

TERMES DE RÉFÉRENCE (TDR)

Concours « Défi IA »

Sujet 1 Gouvernance, données souveraines et cybersécurité

1. Contexte et enjeux

Djibouti, par sa position stratégique régionale et son ambition de bâtir un écosystème numérique national fiable et souverain, fait face à des défis structurants : la modernisation des services publics, la gouvernance et la qualité des données publiques, ainsi que la protection des systèmes d'information contre les nouvelles menaces cyber.

L'intelligence artificielle représente une opportunité majeure pour simplifier l'accès aux démarches administratives, améliorer la fiabilité des données utilisées dans la prise de décision et renforcer la sécurité des assistants IA. Elle présente également des risques lorsqu'elle est utilisée sans encadrement, notamment lorsque des données sensibles transitent vers des services hébergés hors du territoire national ou lorsque des contenus malveillants détournent le comportement d'un système d'IA.

Le présent sujet invite les équipes candidates à proposer des solutions concrètes, réalistes et déployables, contribuant à la modernisation de l'administration, à la souveraineté des données publiques et à la cybersécurité nationale.

2. Objectif général du sujet

Concevoir et développer un prototype fonctionnel et exécutable, s'appuyant sur l'intelligence artificielle, qui apporte une réponse concrète à l'une des trois problématiques présentées ci-dessous. Chaque équipe choisit une seule problématique comme socle de son projet. Chaque problématique impose un livrable technique précise : il ne s'agit pas d'une réflexion théorique, mais d'un outil réellement fonctionnel, testable et démontrable devant le jury.

3. Défis et problématiques au choix

Défi 1 IA pour la modernisation des services publics

Problématique 1 : Comment développer un assistant IA souverain capable d'accompagner les citoyens et les agents publics dans leurs démarches administratives, tout en garantissant des réponses fiables, accessibles et fondées sur des sources officielles ?

Les informations relatives aux démarches administratives — procédures, pièces à fournir, délais, conditions et services compétents — sont souvent réparties entre plusieurs documents, formulaires et textes officiels. Cette dispersion complique l'accès à une information fiable pour les citoyens et ralentit le travail des agents publics. Un assistant capable de répondre à ces questions en s'appuyant fidèlement sur les documents officiels contribuerait directement à la modernisation des services publics.

Ce qu'il faut développer : un assistant IA qui répond en langage naturel aux questions relatives aux démarches et à la réglementation publiques, indique les étapes et les pièces nécessaires lorsqu'elles figurent dans le corpus, cite précisément les sources de chaque réponse et signale clairement lorsqu'une information est absente ou incertaine. La solution devra être déployable localement afin de limiter la sortie de données sensibles.

- Livrable attendu : un assistant exécutable, interrogé en direct devant le jury sur de nouvelles questions, qui fournit une réponse claire accompagnée des références officielles utilisées.
- Le jury évaluera notamment : l'exactitude des réponses, la présence systématique des sources, l'absence d'informations inventées, la clarté de la restitution et le caractère déployable localement de la solution.

Ressources spécifiques nécessaires : un corpus de textes officiels, de fiches de démarches, de formulaires et de guides administratifs publics, accompagné d'un jeu de questions représentatives et de leurs réponses attendues.

Défi 2 IA pour la gouvernance des données publiques et l'aide à la décision

Problématique 2 : Comment utiliser l'intelligence artificielle pour détecter et corriger les erreurs, les doublons, les incohérences et les données manquantes dans les bases publiques, afin de produire des informations fiables pour l'aide à la décision ?

Les administrations produisent de nombreuses données nécessaires au suivi des politiques publiques et à la prise de décision. Ces bases peuvent néanmoins contenir des doublons, des valeurs manquantes, des formats invalides, des incohérences entre champs ou des valeurs anormales. Lorsque ces défauts ne sont pas identifiés, ils peuvent fausser les indicateurs, réduire la qualité des analyses et fragiliser les décisions publiques.

Ce qu'il faut développer : un outil qui analyse un jeu de données public synthétique, détecte les valeurs manquantes, les doublons, les formats invalides, les incohérences logiques et les valeurs atypiques. L'outil doit attribuer un score de qualité, expliquer les anomalies détectées, proposer des corrections ou des actions de vérification et présenter des indicateurs dans un tableau de bord d'aide à la décision.

- Livrable attendu : un outil exécutable, testé en direct devant le jury sur un nouveau fichier, qui produit un rapport d'anomalies, un score de qualité, des propositions de correction et un tableau de bord synthétique.
- Le jury évaluera notamment : le taux de détection correcte, le taux de faux positifs, la pertinence des corrections proposées, la clarté des explications et l'utilité des indicateurs produits.

Ressources spécifiques nécessaires : des jeux de données administratifs synthétiques accompagnés d'un dictionnaire des données et comportant des anomalies connues : doublons, valeurs manquantes, formats incompatibles, incohérences et valeurs atypiques.

