DÉCRET D/2026/0161/PRG/SGG

PORTANT DÉPLOIEMENT ET EXPLOITATION D'UNE PLATEFORME NATIONALE DE CERTIFICATION DE L'IDENTITÉ DES DÉTENTEURS DE CARTES SIM ET UTILISATEURS DES SERVICES/PRODUITS DE TELECOMMUNICATIONS

LE PRÉSIDENT DE LA RÉPUBLIQUE,

Vu la Constitution ;

Vu la Loi L/2015/018/AN du 13 août 2015 relative aux Télécommunications et aux Technologies de l'Information et de la Communication ;

Vu les dispositions en vigueur relatives à l'identification obligatoire des abonnés des services de télécommunications ;

Vu les dispositions en vigueur relatives à la protection des données à caractère personnel ;

Vu la nécessité de sécuriser les communications électroniques et de lutter contre la fraude identitaire ;

Vu la nécessité de préserver la sécurité publique et de lutter contre la cybercriminalité, le terrorisme et la criminalité organisée ;

Vu les missions dévolues à l'Autorité de Régulation des Postes et Télécommunications ;

DÉCRÈTE :

TITRE I : DISPOSITIONS GÉNÉRALES

Article 1er : Objet

Le présent décret détermine les conditions de déploiement, les modalités d'exploitation, les règles techniques, les obligations réglementaires, les exigences de sécurité ainsi que les modalités de contrôle applicables à la Plateforme Nationale de Certification de l'Identité des détenteurs de cartes SIM et utilisateurs des services/produits de télécommunications en République de Guinée.

Article 2 : Finalités de la plateforme

La plateforme nationale a pour finalités :

- l'authentification des abonnés et la certification de leurs pièces d'identité ;

- l'élimination des cartes SIM anonymes et la prévention de la fraude documentaire ;
- le renforcement de la sécurité nationale ainsi que la sécurisation des services numériques et financiers ;
- l'amélioration de la fiabilité des bases d'abonnés des opérateurs de télécommunications.

Article 3 : Champ d'application

Le présent décret s'applique aux opérateurs de télécommunications, aux fournisseurs d'accès à Internet, aux distributeurs agréés, aux exploitants de plateformes de vérification d'identité, aux administrations détentrices de bases nationales d'identité, ainsi qu'à tout souscripteur de services de télécommunications.

TITRE II : GOUVERNANCE DE LA PLATEFORME

Article 4 : Autorité de supervision

L'Autorité de Régulation des Postes et Télécommunications (ARPT) assure la supervision technique et réglementaire de la plateforme. À ce titre, elle est chargée d'approuver les spécifications techniques, d'assurer le contrôle réglementaire, d'homologuer les systèmes, d'autoriser les interconnexions, de diligenter les audits et de veiller au respect des obligations des opérateurs.

Article 5 : Comité national de supervision

Il est institué un Comité National de Supervision de la Certification des Identités Télécoms. Ce comité réunit notamment le Ministère en charge des Télécommunications et de l'Economie Numérique, l'ARPT, le Ministère en charge de la Sécurité, le Ministère de l'Administration du Territoire, l'Agence Nationale de la Sécurité des Systèmes d'Informations, les opérateurs de télécommunications, ainsi que toute autre structure concernée par la mise en œuvre du présent décret.

Les membres du comité sont nommés par Décret.

Article 6 : Missions du Comité

Le Comité est chargé du suivi stratégique du système, de la coordination interinstitutionnelle, de la validation des politiques de sécurité, du suivi des incidents majeurs et de la supervision des mécanismes de conformité.

TITRE III : ARCHITECTURE ET FONCTIONNEMENT DE LA PLATEFORME

Article 7 : Architecture de la plateforme

La plateforme nationale comprend notamment :

- un système central de certification ;
- un moteur de vérification documentaire ;
- un système de vérification biométrique ;
- un système d'authentification ;
- un registre centralisé des certifications ;
- un système de journalisation sécurisé ;
- un centre de supervision de la sécurité.

Article 8 : Interconnexion avec les bases nationales

La plateforme est interconnectée avec :

- le registre national d'identité, les bases biométriques nationales ;
- les systèmes de gestion des passeports ;
- les registres d'état civil ;
- et les bases de données des étrangers résidents.

Toute interconnexion est subordonnée à une autorisation préalable, à la mise en place d'un protocole sécurisé, à la réalisation d'un audit de conformité et à une validation par les autorités compétentes en matière de cybersécurité.

Article 9 : Hébergement des données

Les données collectées et traitées dans le cadre du présent décret doivent être hébergées sur le territoire national, dans des infrastructures sécurisées conformes aux normes internationales en vigueur. Tout transfert transfrontalier de données est soumis à l'autorisation préalable des autorités compétentes.

