CAP CYBER 2026

AI Act, liens avec le RGPD, ISO 42001

et plein de prétextes pour discuter IA et sécurité

Frédéric Martin, Hello World

Expert Cybersécu

- PKI (Secure Elements de téléphone, HSM, cartes à puces…) et identité numérique au sens large depuis 20 ans
- Web3 / Blockchaine publique / protection des actifs numériques depuis 9 ans
- Sécurité de l'IA depuis 1 an

Militant évangéliste

- Hacking éthique
- Open Source
- Intégrité numérique

CEO de myDid (Social listening + marketing IA + activation de communautés), souverain…*

Association WallCrypt : Discussions / vulgarisations des sujets "Cryptos" et "IA"

L'AI Act vise la confiance

🛡️ Protéger

Sécurité et droits fondamentaux

🤝 Harmoniser

Un cadre commun dans l'UE

🚀 Accélérer

Favoriser l'innovation

> La confiance est la condition d'une adoption durable de l'IA.

Une régulation par le risque

Le niveau de risque détermine l'intensité des obligations imposées aux acteurs.

🚫 Risque inacceptable

On proscrit

⚠️ Risque élevé / Haut risque

On encadre fort

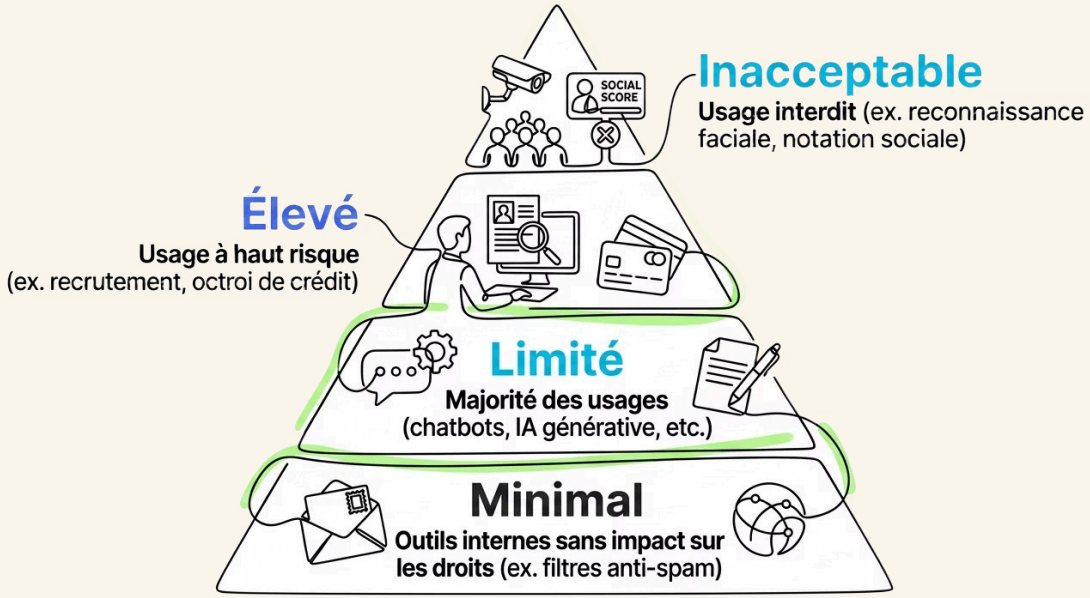
💬 Risque classique / limité

On documente et informe

✅ Risque faible

On laisse respirer

4 niveaux de risque



Attention aux capacités ajoutées aux agents (plugin / skills)

Les enjeux RH peuvent être aussi importants que ceux de l'infrastructure

L'AI Act et RGPD, sujets communs

RGPD et IA Act

- Données personnelles
- Bases juridiques
- Droits des personnes
- Devoir de documentation et d'information
- Sécurité
- Référents ?

