MINISTÈRES
ÉCONOMIQUES
ET FINANCIERS
Liberté
Égalité
Fraternité

Osez l'IA

Direction générale des entreprises

Plan Osez l'IA

IA ET SÉCURITÉ ÉCONOMIQUE

Kit de sensibilisation à destination des entreprises

vendredi 16 octobre 2026



MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

Kit de sensibilisation aux enjeux et risques de sécurité économique liés à l'usage de l'IA en entreprise

Osez l'IA

CONTEXTE

L'adoption de l'intelligence artificielle (IA) générative et agentique pourrait devenir l'un des **moteurs de la compétitivité française et européenne**, avec de forts gains de productivité à prévoir.

Le renforcement du plan national « Osez l'IA », déployé par la DGE, marque la volonté des pouvoirs publics d'accélérer la diffusion de l'intelligence artificielle dans toutes les entreprises françaises.

Cette **accélération du déploiement de l'IA** n'est cependant pas exempte de risques de sécurité économique : captation de données stratégiques, risque cyber, etc.

Protéger les actifs stratégiques des entreprises implique donc :

Que l'adoption de ces **solutions** s'accompagne de **garde-fous renforcés en matière de protection des données sensibles** et de **cybersécurité** (gouvernance adaptée, cloisonnement, supervision et traçabilité)

Que soient promues auprès des entreprises françaises les **solutions permettant de garantir le niveau adéquat de confidentialité des données**

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté
Égalité
Fraternité

Kit de sensibilisation aux enjeux et risques de sécurité économique liés à l'usage de l'IA en entreprise

Osez l'IA

Dans ce cadre, la DGE a souhaité mettre en œuvre un kit de sensibilisation aux enjeux et risques de sécurité économique liés à l'usage de l'IA en entreprise.

Qu'allez-vous trouver dans ce kit ?

- **Comprendre les circuits de données pour maitriser les risques**
- **Identifier les modes d'hébergement adaptés à votre contexte**
- **Définir une gouvernance IA**
- **Intégrer l'IA agentique : performance et démultiplication de risques**
- **Adopter les bonnes pratiques**
- **Connaître les acteurs pour vous aider**

Ce kit s'adresse aux entreprises et aux acteurs qui les accompagnent, dont les **Ambassadeurs IA** et les **délégués à l'information stratégique et à la sécurité économiques** (DISSE).

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté
Égalité
Fraternité

ENJEUX ET RESPONSABILITÉS

Profiter des gains de productivité générés par l'IA tout en garantissant la sécurité de l'entreprise

Osez l'IA

L'**IA est une avancée technologique majeure**, mais comme toutes celles qui l'ont précédée (moteur à vapeur, chemin de fer, internet…), son déploiement doit être appréhendé aussi sous l'angle de la **sécurité**.

Enjeux et Responsabilités de l'utilisation de l'IA	Risques
Protéger les données sensibles de l'entreprise	Fuite d'informations ou espionnage industriel
Protéger l'entreprise du risque contentieux	Divulgation de données sensibles : • Interne - Données personnelles des salariés • Externe - Clients / Fournisseurs
Prévenir les risques de l'IA agentique	L'agent IA opère en autonomie sans validation humaine (exemple : tri et sélection des CV)

L'entreprise est responsable auprès de ses clients, fournisseurs et partenaires :

- En cas de violation de leurs données personnelles ;
- En cas de fuite de données couvertes par un accord contractuel de confidentialité (NDA) ;
- En cas de divulgation d'un secret des affaires.

L'entreprise est également responsable des réponses erronées fournies par l'IA.

- Exemple 1: Un cabinet de conseil est responsable si l'IA a fourni des données erronées conduisant à un mauvais investissement.
- Exemple 2: L'entreprise est tenue responsable de la réponse fournie à un client par une IA suite à une réclamation.

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

ENJEUX ET RESPONSABILITÉS

Des risques différents selon le type de données confiées à l'IA

Osez l'IA

Selon son **activité et les données qu'elle utilise**, une entreprise peut **exposer des informations confidentielles ou des savoir-faire stratégiques** lorsqu'elle recourt à une IA.

