NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

IA de confiance, IA éthique, IA souveraine… le point pour s'y retrouver et comprendre le rôle que peut y jouer le cloud

Résumé

- L'**IA souveraine** garantit la maitrise de la non-utilisation de données sensibles en-dehors d'usages définis en amont.
- L'**IA de confiance** garantit **transparence** et **sécurité** aux utilisateurs, en intégrant le contrôle humain.
- L'**IA éthique** mène une réflexion globale sur l'**utilisation humaine** de la technologie et ses conséquences sur les rapports ainsi que sur l'environnement.

A l'heure où l'IA fait couler beaucoup d'encre et ce depuis un certain temps, revenons sur les **différents qualificatifs** de celle-ci et ce qu'ils recouvrent concrètement.

L'IA souveraine

- **Le sujet de la souveraineté numérique est au cœur des discussions sur plusieurs aspects et l'IA n'y échappe pas.**

L'IA souveraine fait référence à des systèmes d'IA développés et utilisés dans un environnement garantissant la **maîtrise complète** de cette technologie par rapport à des IA classiques, qui peuvent dépendre de ressources ou de technologies hors UE et tombent donc sous le coup de **lois extraterritoriales**.

Cloud Souverain

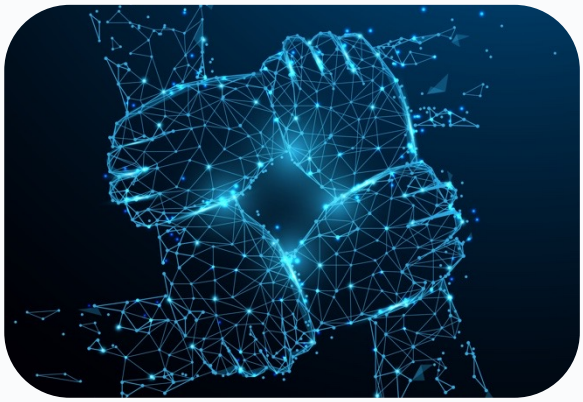
Ainsi des acteurs de confiance comme La Poste se positionnent sur le terrain de l'IA : la branche Santé et Autonomie de La Poste a ainsi lancé récemment une solution d'IA générative souveraine et de confiance, Medassitant, sous la houlette de Docaposte, leader de la confiance numérique, regroupant plusieurs acteurs 100% français pour proposer cette solution, et qui a fait le choix d'un **hébergement souverain et de confiance** pour celle-ci, via NumSpot.

L'IA de confiance

> **Elle recouvre plusieurs aspects.**

Tout d'abord, une IA de confiance est une IA dans laquelle **l'humain est présent** car la fiabilité de l'IA, aussi paradoxal que cela puisse paraître, passe par le contrôle. Les usages de l'IA sont multiples et les résultats générés peuvent se révéler d'une importance vitale, c'est par exemple le cas des IA utilisées dans le domaine de la santé, d'aide au diagnostic ou d'aide à la recommandation de traitement. Vérifier les données proposées par les moteurs dans des phases de tests est donc incontournable.

- Une IA de confiance se doit ensuite d'être **transparente**, c'est-à-dire qu'il s'agit ici d'avoir la capacité de décrypter et de comprendre les mécanismes qui entrent en jeu pour produire une réponse. Le syndrome de la « black box » est totalement contraire à une IA dite de confiance. L'open source est ainsi un bon début de réponse en matière d'IA de confiance.



Enfin, une IA de confiance est une IA **sûre au sens sécuritaire du terme**. Cet aspect revêt plusieurs volets.

Il est en effet clef que l'IA soit à l'abri de toute corruption, malversation qui conduirait à fausser les données et donc les résultats.
Il est aussi impératif de s'assurer que les données qui tournent sur ces modèles ne puissent être volées ou exploitées par des puissances étrangères, surtout s'il s'agit de données sensibles (données de santé, données secrètes, données de patrimoine).

Deux possibilités pour éviter cela :

- Des données anonymisées (quand il s 'agit de données personnelles), mais souvent cela se fait au détriment de la performance des modèles.

- Seconde possibilité, faire tourner ses IA sur des environnements de **cloud souverain et de confiance** bénéficiant de la qualification **SecNumCloud**. Cette qualification garantit une non-exposition aux lois extraterritoriales d'une part, et d'autre part un niveau de sécurisation très élevé.

L'IA éthique

> **C'est du côté de l'UNESCO qu'il convient de chercher des éclaircissements, puisqu'elle a inauguré en 2022 un premier forum consacré à l'éthique de l'intelligence artificielle. Le second forum dédié à ce sujet se tiendra d'ailleurs en février 2024.**

L'IA est un sujet vaste dont tous les aspects ne sont pas encore détourés et sur lesquels il est indispensable de légiférer.

L'Europe est d'ailleurs pionnière en la matière via l'IA Act. Les discussions se sont révélées âpres et longues sur le sujet car il s'agissait de ménager l'équilibre entre régulation et innovation, tout en prévoyant des restrictions et des sanctions. Après adoption aux votes par le Parlement européen, les États membres devront travailler sur l'adaptation de leur loi nationale à ce règlement, qui devrait rentrer en vigueur en 2026.

Les préoccupations en matière d'éthique portent sur plusieurs aspects :

- Le risque que les systèmes intègrent des biais qui peuvent se révéler **discriminatoires** et qui pourraient aller jusqu'à menacer les droits de l'homme,
- Sur l'aspect de l'environnement, le cloud peut aussi se révéler un levier intéressant. Avec l'utilisation des ressources à la demande et la mutualisation de celles-ci, on peut limiter l'impact sur l'environnement ou tout du moins mieux le maîtriser. De plus, les cloud providers sont très engagés pour la plupart dans des démarches de green IT et de **mesure de l'empreinte carbone**.
- Le risque de **dégradation du climat**, car on sait que l'usage du numérique a un impact sur la planète et l'on sait que les ressources nécessaires pour faire tourner certaines IA sont importantes. Se développe à ce titre une voie vers une IA plus frugale, caractérisée par de petits modèles de langage avec moins de paramètres.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot
@NumSpotCloud