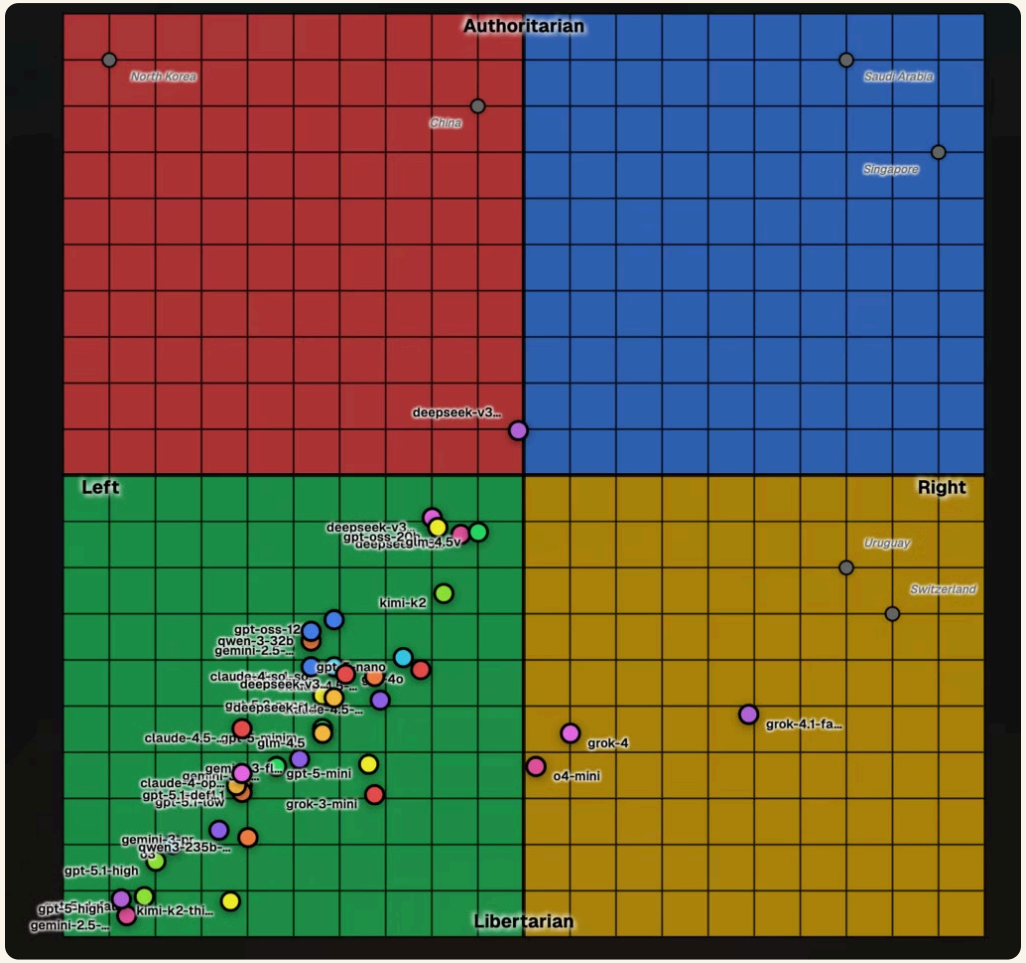
Risques communs mais aussi nouveaux

War. War Never Changes

- Risques d'intégration de nouveaux outils à un SI (leaks, dépendances, SPOF, HA…)
- Shadow IT => Shadow IA
- BYOD => BYOD + BYOIA
- Entre la chaise et le bureau (sensibilisation/formation)

"Nouveautés" AI

- Explicabilité
- Alignement (entreprise, humain, nation…)
- Sycophancy ("réponses flatteuses")
- Biais*
- Hallucinations
- Bad Buzz dans l'interaction automatisées
- Utilisation volontairement cachées
- Automatisation des navigateurs et des "bureaux" (ex: Open Claw)



Premières tentatives de différenciations des biais "politiques"

pssttt… essayez les modèles chinois quand même

Nouveaux pouvoirs pour les attaquants

- Automatisation des attaques
- Spear phishing et autres attaques personnalisées
- Scans plus intelligents
- Deep Fake / Ingénierie Sociale
- Attaquants Solo mieux organisés (agents orchestrés)
- Nouveaux outils et frameworks
- Accès à des moyens de paiements
  (traditionnels type CB, mais aussi crypto : X402*)

Il y a quelques améliorations côté défense notamment en audit de code, tests de vulns, honeypots plus intelligents, analyses comportementales…