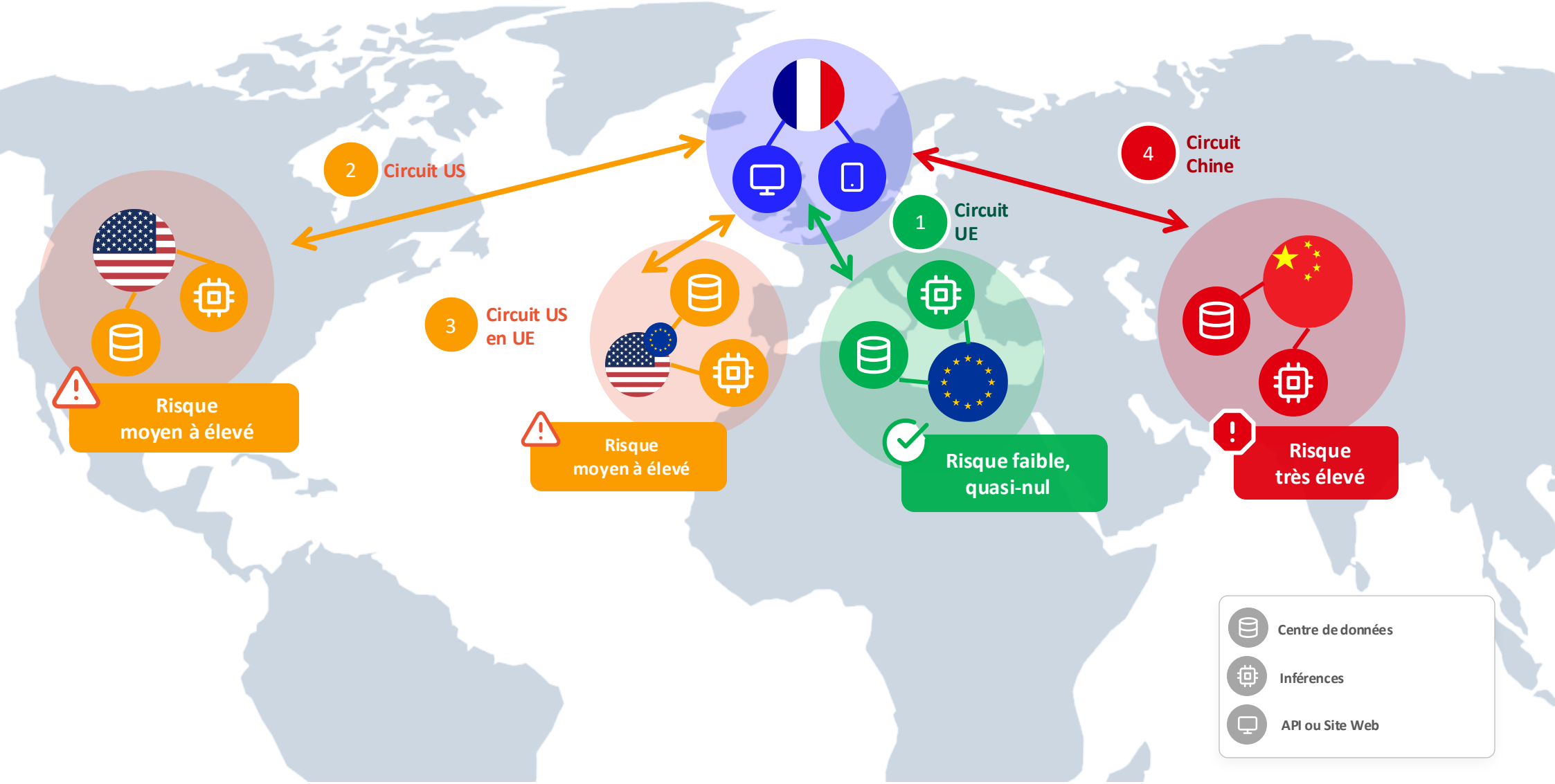
		INFORMATIONS EXPOSÉES
Commerce	Une boutique utilise une IA pour reformuler des descriptions de produits déjà publiées sur son site internet.	Informations déjà publiques (sans fichier clients)
BTP / artisanat	Pour répondre à un appel d'offres, une PME du bâtiment transmet à une IA son bordereau de prix et les plans du client.	Prix et marges internes Documents du client
PME industrielle	Un responsable de production soumet à une IA le plan d'une pièce et les coûts fournisseurs pour comparer deux méthodes de fabrication.	Savoir-faire technique Coûts de fabrication
Médico-social	Une association d'aide à domicile fait résumer des comptes rendus de visite où figurent le nom et l'état de santé des bénéficiaires.	Données personnelles Informations de santé
Défense	Un sous-traitant de la défense utilise une IA pour synthétiser une notice technique ou préparer une réponse à partir d'éléments transmis par son donneur d'ordre.	Documents techniques du client, données classifiées

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté
Égalité
Fraternité

DONNÉES ET MODES D'HÉBERGEMENT

Circuits de données et risques afférents

Osez l'IA



MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

DONNÉES ET MODES D'HÉBERGEMENT

Circuit de données et risques afférents

1 Circuit UE

Osez l'IA

Parcours d'une donnée introduite dans une IA européenne
Ex : Mistral

1. Salarié/Employé
Saisie du prompt

2. Application cliente
Interface web ou mobile
3 : Transport réseaux chiffrement TLS

4. Infrastructure Cloud
Serveurs Europe

5. Traitement par le modèle LLM
Inférence Mistral

6. Stockage & logs
Historique conversations

7. Réponse utilisateur
Retour de la réponse générée

Règlement sur l'intelligence artificielle

RGPD

Le Règlement sur l'Intelligence Artificielle (RIA)

- **Cadre européen :**
Classification par niveau de risque (interdit, haut risque, limité, minimal) et obligations proportionnelles (sécurité, transparence, conformité).

