ITEANU
Société d'Avocats | Law Office

IA & Société :
Le coût réel de la Souveraineté

Cloud Act, RGPD et dépendance juridique

Alexandra ITEANU, Avocate responsable du pôle Data, RGPD et IA au sein du Cabinet ITEANU AVOCATS

Aix-Marseille Université

27 JANVIER 2026 – Journée CEDRE

SOMMAIRE

Iteanu Avocats – https://www.iteanu.law/ – @iteanu – contat@iteanu.law

01.

IA ET SOUVERAINETÉ NUMÉRIQUE

Les définitions (IA et souveraineté slide 5)

Définition d'un système d'IA : art. 3 du règlement (UE) 2024/1689 du 13 juin 2024 pour l'utilisation de l'intelligence artificielle au sein de l'Union européenne (AI Act).

(1) un système basé sur une machine qui est conçu pour fonctionner avec différents niveaux d'autonomie et qui peut faire preuve d'adaptabilité après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des données qu'il reçoit, comment générer des résultats tels que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer des environnements physiques ou virtuels.

La non-définition légale de la souveraineté numérique :

LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique (LREN) – art. 29 :

Le Gouvernement remet au Parlement, dans un délai de trois mois à compter de la promulgation de la présente loi, un rapport sur la possibilité de créer un ***Commissariat à la souveraineté numérique*** *rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège.* [...]

Rapport de la commission d'enquête du Sénat sur la souveraineté numérique, 2019

« *La capacité de l'État à agir dans le cyberespace* », ce qui est une « *condition nécessaire à la préservation de nos valeurs* », impliquant, d'une part, « *une capacité autonome d'appréciation, de décision et d'action dans le cyberespace* » et, d'autre part, la maîtrise de *« nos réseaux, nos communications électroniques et nos données »*.

La non-définition (légale) de la souveraineté numérique

Commission européenne , *Cloud Sovereignty Framework*, Oct. 2025 :

Objectif – « Data & AI Sovereignty »:

"*Data & AI sovereignty focuses on the protection, control, and independence of data assets and AI services within the EU. It addresses how data is secured, where it is processed, and the degree of autonomy customers retain over AI capabilities*"

$$\text{Sovereignty Score} = \sum_{n=1}^{8} \left(\frac{\text{Score}(\text{SOV}_n)}{\text{Max.Score}(\text{SOV}_n)} \times \text{Weight}(\text{SOV}_n) \right) \%$$

Evaluation du niveau de souveraineté numérique – Sovereignty Effectiveness Assurance Level (SEAL)

SEAL -4 : Full Digital Sovereignty:

Technology and operations under complete EU control, subject only to EU law, with no critical non-EU dependencies.

SEAL -0: No Digital Sovereignty:

Service, technology or operations under exclusive control of non-EU third parties, governed entirely in non-EU jurisdictions.

02.

IA et protection des données à caractère personnel

IA & protection des données : le cadre juridique

Deux règlements complémentaires :

Règlement (UE) 2016/679 du 27 avril 2016 (RGPD)

- S'applique à tout traitement de données à caractère personnel dans l'UE ou ciblant des personnes dans l'UE
- Donnée à caractère personnel (art. 4 RGPD) = toute information permettant d'identifier directement ou indirectement une personne physique
- Objectifs : protection des droits fondamentaux des personnes, minimisation et licéité du traitement, transparence et responsabilisation des acteurs