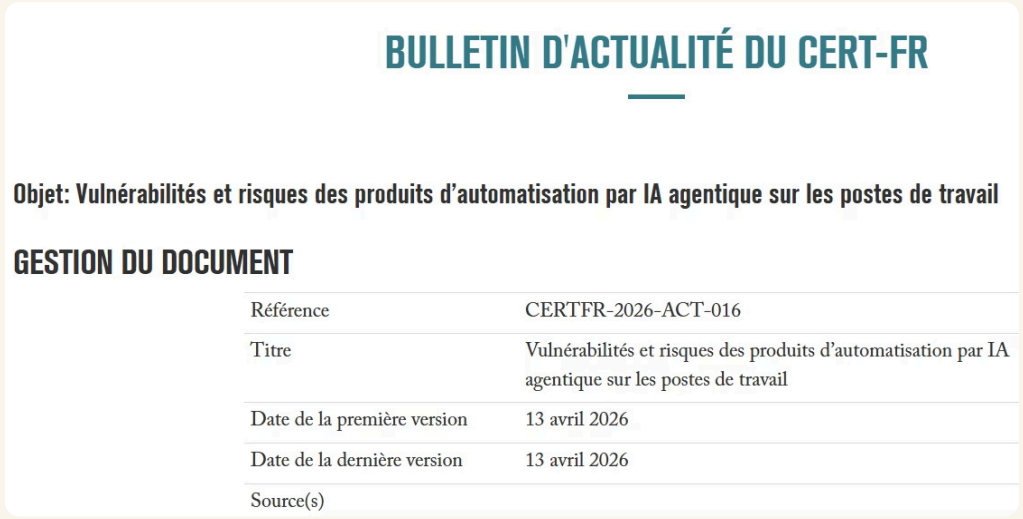
… mais l'amélioration des capacités est plutôt côté attaquants (donnez les moyens à vos RED Team pour se mettre à jour)

Nouveaux risques associés étranges…

maj, Frida…

ANSSI, CERTFR, ça bouge…

Nom trompeur (cloisonement, généralités, code source)