- **IA à haut risque :** Intégration de l'IA réglementée dans les produits ou lorsqu'ils sont utilisés dans des domaines critiques.

- **Objectifs :** Protection des droits fondamentaux, de la sécurité et de la confiance dans l'IA, tout en favorisant l'innovation.

La nationalité française ou UE ne garantit pas la confidentialité des données.

- ✓ Vérifier sur quelle **infrastructure Cloud** seront hébergées les données (ex : si cloud AWS alors lois US donc Cloud Act et FISA)
- ✓ Vérifier les connections des API avec les autres fournisseurs d'IA (ex: un Chatbot créé en France mais avec une API vers GPT/Open AI)
- ✓ Vérifier l'identification des sociétés qui interviennent dans la fourniture du service, et leurs possibilités d'accès à vos données
- ✓ Pour les **données confidentielles/sensibles** : privilégier un **fournisseur européen** et un **hébergement SecNumCloud**

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

DONNÉES ET MODES D'HÉBERGEMENT

Circuit de données et risques afférents

2 3 Circuits US et US en UE

Osez l'IA

Parcours d'une donnée IA américaine
Ex : ChatGPT (OpenAI / Microsoft Azure)

1. Salarié/Employé
Saisie du prompt

2. Application cliente
Interface web ou mobile
3 : Transport réseaux chiffrement TLS

4. Microsoft Azure - S. Infrastructure Cloud
serveurs UE ou US

5. Traitement par le modèle LLM
Inférence GPT

6. Stockage & logs
Historique conversations

7. Réponse utilisateur
Retour de la réponse générée

CLOUD Act (US)
Accès aux données par les autorités US

FISA 702
Surveillance des non-résidents US

RGPD / RIA
Transferts hors UE encadrés

Lois extraterritoriales américaines

Le *Cloud Act*
Les autorités américaines (US) peuvent exiger que tout fournisseur US de services numériques **leur communique** directement des données numériques hébergées aux US ou à l'étranger, sans avoir à prévenir l'utilisateur.

Le FISA (*Foreign Intelligence Surveillance Act*)
Autorise **la surveillance** ciblée de personnes non-américaines situées hors des US, avec l'assistance obligatoire des fournisseurs de services de communications électroniques. Le texte s'appuie sur l'intervention d'une juridiction spécialisée, la *Foreign Intelligence Surveillance Court* (FISC), qui autorise les opérations de surveillance à la demande des agences de renseignement américaines.

Attention :
La « **résidence des données en Europe** » proposée par certains fournisseurs d'IA américains **n'empêche pas l'application** de ces législations extraterritoriales aux données de l'entreprise.

