



## GROUPE DE TRAVAIL SUR LA CHAÎNE LOGISTIQUE

UPAP/CET/GCL/GASU/01/2026 - Doc N°4

GROUPE D'ACTION SUR LA SÉCURITÉ DE L'UPAP (GASU)

25 JANVIER 2026 (MODE VIRTUEL) HEURE : 09H00 (TU)

### QUESTIONS STRATÉGIQUES EN MATIÈRE DE SÉCURITÉ EN AFRIQUE POUR LE CYCLE 2026/2027 – 2029/2030

|   |   |
|---|---|
| <b>1. Objet</b><br>Enjeux stratégiques de sécurité pour le cycle  | <b>Références/Alinéas</b><br><br><b>Projet de stratégie postale africaine (2026-2030)</b> |
| <b>2. Décisions attendues.</b> <ul style="list-style-type: none"><li>• Prenez note du document ;</li><li>• Fournir les conseils nécessaires</li></ul> |   |

## 1. INTRODUCTION

La Stratégie postale africaine 2026-2030 définit une vision renouvelée et unifiée de la transformation postale en Afrique, en cohérence avec la Stratégie de Dubaï 2026-2029 de l'Union postale universelle (UPU), l'Agenda 2063 de l'Union africaine et la Stratégie de transformation numérique pour l'Afrique (2020-2030). Elle témoigne de l'engagement collectif des États membres africains, sous la coordination de l'Union panafricaine des postes (UPAP), à faire du secteur postal un acteur essentiel de la connectivité numérique, de la facilitation des échanges et de l'inclusion sociale sur le continent.

La stratégie postale africaine adopte une approche intégrée de la transformation, alignant les priorités régionales de l'Afrique sur les trois objectifs mondiaux approuvés par l'UPU, tout en maintenant les cinq piliers distinctifs qui définissent l'identité opérationnelle de l'UPAP et répondent aux réalités contextuelles de l'Afrique.

## 2. CADRE STRATÉGIQUE

La Stratégie postale africaine 2026-2030 s'articule autour de cinq piliers stratégiques, chacun conçu pour contribuer à la réalisation des objectifs mondiaux de l'UPU et des aspirations de développement de l'Afrique, comme suit :

- **Pilier 1 : Politique, réglementation et gouvernance ;**
- **Pilier 2 : Innovation, transformation numérique et commerce électronique ;**
- **Pilier 3 : Opérations, qualité de service et développement des infrastructures ;**
- **Pilier 4 : Inclusion financière et sociale ;**
- **Pilier 5 : Capacités institutionnelles, partenariats et mobilisation des ressources.**

### 3. ENJEUX STRATEGIQUES DE SECURITE POUR LE CYCLE

Conformément au cadre stratégique susmentionné, les enjeux stratégiques liés à la sécurité postale seront intégrés afin de garantir que les pays en développement puissent respecter les normes internationales en matière de sécurité aérienne et de chaîne logistique. Les enjeux stratégiques suivants orientent la mise en œuvre des activités de sécurité par l'Union au cours du cycle.

#### 3.1. Pilier 1 : Politique, réglementation et gouvernance

| N° d'ordre | Enjeu stratégique   | Orientation stratégique   |
|------------|---|---|
| 1.         | Disparité entre les normes internationales de sécurité postale et les cadres réglementaires nationaux | i) Les pays membres s'efforcent d'intégrer pleinement les articles 58 et 59 de l'UPU, les exigences en matière de sûreté aérienne ou de sûreté douanière dans leur droit national.    |
| 2.         | Mise en œuvre incohérente des obligations de conformité en matière de sécurité dans les pays membres  | i) Harmoniser les interprétations des règles de sécurité pour remédier aux vulnérabilités de la chaîne postale mondiale   |
| 3.         | Complexité croissante des réglementations en matière de sécurité transfrontalière                     | i) Répondre aux exigences accrues et plus strictes en matière de sûreté aérienne, de douanes et de lutte contre le terrorisme qui constituent un fardeau pour les opérateurs.         |
| 4.         | Mettre à jour les cadres réglementaires pour faire face aux nouvelles menaces                         | i) Renforcer l'adaptation réglementaire pour faire face à l'augmentation des marchandises dangereuses, des substances illicites, des articles contrefaits et des risques biologiques. |