Enfin des mises en garde sur OpenClaw, Claude Cowork…

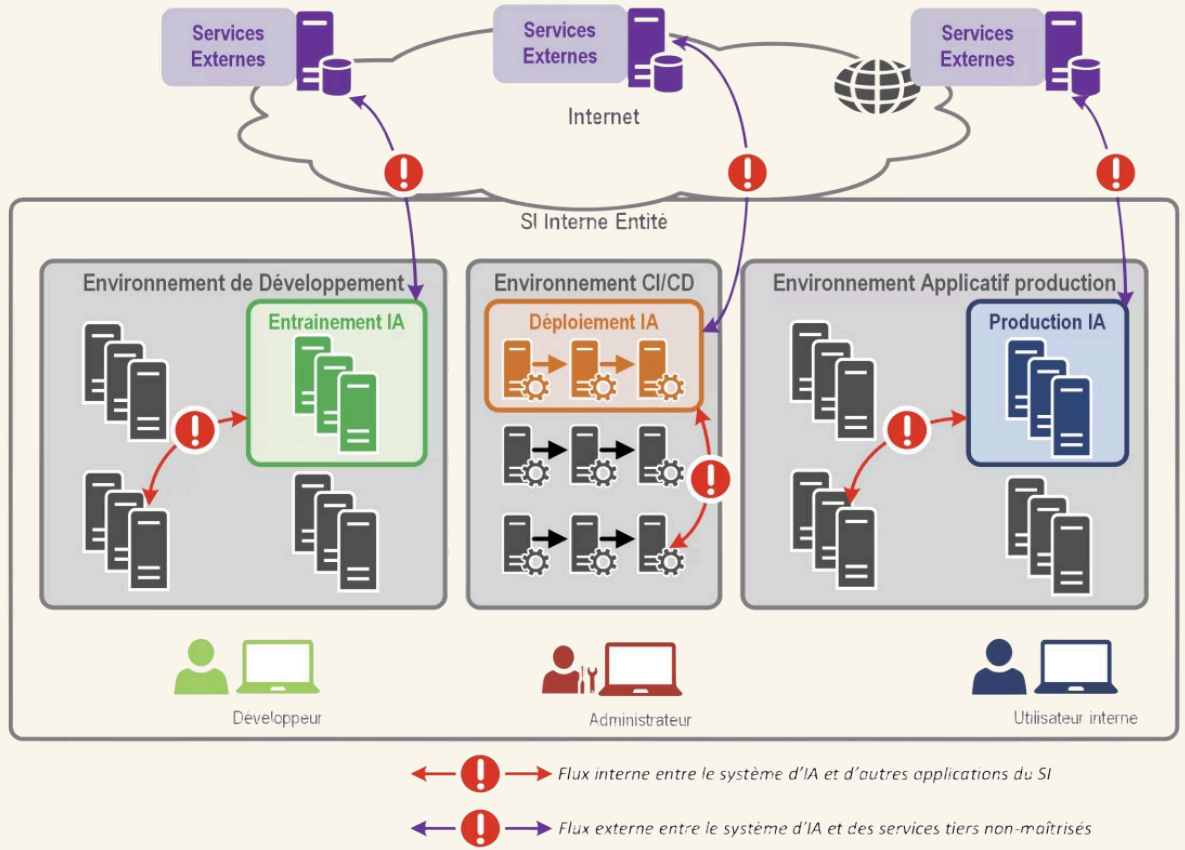


FIGURE 3 – Intégration d'un système d'IA générative dans un SI existant

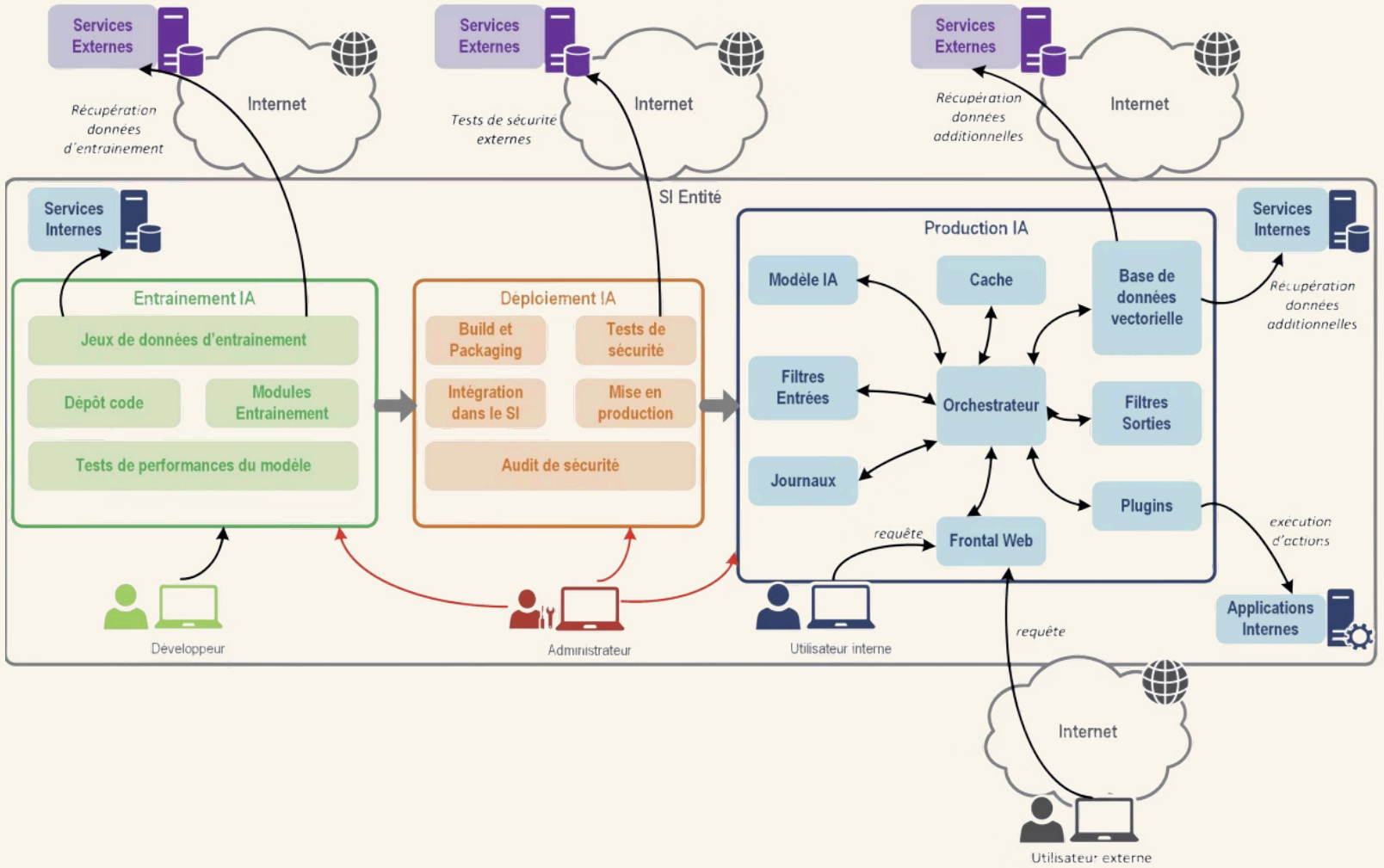


FIGURE 4 – Exemple d'architecture générique d'un système d'IA générative

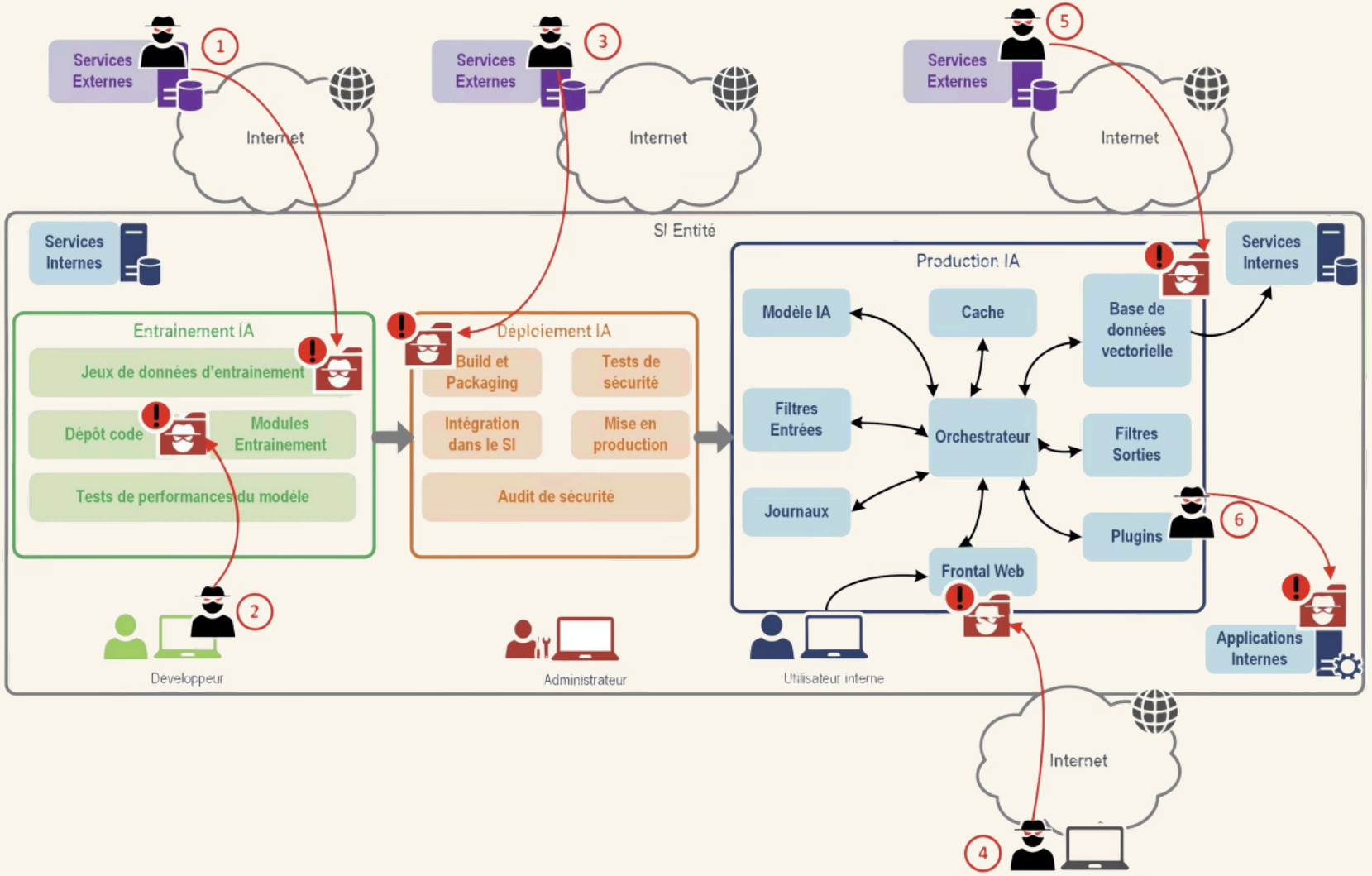


FIGURE 5 – Scénarios d'attaques sur un système d'IA générative dans un SI

Exemple d'analyses complémentaires

AIPD

Analyse d'impact relative à la protection des données

- Focalisée sur les données personnelles
- Risque pour les droits et libertés
- Base : article 35 RGPD

AIDF