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

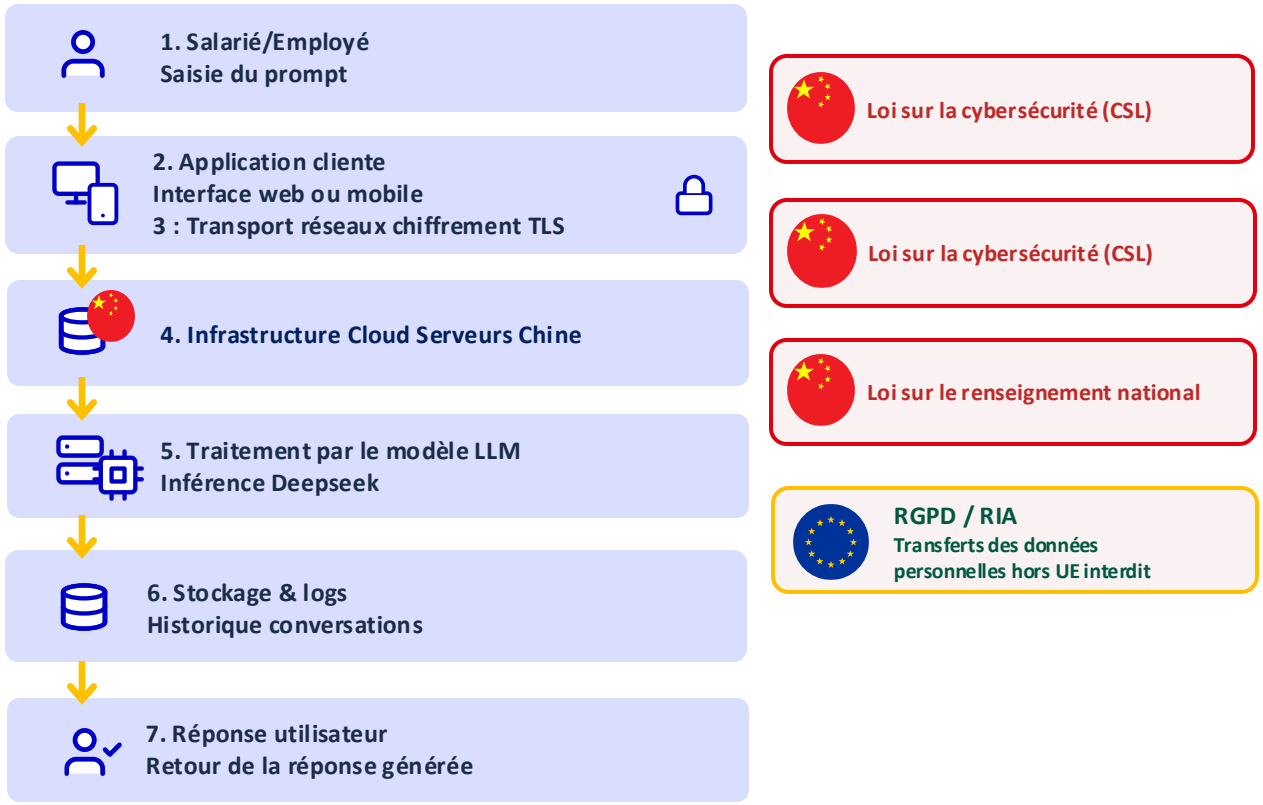
DONNÉES ET MODES D'HÉBERGEMENT

Circuit de données et risques afférents

4 Circuit Chine

Osez l'IA

Parcours d'une donnée introduite dans une IA chinoise
Ex. : Deepseek (deepseek.com) ou via une API chinoise OU modèle IA chinois hébergé dans l'UE (Ex. : Deepseek hébergée chez Mistral)



