, prenant l'exemple si un jour nous l'on génère par une IA qui contient une faille de sécurité dans le cadre d'un projet dans une entreprise. Si le client de l'entreprise se fait pirater à cause de ça, c'est l'entreprise pour qui l'on travaille qui est responsable juridiquement et surtout pas l'éditeur de l'IA. Et cela montre juste qu'en tant que développeur on a des responsabilités car si il y a des problèmes ça en pâtit pas seulement sur nous mais surtout aux entreprises qui ont une obligation de résultat envers leurs clients. En droit français l'employeur est responsable des actes de ses salariés et la personne qui en assume les conséquences n'est pas les développeurs mais le patron. Une autre cas de responsabilité est que si le développeur utilise l'IA en cachette c'est-à-dire sans l'accord de l'entreprise, il peut être sanctionné disciplinairement mais l'entreprise reste malgré tout responsable vis-à-vis de l'extérieur. C'est pour cela qu'il est important de sensibiliser les développeurs et les développeurs de demain par rapport à la responsabilité qui ont envers leurs sociétés et même envers les clients de leurs sociétés. C'est pourquoi la mise en place d'une politique d'utilisation stricte de l'IA et la sensibilisation des équipes sont cruciales. L'objectif est de transformer le risque de "Shadow AI" en une utilisation maîtrisée et conforme, assurant ainsi la protection de l'entreprise.

Pour conclure, l'intégration des IA génératives au sein des équipes de développement représente une contradiction pour l'entreprise. Si le gain de productivité est indéniable, les risques juridiques identifiés, qu'il s'agisse de la violation du secret des affaires comme l'exemple par l'affaire Samsung ou du non-respect des licences Open Source et ceci font peser une menace réelle sur la pérennité des actifs de la société. Sur le plan de la légalité, le nouveau cadre européen (AI Act) impose désormais une transparence et une vigilance accrues, transformant l'usage de l'IA d'un simple choix technique en un véritable enjeu de conformité réglementaire. Et concernant la responsabilité, on comprend clairement que l'outil ne dédouane jamais l'humain, l'entreprise reste l'unique responsable juridique des erreurs ou des failles de sécurité produites par une machine. Tout ça pour faire comprendre que pour avancer sereinement, la solution ne se trouve pas dans l'interdiction, mais dans la gouvernance. La mise en place d'une Charte interne de l'IA et d'un protocole de revue de code systématique sont les seuls moyens efficaces pour protéger la société tout en profitant de l'innovation technologique.

Sources

- **Règlement (UE) 2024/1689** du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (connu sous le nom de « **règlement sur l'intelligence artificielle** » ou « **AI Act** »). *Publié au Journal officiel de l'Union européenne le 12 juillet 2024.*
- *Le Monde (02/05/2023). "Samsung interdit à ses salariés d'utiliser ChatGPT après une fuite de données".*
- *Code de la propriété intellectuelle (France). Article L335-2.*
- *Code civil (France). Article 1242, alinéa 5.*