



# Securit.i 2026

IA et sécurité

GAYTE Dominique - dominique@gayte.it

## Y'a pas de sécurité !

- IA : pas de sécurité !
- L'IA est à la fois
  - Un puissant atout pour la défense
  - Et un excellent outil pour augmenter la surface d'attaque
- Mais est devenue indispensable pour les métiers
  - On ne peut éviter leur utilisation
  - Et l'intégration des IBM i



## Chat/agent IA

- Une IA qui répond
  - Seul le modèle est sollicité : une question entre, du texte sort
  - Si elle se trompe
    - La conséquence est une mauvaise réponse, le risque s'arrête à l'écran (ou à ce que vous faites de la réponse)
- Un agent IA
  - Même fenêtre que le chat en façade
  - Mais derrière : des données réelles sont traitées
  - Des outils sont exécutés (requêtes, calculs, actions)
    - Avec la capacité de modifier (les données, le système...)
  - Le risque devient une fuite, une décision, une action...

## Chat/agent IA

- Une IA qui répond
  - Seul le modèle est sollicité : une question entre, du texte sort
  - Si elle se trompe
    - La conséquence est une mauvaise réponse, le risque s'arrête à l'écran (ou à ce que vous
- Une IA qui ne fait que répondre produit du texte. Un agent IA accède à des données, utilise des outils et peut déclencher des actions. Il doit donc être sécurisé comme une identité informatique disposant de pouvoirs sur le système d'information.
  - Mais derrière : des données réelles sont traitées
  - Des outils sont exécutés (requêtes, calculs, actions)
    - Avec la capacité de modifier (les données, le système...)
  - Le risque devient une fuite, une décision, une action...

# Les problématiques liées à la sécurité de l'IA dans un monde IBM i

- L'IA peut être utilisé dans deux grands domaines
- Développement
  - Vous utilisez des assistants IA pour vos développements (création, maintenance, documentation...)
  - Bob, Claude...
  - Pour l'équipe IT
- Les agents IA
  - Intégration des données de l'IBM i dans les processus IA
  - Avec ou sans serveur MCP
    - De manière contrainte, ou pas
  - À destination des métiers

## La sécurité dans un contexte de développement

- Les données remontent sur les serveurs IA dans le cloud
  - Les codes sources
  - Les formats de fichiers
  - Les données des fichiers...
- Il faut cacher des IA les informations sensibles
  - Mots de passe et autres secrets dans les codes source
  - Algorithmes importants
  - Définissez un espace de travail adapté au projet
  - Ne partagez que ce qui est indispensable
  - .bobignore, .gitignore
- Ne pas tout laisser faire en automatique
  - Limitez les approbations automatiques (utilisez le [mode](#) adapté)
  - Pas d'exécution de commandes sans validation humaine
  - Vérifiez les permissions des outils
  - Vérifiez et testez ce qui est généré avant la mise en production

## La sécurité et les agents IA

- La base de données de l'IBM i contient souvent l'essentiel de vos données
- Il paraît donc normal (et même essentiel, souvent) d'utiliser ces données dans les processus IA
- Mais il faut s'assurer :
  - Que des informations sensibles ne vont pas remonter dans le cloud
  - Que les agents IA ne pourront pas faire plus que ce qui est prévu
    - Que de la lecture, et que sur les fichiers admis
  - Que les profils utilisateur concernés ont un niveau de sécurité adapté
    - Pas de \*ALLOBJ, droit de lecture des données uniquement

## L'architecture que nous préconisons

- Impossible d'utiliser les données de l'IBM i sans les remonter dans les IA
- L'idée est donc de disposer d'une architecture sécurisée
- *On promise* c'est tout à fait possible
- Vous disposez d'un LLM (open source) en local (ou cloud privé)
  - Il y a maintenant de bons produits
  - Se pose la question du matériel
- Vous l'enrichissez avec vos règles métier et vos documents si besoin
  - RAG par exemple
- Vous pouvez même utiliser un serveur MCP qui va assurer le tampon entre l'IA et vos données. Seules les requêtes (tools) prédéfinies pourront être exécutées
- Voir l'intervention de Pierre SICCARDI (AI Tech Lead) & Laetitia TURQUOIS (I.GAYTE.IT)