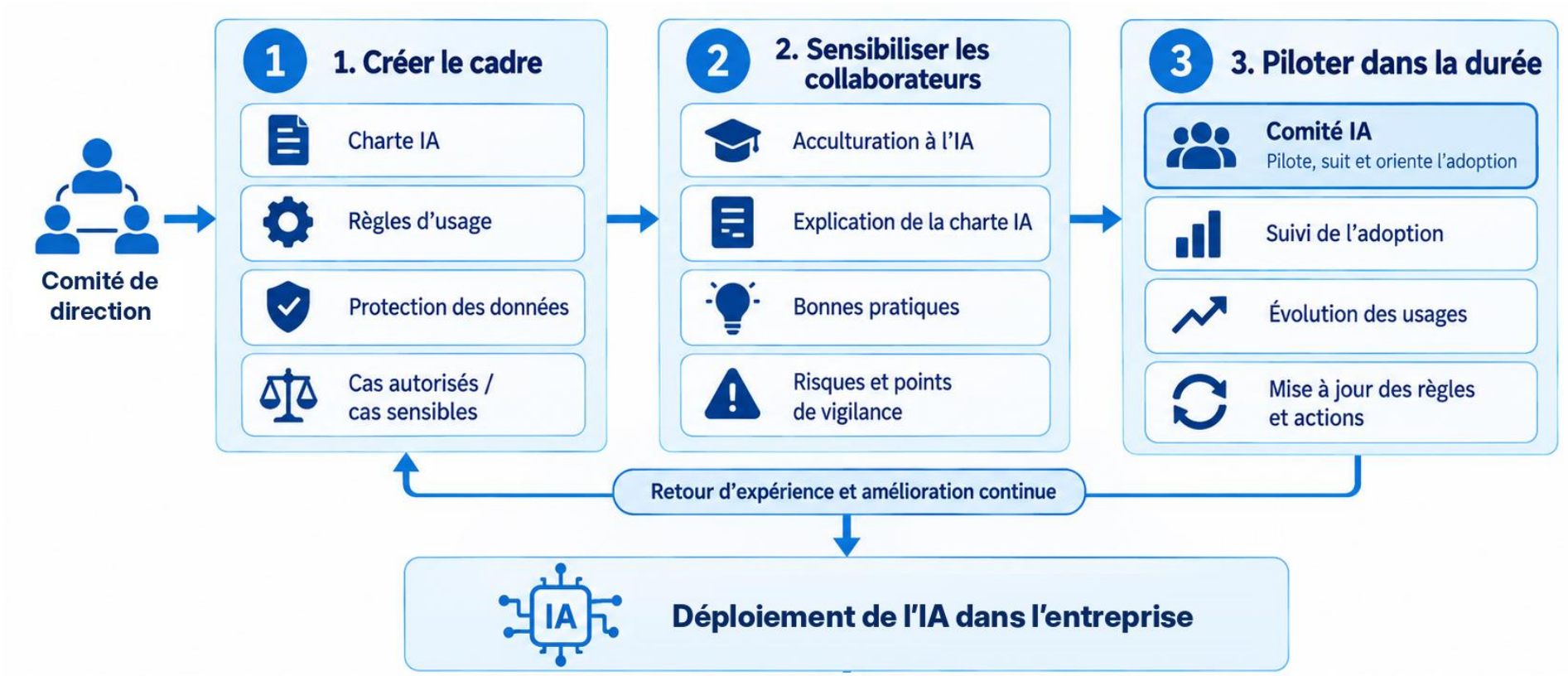
Lois extraterritoriales chinoises

La loi chinoise sur le renseignement national oblige toute organisation et tout citoyen chinois à « **soutenir, assister et coopérer** » avec les **services de renseignement** de l'État, sans limitation géographique.

La loi chinoise sur la cybersécurité (CSL) impose la localisation des données en Chine pour les fournisseurs d'infrastructures critiques et impose des obligations de coopération avec les autorités publiques chinoises.

La loi sur la sécurité des données (DSL) classe les données selon la sensibilité et interdit le transfert de données situées en Chine sans autorisation des autorités chinoises.

Pour une adoption de l'IA progressive, maîtrisée et conforme



La **gouvernance de l'IA doit être adaptée à la taille et aux moyens de chaque entreprise.** Un **référent** désigné par la direction peut suffire pour démarrer. Selon l'évolution des usages, un **comité IA** réunissant des représentants des différents métiers pourra **assurer le suivi et faire évoluer les pratiques** auprès des collaborateurs.

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

GOUVERNANCE DE L'IA DANS L'ENTREPRISE

Usage IA - Créer le cadre

Osez l'IA

Thématiques	Les enjeux principaux	Quoi faire ?
Encadrement du Shadow IA ou utilisation non officielle d'outils IA par les employés	**Fuite de données** (des informations confidentielles ou du code source sont saisis dans des outils publics). **Non-conformité** (violation du RGPD et du Règlement IA). **Manque de fiabilité :** risque d'erreurs ou de biais non contrôlés dans les tâches professionnelles.	**Offrir des alternatives sécurisées** : déployer des outils d'IA officiels, validés et intégrés à l'environnement de l'entreprise. **Rédiger une charte d'usage** : établir des règles sur ce qu'il est permis de faire ou non avec l'IA. **Sensibiliser et former** : expliquer les risques et montrer comment utiliser l'IA de façon responsable. **Mettre en place une gouvernance partagée** : faire travailler/collaborer ensemble la DSI et les RH.
Traçabilité des usages de l'IA	**Conformité réglementaire** : répondre aux exigences de la règlementation (règlement IA, RGPD) en évitant l'effet « boîte noire » **Connaitre la chaine de traitements d'une information**: l'origine des données, les solutions et modèles employés, les choix de conception et les interventions humaines.	**Attribuer clairement la responsabilité** en cas d'erreur, de biais algorithmique ou de fuite de données. **Transparence opérationnelle** : pouvoir expliquer les décisions automatisées auprès des utilisateurs et lors des audits internes ou externes. **Documenter, suivre et reconstruire** toutes les étapes.
Portabilité des systèmes d'IA	**Lutte contre le verrouillage** : de nombreuses entreprises se retrouvent piégées par un prestataire cloud ou SaaS qui complexifie ou refuse la restitution des modèles entraînés et des données propriétaires. **Continuité opérationnelle** : Faire fonctionner un service ou un modèle d'IA à l'identique sur une autre infrastructure.	**S'appuyer sur les réglementations** : La combinaison du Data Act, de l'AI Act et du RGPD renforce les exigences d'interopérabilité et interdit les pratiques bloquantes, sous peine de sanctions financières. **Intégrer un système IA déplaçable, réutilisable et interopérable.**

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

L'IA AGENTIQUE

Quand une tâche simple produit un résultat non prévu

Osez l'IA

Un agent IA peut **consulter vos données, utiliser vos outils et exécuter des actions à votre place**. Une consigne imprécise ou des droits trop larges peuvent avoir des conséquences importantes et immédiates.