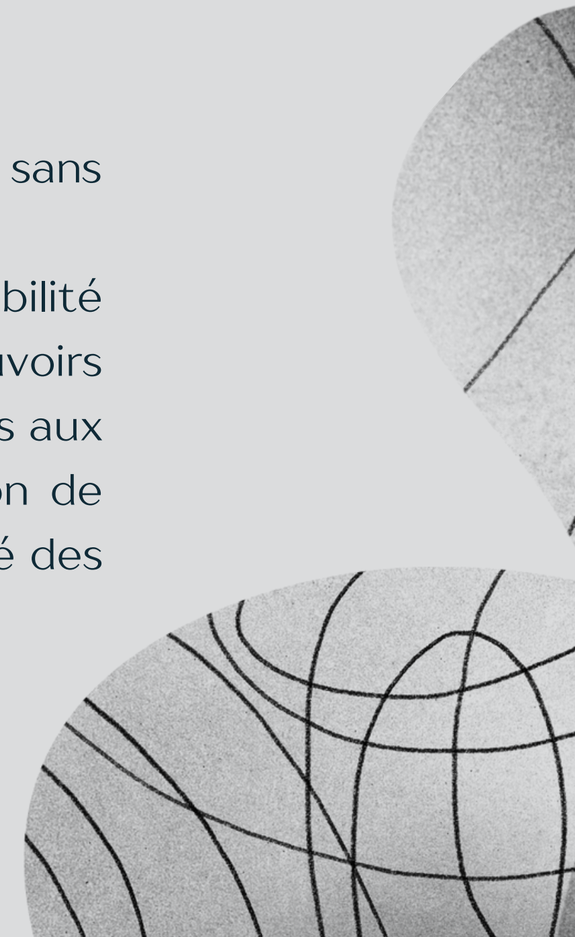
Règlement (UE) 2024/1689 du 13 juin 2024 (AI Act)

- Couvre le développement, la mise sur le marché ou le déploiement de systèmes et modèles d'IA
- Approche par niveau de risque, avec des obligations proportionnées
- Objectifs : encadrer de manière éthique et responsable le développement et l'utilisation de l'intelligence artificielle, en protégeant les droits fondamentaux des personnes et en garantissant le respect du RGPD

Publications de la CNIL : « Recommandations pour accompagner une innovation responsable », guide d'auto-évaluation pour les systèmes d'IA, fiches pratiques, etc.

IA et droit à l'oubli (art. 17 RGPD)

- **Difficulté technique d'isoler les données** : certains systèmes d'IA absorbent des volumes massifs de données non structurées : difficiles à tracer, récupérer ou supprimer de manière identifiable.
- **Risque d'effacement partiel** : même si un éditeur propose une procédure d'effacement, il n'existe aucune garantie que les données aient disparu des paramètres du modèle.
- **Limites des solutions proposées par la CNIL** :
    - *machine unlearning* (réentraînemen) : coûteux, difficile à mettre en œuvre,
    - *output filtering* (filtrage des données de sortie) : empêche certaines restitutions sans effacer les données internes.
- **Pistes : « réarmer » juridiquement ce droit**, en imposant des exigences minimales de traçabilité des jeux de données et des capacités d'*unlearning* vérifiables ; en renforçant les pouvoirs d'enquête et de sanction des autorités de contrôle et des juges, spécifiquement adaptés aux LLM ; et en mettant à la charge des fournisseurs de modèles une véritable obligation de preuve, permettant aux personnes concernées et aux autorités de constater l'effectivité des effacements réalisés.



« Existe-t-il un droit à l'oubli avec Chat GPT ? », A. Iteanu, *Solutions Numériques & Cybersécurité,* 19 nov. 2025

03.

IA, ingérence étatique et dépendance juridique

Ingérence et dépendance

Focus sur le Cloud Act (Clarifying Lawful Overseas Use of Data Act , 2018)

- Accès aux données par les autorités de contrôle et d'enquête américaines dans le cadre d'une enquête criminelle : impose aux sociétés américaines (et leurs filiales contrôlées) de remettre tout contenu demandé par un juge, **indépendamment de la localisation du serveur** et sans que la personne concernée ou que son pays de résidence ne soient informés.

  → **Risque important** : les données hébergées en Europe peuvent être accessibles aux autorités américaines.