Défi 3 IA pour la cybersécurité et la protection des systèmes d'information

Problématique 3 : Comment détecter automatiquement les tentatives d'injection de prompt dissimulées dans des documents, des courriels ou des pages web, afin de protéger les systèmes d'IA publics contre leur détournement et l'accès non autorisé aux données sensibles ?

De plus en plus d'administrations utilisent des assistants IA connectés à des documents, des courriels ou des outils externes. Un attaquant peut dissimuler des instructions malveillantes dans un contenu afin de détourner le comportement de l'assistant, de contourner ses règles ou de tenter d'obtenir des informations sensibles. Cette menace propre à l'IA générative reste encore mal couverte par les mécanismes de cybersécurité classiques.

Ce qu'il faut développer : un outil qui analyse un texte fourni en entrée document, courriel, métadonnée ou extrait de page web et détermine s'il contient une tentative d'injection de prompt. L'outil doit retourner un score de suspicion, proposer une décision autoriser, signaler ou bloquer — et expliquer les indices ayant motivé son verdict.

- Livrable attendu : un outil exécutable, testé en direct devant le jury sur de nouveaux contenus, qui distingue les contenus légitimes des tentatives de manipulation.
- Le jury évaluera notamment : le taux de détection correcte, le taux de faux positifs, la robustesse face aux formulations dissimulées et la clarté des explications fournies.

Ressources spécifiques nécessaires : un corpus de textes, courriels, documents et extraits web simulés, mêlant contenus légitimes et injections de prompt directes, indirectes ou dissimulées.

4. Jeux de données nécessaires

Pour chacune des trois problématiques, des données synthétiques, conçues spécifiquement pour le concours, anonymisées ou tirées de sources ouvertes seront nécessaires. Aucune donnée confidentielle ou à caractère personnel appartenant à des tiers ne sera fournie ni ne devra être utilisée.

Pour la problématique 1 (assistant administratif souverain)

- Un corpus de textes officiels publics : fiches de démarches, formulaires, procédures, délais, conditions et guides administratifs.
- Un jeu de questions représentatives, accompagné des réponses attendues et de leurs références.

Pour la problématique 2 (qualité des données publiques)

- Un ou plusieurs jeux de données administratifs synthétiques : identifiants fictifs, catégories, dates, localisations, statuts et indicateurs.
- Des anomalies documentées : doublons, valeurs manquantes, formats invalides, incohérences logiques et valeurs atypiques.

Pour la problématique 3 (injection de prompt)

- Un corpus de textes variés — notes, courriels, documents et extraits web simulés — dont certains contiennent des injections directes, indirectes ou dissimulées et d'autres sont entièrement légitimes.

5. Livrables attendus (communs aux trois problématiques)

- Un prototype fonctionnel et exécutable, avec le code source complet, capable de traiter de nouveaux exemples en direct devant le jury et non une simple maquette ou un document de réflexion.
- Une documentation technique concise décrivant l'architecture, les choix effectués, les données utilisées et le rôle exact de l'intelligence artificielle dans la solution.
- Une documentation d'installation et d'utilisation permettant de reproduire la démonstration.
- Un support de présentation synthétisant le problème traité, la solution développée, les résultats obtenus et l'impact potentiel pour le pays.
- Une brève note présentant les limites de la solution et les pistes d'amélioration.

6. Contraintes spécifiques à ce sujet

- Toute solution doit respecter les principes de protection des données personnelles et n'utiliser que des données publiques, synthétiques ou anonymisées.
- Les solutions doivent être conçues dans une logique de souveraineté : privilégier des approches déployables localement ou ne dépendant pas exclusivement de services étrangers non maîtrisables.
- Pour la problématique 1, l'assistant doit citer ses sources, ne pas inventer de procédure et signaler les informations absentes ou incertaines.
- Pour la problématique 2, aucune correction ne doit être appliquée irréversiblement aux données sans validation humaine ; les données originales doivent être conservées.
- Pour la problématique 3, les attaques utilisées doivent être simulées et ne doivent cibler aucun système, organisme ou utilisateur réel.

7. Critères d'évaluation spécifiques

En complément des critères généraux définis dans le règlement du Concours, une attention particulière sera portée aux éléments suivants :

- Pertinence de la solution par rapport au défi choisi et à un besoin réel de l'administration ;
- Performance de l'outil sur des cas nouveaux, non vus pendant le développement ;
- Rigueur dans le traitement, la protection et la traçabilité des données ;
- Clarté des résultats, des explications et des sources fournies ;
- Réalisme, sécurité et faisabilité d'un déploiement local ;
- Qualité de la démonstration et capacité de l'équipe à justifier ses choix techniques.

8. Calendrier propre au sujet

Le calendrier détaillé date limite de soumission, présélection et phase finale sera communiqué par l'Organisateur conformément au règlement général du Concours.

9. Contact et assistance

Pour toute question technique relative à ce sujet format des données, clarification de la problématique ou conditions de démonstration les équipes peuvent contacter l'Organisateur aux coordonnées communiquées lors de l'inscription.

Fait à Djibouti, le 18/07/2026