Analyse d'impact sur les droits fondamentaux

- Focalisée sur les droits fondamentaux
- Biais, discrimination, accès aux droits
- Base : article 27 AI Act

Usage Perso (même avec un compte "Pro") de l'IA en entreprise : pas conforme RGPD

Risque

Données et prompts mal maîtrisés

RGPD

Transferts, contrat, information, réutilisation

Exemples

ChatGPT, Gemini, Claude en mode public

⚠ Les interfaces grand public ne sont pas adaptées par défaut à un usage entreprise sensible.

Les versions entreprise peuvent être compatibles

Conditions requises

- Contrat de sous-traitance
- Paramètres anti-réentraînement
- Gouvernance des prompts
- Encadrement des transferts

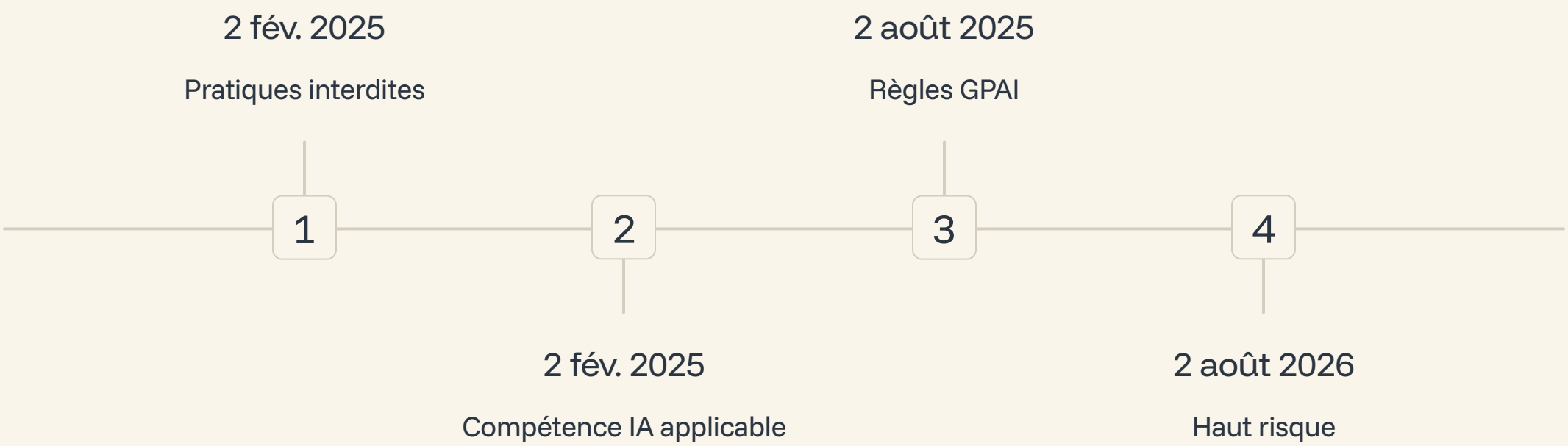
Bon réflexe

- Préférer Business / Enterprise / API
- Former les utilisateurs
- Documenter les usages
- Relire les clauses fournisseur

Les offres entreprise donnent plus de contrôle contractuel et technique.

Les dates clés pour l'entreprise

⚠ Certaines obligations sont déjà applicables.



Cartographier les usages IA

À inventorier

- Outils
- Cas d'usage
- Données
- Impacts
- Fournisseurs

Pourquoi

- Identifier l'interdit
- Qualifier le risque
- Préparer les contrats
- Attribuer les rôles
- Tracer les preuves

> Le registre d'usages est la base de la conformité.