Illustration avec le Health Data Hub

- **Plateforme des données de santé**, créée par en 2019 pour faciliter le partage des données de santé, issues de sources très variées afin de favoriser la recherche.
- **Hébergement** : Microsoft Ireland (UE certes, mais Société-mère aux Etats-Unis)
  - Risques de transfert ou d'accès par les autorités américaines au regard du RGPD
  - CE, ord. de référé n° 444937 du 13 octobre 2020 : le Conseil d'État a décidé de ne pas suspendre le fonctionnement du Health Data Hub — mais a souligné l'existence d'un risque réel de transfert ou d'accès aux données de santé par des autorités étrangères, et imposé des garanties supplémentaires.

Les « garde-fous »

Référentiel SecNumCloud : à l'échelle de la France (délivrée par l'ANSSI, s'adresse aux prestataires Cloud)

Chapitre 19.6 (version 3.2) – Protection vis-à-vis du droit extra-européen

- Le siège social du prestataire doit être dans l'Union européenne
- Participation non européenne limitée à 24% du capital ou des droits de vote
- Administration & maintenance majoritairement réalisées depuis l'Europe.

La Cour des comptes souligne que SecNumCloud permet d'éviter la prolifération de labels "cloud souverain" sans contenu, mais que cette exigence a un coût et limite encore l'offre disponible.

Certification EUCS : Projet de **Certification européenne pour les services de cloud** (EUCS), porté par l'Agence de l'Union européenne pour la cybersécurité (ENISA) – n'a **pas encore été adopté.**

- 3 niveaux de certifications : basique, substantiel, et élevé (sous-divisé en High et High+)
- Garantie de la **solidité de la solution Cloud** face aux cyberattaques courantes :
- Certifie la **rigueur de la formalisation des processus** et méthodes du fournisseur du service Cloud ;
- Garantie la **protection du service Cloud vis-à-vis du droit extra-européen**.

04.
IA et responsabilité

IA et responsabilité

- L'IA ne peut pas être responsable des dommages qu'elle cause : **l'IA n'a pas de personnalité juridique**

- **Proposition de directive européenne relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle** (directive sur la responsabilité en matière d'IA), Commission européenne, 28 septembre 2022 (2022/0303). Abandonnée en février 2025, elle prévoyait :
  - L'instauration d'un régime extracontractuel spécifique ;
  - Le renversement de la charge de la preuve, faisant peser sur les fabricants la démonstration de l'absence de faute ;
  - La possibilité pour le juge d'ordonner la divulgation de preuves concernant les systèmes d'IA à haut risque.

- **Nouvelle directive (UE) 2024/2853 relative à la responsabilité du fait des produits défectueux, entre en vigueur le 9 décembre 2026 :**
  - Modernisation du régime européen de responsabilité du fait des produits défectueux en intégrant explicitement les logiciels et les systèmes d'IA comme des « produits » susceptibles d'être défectueux
  - Considérée comme insuffisante pour régir les systèmes d'IA de manière adéquate.

05.

Les réflexes à avoir

Les réflexes à avoir

- ❑ La juridiction et la loi applicable européenne
- ❑ Clauses relatives à la fin du contrat :
  - Réversibilité
  - Portabilité
- ❑ Clause de responsabilité (qui se cache parfois dans d'autres clauses – SLA)
- ❑ Confidentialité et contrôle sur les données:
  - Transferts hors UE (Garanties appropriées)
  - Chaine de sous-traitance (nationalité ? 2e degré idéalement)
- ❑ Continuité de services : exigences techniques et de sécurité (SLA, chiffrement, politique des accès, sauvegardes multiples, etc.)
- ❑ Exigences de conformité (RGPD, AI Act, NIS2…)
- ❑ Existence de qualification (SECNUMCLOUD) ou certification (ISO27001 ou ISO42001, HDS,…)

FIN

Merci pour votre attention !

A VOS QUESTIONS

Iteanu Avocats – https://www.iteanu.law/ – @iteanu –
contact@iteanu.law