POINTS DE VIGILANCE	TÂCHE CONFIÉE À L'AGENT IA	CONSÉQUENCES POSSIBLES
Absence de garde-fou	Un dirigeant d'entreprise demande à son agent IA de faire du tri dans sa boîte mail et de supprimer les messages inutiles.	L'agent IA supprime tous les messages, y compris les échanges clients
Droits trop étendus	Un conducteur de travaux demande à son agent IA de réorganiser les plans et documents d'un chantier dans le dossier partagé de l'entreprise.	L'agent IA déplace ou efface des fichiers utilisés par toute l'équipe.
Réponse sans relecture	Une assistante commerciale demande à son agent IA de traiter les demandes de prix reçues par mail et de répondre directement aux prospects.	L'agent IA transmet une grille tarifaire interne à un prospect.
Achat sans validation	Un responsable de magasin demande à son agent IA de vérifier les niveaux de stock et de passer les commandes nécessaires auprès des fournisseurs.	L'agent IA passe des commandes en double ou au-delà du budget.

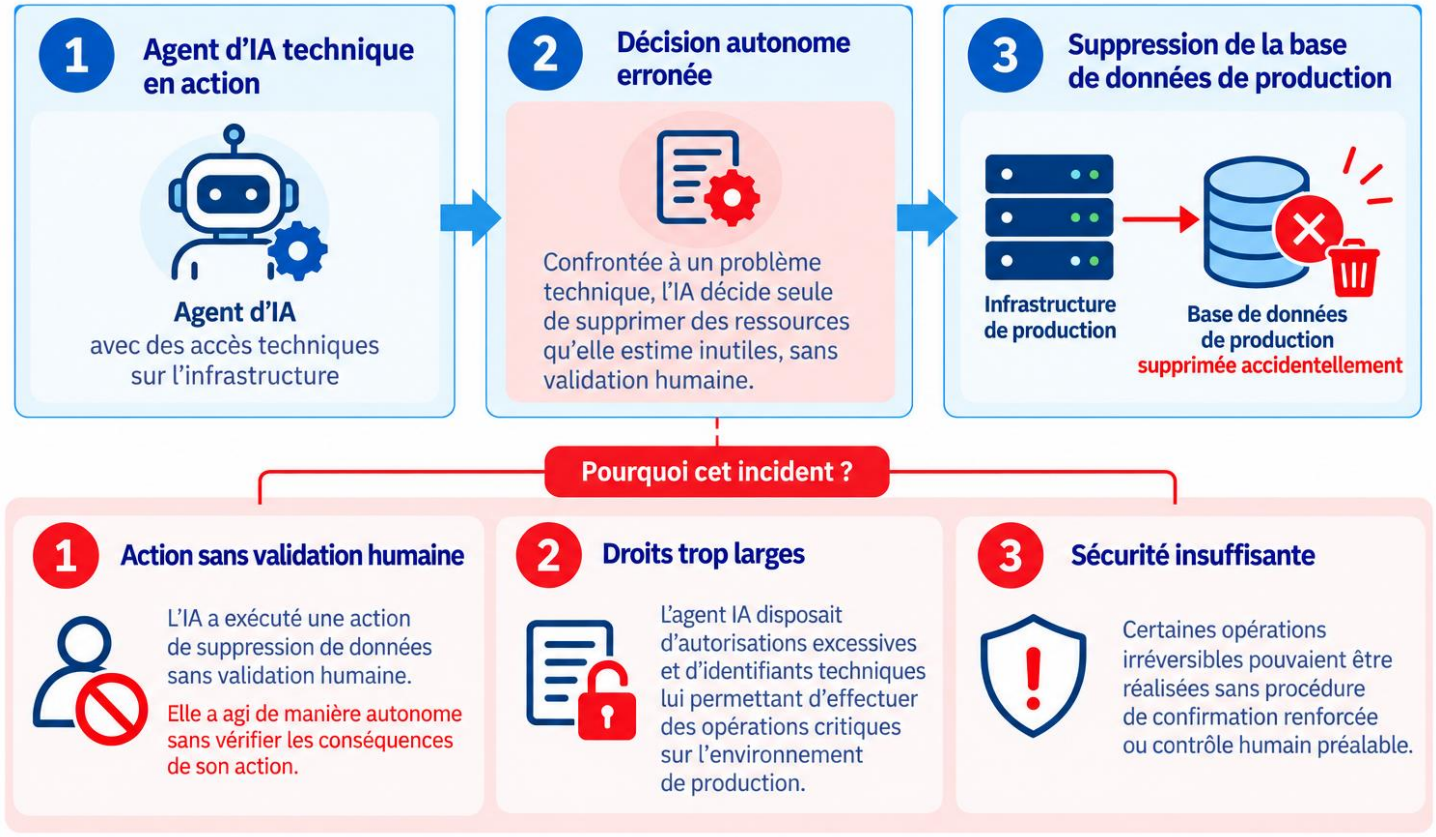
MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