Le rôle juridique change les contraintes

Fournisseur

Conçoit et met sur le marché le système d'IA.

Déployeur

Utilise le système en contexte professionnel.

Importateur

Fait entrer le système dans l'UE.

Distributeur

Met le système à disposition sur le marché.

Le rôle réel dépend autant du contrat que de la réalité technique.

Dans les faits, tous "déployeurs" sauf solutions "maison" / "affinées"

Ce qu'un déployeur doit démontrer

Organisation

- Usage conforme
- Contrôle humain / HITL (Human in the Loop*)
- Données d'entrée maîtrisées
- Surveillance
- Escalade incidents

Preuves

- Logs
- Critères de décision
- Tests
- Alerte fournisseur/autorités
- Suspension si risque

> Le déployeur doit démontrer la maîtrise opérationnelle du système.

Pas seulement le haut risque

Les obligations de transparence touchent souvent les cas génératifs, bien au-delà des seuls systèmes à haut risque.

💬 Interaction

Dire quand on parle à une IA — l'utilisateur doit savoir qu'il interagit avec un système automatisé.

🖼️ Contenu

Signaler le synthétique — les contenus générés par IA (images, textes, vidéos) doivent être identifiés (*abus, espoir C2PA)

⚖️ Décision

Informer selon le contexte — les personnes concernées par des décisions automatisées doivent en être informées.

Former les équipes n'est plus optionnel

Qui former

- Utilisateurs / Métiers
- Managers
- Achats et juridique
- DPO / conformité
- IT / sécurité

Sur quoi

- Capacités et limites
- Risques
- Supervision humaine
- Confidentialité
- Signalement / Escalade incidents

Risques hors sécurité

- Risque commercial (pas conforme pas vendable)
- Risque juridique
- Risque réputation / ethique
- Risque sanction (théoriquement élevée)
- Risque de dépendance / souveraineté
- Risque non alignement

Points aveugles et focus liés aux déformations professionnelles…

ISO 42001 / systèmes de management de l'IA

🏛️ Gouvernance

Politiques, objectifs, rôles — définir qui décide quoi et comment dans l'organisation.

🔄 Cycle de vie

Conception, déploiement, suivi, retrait — accompagner le système d'IA à chaque étape.

🤝 Tiers

Fournisseurs et composants externes — maîtriser les dépendances* et les risques associés.

ISO 42001 structure la gouvernance de l'IA de manière systématique et auditée.

SMSI / ISO 27001 et SMIA / ISO 42001

SMSI — ISO 27001

Système de Management de la Sécurité de l'Information

- Protège l'information
- Confidentialité, intégrité, disponibilité
- Risque cyber et sécurité globale
- Applicable à tous les actifs informationnels

SMIA — ISO 42001

Système de Management de l'Intelligence Artificielle

- Gouverne les systèmes d'IA
- Biais, explicabilité, supervision humaine
- Cycle de vie, impacts, responsabilité
- Applicable aux usages IA et GPAI

> 27001 donne le socle sécurité, 42001 ajoute la couche gouvernance IA.

Trois niveaux de formations ISO/IEC 42001

Foundation

Comprendre les principes, le vocabulaire et les exigences du standard ISO 42001.

Lead Implementer

Mettre en place, piloter et améliorer un système de management de l'IA au sein de l'organisation.

Lead Auditor

Auditer la conformité et préparer ou conduire les audits de certification ISO 42001.

🧭 Question légitime : Combien ?!

A peu près partout pareil : Fondation, c'est 2j soit 2K€ et chacun des deux autres, c'est 5j soit 5K€

🧭 Feuille de route

01

Registre des usages*

Inventorier tous les outils, cas d'usage, données, impacts et fournisseurs IA de l'organisation.

02

Tri des risques

Qualifier chaque usage selon les quatre niveaux de l'AI Act et prioriser les actions correctives.

03

Contrats, tests, logs

Sécuriser les relations fournisseurs, mettre en place les tests de robustesse et tracer les preuves.

04

Formation et gouvernance

Former les équipes, attribuer les rôles et structurer la gouvernance IA selon ISO 42001.

*cheatcode ''Finops'' pour démarrer

Conclusion

une IA de confiance…
à encadrer avec la culture Cyber habituelle
mais attention aux spécificités