## IA Act

- L'IA Act (Règlement (UE) 2024/1689 et autres) est la première loi au monde à encadrer de manière complète le développement, le déploiement et l'utilisation des systèmes d'IA dans l'UE. Elle est entrée en vigueur le 1er août 2024 et s'applique progressivement jusqu'en 2028
- Renforcement depuis le 2 août 2026
  - Interdictions et pouvoirs de sanction. Les obligations "haut risque" sont provisoirement reportées (2027-2028 selon les annexes)
  - Obligations de transparence (**EU Icons for labelling AI-generated content**)

**AI GENERATED**

**AI**

**AI MODIFIED**



Image maintenant générée par CoPilot



## 4 niveaux de risques définis par l'IA Act

- Minimal : sans impact significatif sur les droits ou la sécurité
  - Correcteur orthographique, recommandations
- Limité : IA peut influencer l'utilisateur, mais sans impact critique. L'obligation principale est la **transparence**. L'utilisateur doit savoir qu'il ne parle pas à un humain.
  - chatbots
  - IA générative (texte, image, vidéo)
  - assistants virtuels
- Élevé : IA peut affecter des droits fondamentaux, la sécurité ou des décisions critiques. Toute entreprise utilisant une IA "risque élevé" doit se préparer à un vrai cadre réglementaire
  - RH
  - Scoring (crédit bancaire, assurance)
  - Surveillance humaine obligatoire
- Interdit : interdiction totale dans l'UE
  - Reconnaissance biométrique temps réel
  - Identification émotionnelle dans le travail ou l'école
  - Scoring social

## IA Act : à partir du 2 août 2026

- Les entreprises ne pourront plus utiliser les intelligences artificielles sans se poser la question de leur conformité
- L'IA devient ainsi un véritable sujet de conformité, au même titre que les données personnelles il y a quelques temps
- La cartographie de vos systèmes doit démarrer sans attendre
  - Vous devez tenir un registre simple des usages IA
  - L'objectif n'est pas de bloquer l'innovation mais d'en prendre (reprendre) le contrôle

## A faire...

- Nommer un pilote AI Act
- Recenser les usages IA
- Créer un registre
  - Outil, fournisseur, finalité, service utilisateur, données traitées, personnes concernées, niveau de risque pressenti, obligation de transparence éventuelle, supervision humaine, preuves disponibles
- Identifier les usages sensibles (risque élevé)
  - RH, recrutement, évaluation des salariés, éducation, crédit, assurance, santé, biométrie, sécurité, accès à des services essentiels
- Préparer la transparence
  - Pour les chatbots, agents conversationnels, contenus générés ...quoi signaler, où, avec quelle formulation, dans quelle interface et avec quelle preuve
- Les contrats
- Former les équipes
  - Ethique, sens critique, créativité, interactions humaines
- Mettre en place une supervision et de la traçabilité
- Constituer un dossier de preuve

## En ce qui nous concerne...

- Identifier les traitements IA qui accèdent à l'IBM i
- S'assurer de la sécurité
  - Coté IBM i (profil utilisé)
  - Coté architecture
    - Serveur MCP ou équivalent afin de limiter les requêtes possibles (SELECT)
  - Coté IA
    - On premise ou cloud privé
    - Sinon s'assurer que les données qui remontent ne sont pas sensibles
- Mettre en place la traçabilité
  - STR-ICT pour tout ce qui est accès à la base de données
  - STR-ICT pour le fonctionnement des agents et des IA



# Merci

GAYTE Dominique – [dominique@gayte.it](mailto:dominique@gayte.it)



[info@gayte.it](mailto:info@gayte.it) - <https://i.gayte.it>