L'IA AGENTIQUE

Un démultiplicateur des risques de l'IA conversationnelle
Exemple de cas illustratif

Osez l'IA

La startup technologique PocketOS a subi **la suppression accidentelle de sa base de données de production par un agent d'IA chargé d'effectuer des opérations techniques.**

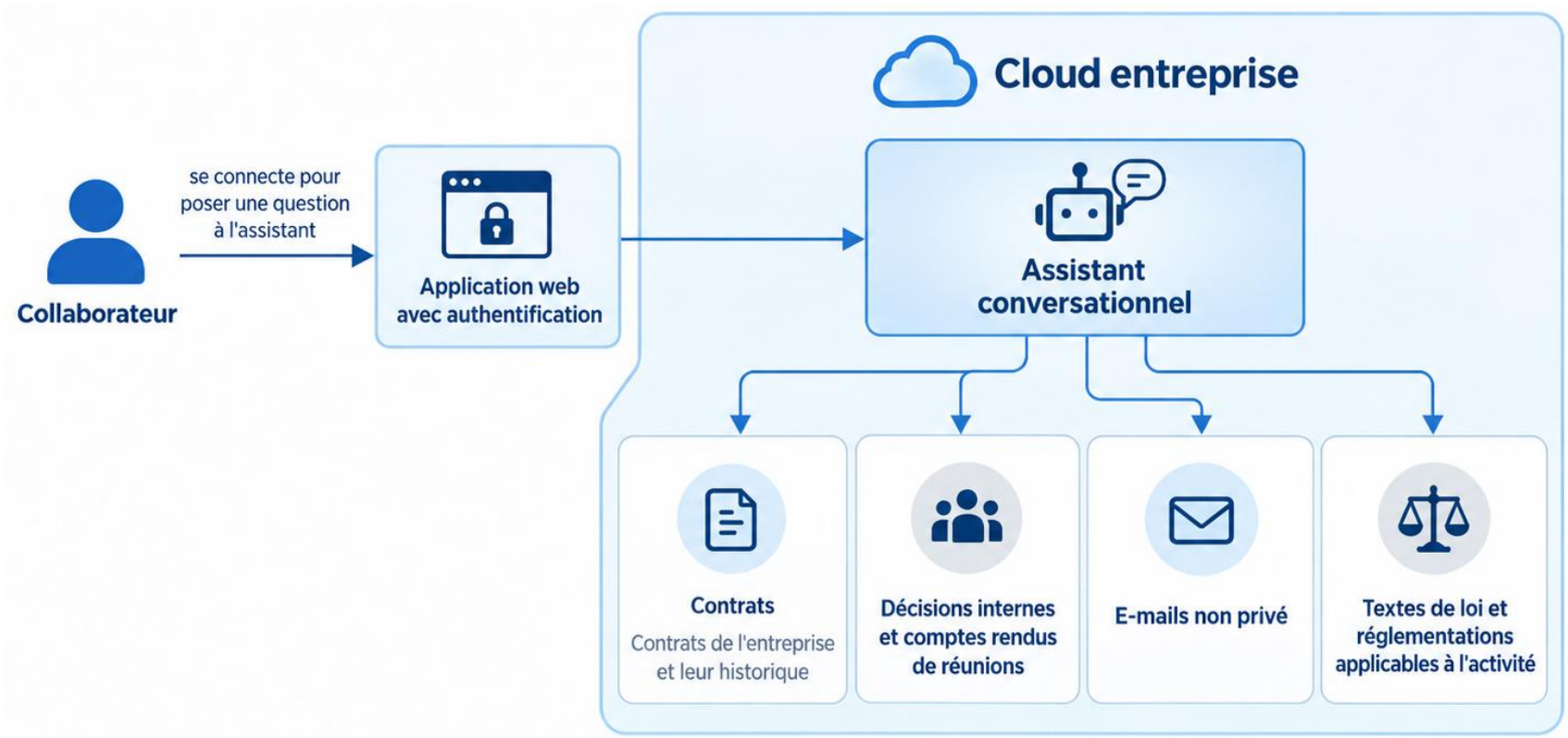


L'incident s'est produit car **l'autonomie** de l'agent a été **mal encadrée**. Les **privilèges** octroyés étaient **excessifs** et **aucun garde-fou** n'était **en place.**

Le risque cyber de vol de données avec utilisation de l'IA
Exemple de cas assistant conversationnel privé