#### 3.2. Pilier 2 : Innovation, transformation numérique et commerce électronique

| N° d'ordre | Enjeu stratégique   | Orientation stratégique  |
|------------|---|--|
| 1.         | Capacité numérique de contrôle, de détection et de suivi des envois à haut risque | i) Développer les capacités, les systèmes et les outils d'analyse des opérateurs désignés pour utiliser pleinement les données électroniques anticipées (EAD). |
| 2.         | Risques croissants de cybersécurité dans les systèmes informatiques postaux       | i) Renforcer l'intégrité et la confiance dans les réseaux postaux, les bases de données clients et les plateformes de suivi                                    |
| 3.         | Nécessité de mécanismes de partage de données en temps réel                       | i) Explorer les moyens d'accroître l'intégration des partenaires afin d'améliorer la capacité à identifier les envois suspects.                                |

|    |   |  |
|----|---|--|
|    | entre les postes, les douanes et les services de sécurité   |  |
| 4. | Augmentation de la circulation d'articles dangereux et interdits via les plateformes de commerce électronique | i) Il convient de remédier à la vulnérabilité des systèmes postaux face à l'expédition de stupéfiants, d'armes et de marchandises contrefaites, compte tenu de l'augmentation du volume de colis dans le réseau.           |
| 5. | Adoption limitée des technologies de sécurité numérique   | i) Déploiement de mesures de protection numériques telles que la détection automatique par rayons X, le profilage basé sur l'IA, les scellés inviolables et les systèmes de chaîne de traçabilité basés sur la blockchain. |

### 3.3. Pilier 3 : Opérations, qualité de service et développement des infrastructures

| N° d'ordre | Enjeu stratégique  | Orientation stratégique  |
|------------|--|--|
| 1.         | Adéquation des infrastructures de sécurité dans les centres de tri                     | i) Préciser les équipements de contrôle, les zones séparées, la vidéosurveillance, les zones de chargement sécurisées et les procédures de manipulation inviolables dans les centres de tri. |
| 2.         | Normalisation des capacités de contrôle et de manutention des marchandises dangereuses | i) Les opérateurs doivent se conformer aux procédures d'identification, de rejet et de conformité des marchandises dangereuses.  |
| 3.         | Vulnérabilités du dernier kilomètre et sécurité de la chaîne de transport              | i) Remédier aux faiblesses de la chaîne de traçabilité lors du transport terrestre ou aérien, qui sont à l'origine de l'augmentation des vols et des détournements de colis.                 |
| 4.         | Déploiement des protocoles de réponse aux incidents et de gestion de crise             | i) Aborder la question de la gestion des incidents de sécurité et des retards dans le rétablissement du service  |

### 3.4. Pilier 4 : Inclusion financière et sociale

| N° d'ordre | Enjeu stratégique  | Orientation stratégique   |
|------------|--|---|
| 1.         | Le coût élevé de la mise en œuvre des normes de sécurité pour les pays en développement        | i) Les opérateurs postaux recherchent des financements pour l'équipement de contrôle, les infrastructures sécurisées et les systèmes numériques.                            |
| 2.         | Risque d'exclusion des flux mondiaux en raison du non-respect des seuils de sécurité           | i) Les opérateurs doivent s'attaquer aux problèmes de sécurité et autres difficultés, comme les coûts de transport élevés, le refus des envois ou les interdictions de vol. |
| 3.         | Les petits pays et les pays isolés sont confrontés à des défis de conformité disproportionnés. | i) Investir dans les technologies de dépistage, le personnel et les transports sécurisés.   |

### 3.5. Pilier 5 : Capacités institutionnelles, partenariats et mobilisation des ressources.

| N° d'ordre | Enjeu stratégique  | Orientation stratégique  |
|------------|--|--|
| 1.         | Comblar les lacunes en matière de connaissances et de compétences en matière de sécurité postale | ii) Des programmes de formation et de renforcement des capacités destinés aux agents de sécurité, aux spécialistes de la DG et aux experts en sécurité numérique                       |
| 2.         | Nécessité de partenariats interinstitutionnels plus solides                                      | ii) Consolider la collaboration avec les douanes, les compagnies aériennes, la police, les agences de cybersécurité, etc., et les organisations internationales (OACI, OMD, INTERPOL). |
| 3.         | Ressources financières limitées pour la modernisation de la sécurité                             | ii) Soutenir la mobilisation des capacités d'investissement pour les technologies de contrôle, les installations sécurisées et les systèmes de sécurité numérique                      |
| 4.         | Programmes d'assistance technique et de sécurité soutenus par les donateurs                      | ii) Collaborer avec l'UPU pour obtenir une assistance technique sur les normes de sécurité afin de répondre aux exigences mondiales en matière d'aviation et de chaîne logistique.     |

#### **4. RECOMMANDATIONS**

Les Etats membres sont encouragés à aligner leurs plans opérationnels postaux nationaux sur la stratégie postale africaine, tout en abordant les questions stratégiques liées à la sécurité postale.

#### **5. DECISIONS ATTENDUES**

Le groupe de travail est par la présente prié de :

- i) Prendre note du présent document et fournir les orientations nécessaires aux Etats membres.
- ii) Soumettre à la Commission Exploitation et Technologies le document consolidé sur les enjeux stratégiques de sécurité pour le cycle 2026/2027 – 2029/2030