TITRE IV : OBLIGATIONS DES OPÉRATEURS

Article 10 : Certification obligatoire

Tout opérateur est tenu de vérifier électroniquement les pièces d'identité de ses abonnés, de certifier tout nouvel abonné, de procéder à la recertification des abonnés existants et d'utiliser exclusivement les interfaces homologuées par l'ARPT.

Article 11 : Activation des cartes SIM

Aucune carte SIM ne peut être activée, réactivée ou remplacée sans validation préalable de l'identité de l'abonné par la plateforme nationale.

Article 12 : Collecte des données

Les opérateurs ne peuvent collecter que les données strictement nécessaires à l'identification des abonnés. Ces données doivent être exactes, à jour, sécurisées et traçables.

Article 13 : Conservation des données

Les opérateurs et les exploitants de la plateforme sont tenus de conserver les données d'identification, les journaux de certification et les preuves de vérification pendant la durée fixée par la réglementation en vigueur.

Article 14 : Obligation de sécurité

Les opérateurs doivent mettre en œuvre des systèmes de chiffrement des données, des mécanismes de contrôle d'accès, des dispositifs anti-intrusion, des procédures d'audit régulières, des plans de continuité d'activité, ainsi que des mécanismes de sauvegarde et de reprise après incident.

TITRE V : PROTECTION DES DONNÉES PERSONNELLES

Article 15 : Confidentialité

Les données relatives aux abonnés revêtent un caractère strictement confidentiel. Toute utilisation non expressément autorisée est interdite.

Article 16 : Protection des données biométriques

Les données biométriques ne peuvent être utilisées qu'aux seules fins d'identification prévues par le présent décret. Elles doivent faire l'objet d'un chiffrement et être protégées contre tout accès non autorisé.

Article 17 : Droits des abonnés

Tout abonné bénéficie d'un droit d'information, d'un droit d'accès à ses données, d'un droit de rectification, d'un droit de contestation et d'un droit de recours devant les autorités compétentes.

TITRE VI : HOMOLOGATION ET AUDIT

Article 18 : Homologation des systèmes

Tout système utilisé dans le cadre du présent décret doit être préalablement homologué par l'ARPT. L'homologation porte notamment sur la cybersécurité, l'interopérabilité, la conformité technique, la protection des données personnelles et la performance du système.

Article 19 : Audit obligatoire

Les exploitants de la plateforme et les opérateurs sont soumis à des audits périodiques, à des contrôles inopinés, à des tests de sécurité et à des vérifications de conformité diligentés par l'ARPT.

Article 20 : Rapports de conformité

Les opérateurs transmettent trimestriellement à l'ARPT un rapport précisant le nombre de certifications réalisées, les anomalies détectées, les cas de fraude identifiés, les incidents de sécurité survenus ainsi que les statistiques de rejet.

TITRE VII : INFRACTIONS ET SANCTIONS

Article 21 : Infractions

Constituent notamment des infractions au présent décret :

- l'activation d'une carte SIM sans certification préalable ;
- l'utilisation d'un système non homologué ;
- la falsification de données ;
- l'accès frauduleux aux bases de données ;
- la divulgation non autorisée de données personnelles ;
- le refus de coopérer avec l'ARPT.

Article 22 : Sanctions administratives

Sans préjudice des poursuites pénales, les infractions au présent décret exposent leurs auteurs aux sanctions administratives suivantes :

- avertissement ;
- mise en demeure ;
- amende administrative ;
- suspension d'activité ;
- retrait d'autorisation.

Article 23 : Sanctions pénales

Indépendamment des sanctions administratives prévues à l'article précédent, toute violation grave des dispositions du présent décret expose son auteur aux sanctions pénales prévues par les lois en vigueur.

TITRE VIII : DISPOSITIONS TRANSITOIRES ET FINALES

Article 24 : Phase de migration

Les opérateurs disposent d'un délai de six (06) mois à compter de la date d'entrée en vigueur du présent décret pour intégrer leurs systèmes à la plateforme nationale, et d'un délai de vingt-quatre (24) mois pour procéder à la recertification de l'ensemble de leurs abonnés existants.

Article 25 : Continuité des services

La migration vers la plateforme nationale ne doit entraîner aucune interruption abusive ni aucune dégradation notable des services fournis aux abonnés.

Article 26 : Textes d'application

Les mobilités techniques de mises en œuvre de la plateforme sont déterminées par Décision de l'ARPT.

Article 27 : Entrée en vigueur

Le présent décret qui prend effet à compter de la date de sa signature sera enregistré au Journal Officiel de la République.

Conakry, le 21 MAI 2026

Président Mamadi DOUMBOUYA