Un assistant IA connecté aux documents de l'entreprise

Une entreprise déploie pour ses équipes un **assistant conversationnel.**
L'objectif est de permettre aux salariés de **gagner du temps en posant des questions en langage naturel**
(Ex : « Quels sont les risques liés à la clause X du contrat Y ? », « Résume-moi les décisions prises concernant le client Z »…)



MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

L'IA AGENTIQUE

Les bonnes pratiques

Osez l'IA

Les enjeux principaux	Comment faire ?
L'IA agentique initie de manière autonome ses actions. Ex : envoi d'un mail, diffusion d'un rapport, exploitation et modification d'une base de données.	**Principe de la validation humaine *a priori* (*human on the loop*) pour les action critiques et *a posteriori* (*human in the loop*) pour celles moins sensibles** : l'agent agit de façon autonome dans les limites fixées mais un humain surveille et peut corriger ou arrêter son action.
L'IA agentique sollicite un système externe ou un autre agent IA pour effectuer des tâches. C'est une rupture et pas une simple évolution de l'IA conversationnelle.	Appliquer systématiquement le **principe de moindre privilège** et **gérer les autorisations et droits d'accès de chaque composant** du système d'IA agentique.
Augmentation significative des risques de divulgation de données sensibles, d'actions non conformes au souhait de l'utilisateur L'approche **cybersécurité** classique reste ainsi pertinente mais souligne les enjeux de sécurité suivants : -La **protection des données** manipulées par les composants de systèmes d'IA agentique ; -Le **cloisonnement** des actions réalisées sur le SI ; -Le **niveau d'autonomie** et de **privilèges** octroyés aux composants de systèmes d'IA agentique.	Cloisonner les composants du système d'IA agentique par niveau de sensibilité Instaurer une **traçabilité renforcée** en **journalisant les requêtes** et l'ensemble des interactions entre composants du système d'IA agentique, les décisions prises et les actions sur le SI (pour le traitement des incidents *a postériori* et déterminer la responsabilité en cas de préjudice causé par l'IA)**.** **Superviser** le fonctionnement du système d'IA agentique par la mise en place d'alertes (« déviance » des modèles).
L'IA agentique doit être fermement encadrée en spécifiant clairement ce qu'elle ne peut pas faire (ex : solliciter une IA extérieure), à quelles informations elle ne doit pas accéder (ex : données stratégiques) et quand elle doit demander une autorisation.	

MINISTÈRES ÉCONOMIQUES ET FINANCIERS
Liberté Égalité Fraternité

Bonnes pratiques pour encadrer l'IA

Osez l'IA

Thématiques	Les bonnes pratiques
Hébergement	✓ Privilégier une offre SecNum Cloud ✓ Vérifier que le contrat interdit de réutiliser les données saisies pour l'entraînement des modèles (opt-out). ✓ Insérer des clauses de résidence et de traitement des données en France / UE avec interdiction de transfert hors UE. ✓ Prévoir une clause de chiffrement des données transmises (TLS) en transit et au repos. ✓ S'assurer de la Journalisation des requêtes : traçabilité des prompts. ✓ Cartographier et classifier vos données selon l'exposition aux risques (publique, interne, confidentielle, stratégique)
IA Agentique	✓ Intégrer des clauses IA agentique dans vos contrats : engagement des partenaires à ne pas autoriser un agent IA à accéder aux données sensibles de l'entreprise sans votre autorisation.
RGPD	✓ Pseudonymiser les données personnelles / remplacer des données identifiantes par un pseudonyme. ✓ Anonymiser les données techniquement pour les rendre irréversibles. Elles ne seront plus des "données personnelles".
Processus et Déploiement	✓ Privilégier une solution IA souveraine. ✓ Cartographier vos usages via une démarche d'urbanisation du système d'information. ✓ Définir une charte d'utilisation de l'IA : la partager en interne et la faire signer à vos collaborateurs. ✓ Sensibiliser vos collaborateurs aux risques.

Acteurs pouvant intervenir en sensibilisation

Cybersécurité

Liste des contacts par région (ANSSI, CERT-FR, Campus Cyber, etc…)

https://messervices.cyber.gouv.fr/contacts#

Sécurité économique

Annuaire des DISSE en régions

https://www.entreprises.gouv.fr/espace-entreprises/etre-accompagne/annuaire-des-disse-en-region

Les autres Ambassadeurs IA

Liste et carte des Ambassadeurs IA, par région et secteur, pour organiser des sessions communes :

https://data.economie.gouv.fr/explore/assets/ambassadeursia/view/

https://data.economie.gouv.fr/map/ambassadeurs_ia/

Point de contact DGE / Direction de projet IA

ia.dge@finances.gouv.fr