MINISTERE DES POSTES, DE L'ECONOMIE NUMERIQUE ET DES INNOVATIONS TECHNOLOGIQQUES

MINISTERE DE LA SECURITE ET DE LA PROTECTION CIVILE

MINISTERE DE LA DEFENSE ET DES ANCIENS COMBATTANTS

REPUBLIQUE TOGOLAISE
Travail - Liberté - Patrie

DECRET N° 2019-095/PR
relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes

---

LE PRÉSIDENT DE LA RÉPUBLIQUE,

Sur le rapport conjoint du ministre des postes, de l'économie numérique et des innovations technologiques, du ministre de la sécurité et de la protection civile et du ministre de la défense et des anciens combattants,

Vu la constitution du 14 octobre 1992 ;

Vu la loi n° 2012-018 du 17 décembre 2012 sur les communications électroniques, modifiée par la loi n°2013-003 du 19 février 2013 ;

Vu la loi d'orientation n° 2017-006 du 22 juin 2017 sur la société de l'information au Togo ;

Vu la loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, notamment ses articles 3 et 6 ;

Vu le décret n° 2012-004/PR du 29 février 2012 relatif aux attributions des ministres d'Etat et ministres ;

Vu le décret n° 2012-006/PR du 07 mars 2012 portant organisation des départements ministériels ;

Vu le décret n° 2014-088/PR du 31 mars 2014 portant sur les régimes juridiques applicables aux activités de communications électroniques modifié par le décret n° 2018-145/PR du 03 octobre 2018 ;

Vu le décret n° 2014-112/PR du 30 avril 2014 portant sur l'interconnexion et l'accès aux réseaux de communications électroniques modifié par le décret n° 2018-144/PR du 03 octobre 2018 ;

Vu le décret n° 2019-003/PR du 24 janvier 2019 portant nomination du Premier ministre ;

Vu le décret n° 2019-004/PR du 24 janvier 2019 portant composition du gouvernement, modifié par le décret n° 2019-005/PR du 25 janvier 2019;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions et organisation et fonctionnement de l'Agence nationale de la cybersécurité ;

Le conseil des ministres entendu,

D E C R E T E :

CHAPITRE Ier - DISPOSITIONS GENERALES

Article 1er : Le présent décret définit les modalités et critères de désignation des opérateurs de services essentiels et de déclaration des infrastructures essentielles situées sur le territoire togolais et fixe les règles relatives à la cybersécurité desdites infrastructures.

CHAPITRE II - OPERATEURS DE SERVICES ESSENTIELS ET INFRASTRUCTURES ESSENTIELLES

Section 1ère : Désignation des opérateurs de services essentiels

Article 2 : La liste des services essentiels pour la sécurité publique, la stabilité économique, la sécurité nationale, la stabilité internationale, la pérennité et la restauration du cyberespace critique mentionnés à l'article 2 de la loi n° 2018-026 susvisée figure à l'annexe du présent décret.

Article 3 : Sont dénommés opérateurs de services essentiels, en application de l'article 2 de la loi n° 2018-026 précitée, les opérateurs fournissant au moins un service mentionné à l'annexe au présent décret lorsque des infrastructures essentielles sont nécessaires à la fourniture de ce service et qu'un incident affectant lesdites infrastructures aurait, sur la fourniture de ce service, des conséquences graves, appréciées au regard des critères suivants :

- le nombre d'utilisateurs dépendant du service fourni via l'infrastructure essentielle ;

- la dépendance des autres secteurs d'activités figurant à l'annexe au présent décret à l'égard du service fourni via l'infrastructure essentielle ;
- les conséquences qu'un incident pourrait avoir, en termes de gravité et de durée, sur le fonctionnement de l'économie ou de la société ou sur la sécurité publique ;
- la part de marché de l'opérateur fournissant ledit service via l'infrastructure essentielle ;
- la portée géographique eu égard à la zone susceptible d'être touchée par un incident ;
- l'importance que revêt l'opérateur pour assurer un niveau de service suffisant, compte tenu de la disponibilité de moyens alternatifs pour la fourniture du service ;
- le cas échéant, des facteurs sectoriels.

Article 4 : Les opérateurs de services essentiels sont désignés par décision de l'Agence Nationale de Cybersécurité (ANCy). Cette décision mentionne les services essentiels pour la sécurité publique, la stabilité économique, la sécurité nationale, la stabilité internationale, la pérennité et la restauration du cyberespace critique fournis par chacun des opérateurs de services essentiels désignés.

Article 5 : L'ANCy notifie à chaque opérateur concerné son intention de le désigner comme opérateur de services essentiels. L'opérateur dispose d'un délai d'un mois à compter de cette notification pour présenter ses observations.

Pour la désignation des opérateurs de services essentiels, chaque ministre dont le domaine de compétence recouvre un secteur ou sous-secteur d'activité figurant à l'annexe au présent décret (ci-après désigné autorité sectorielle) propose à l'ANCy une liste d'opérateurs, relevant de ce secteur ou sous-secteur, susceptibles d'être désignés en tant qu'opérateurs de services essentiels en justifiant, pour chaque opérateur, sa proposition au regard des critères mentionnés à l'article 3 du présent décret.

L'Agence nationale de la cybersécurité peut également, après concertation avec les ministres concernés, désigner des opérateurs de services essentiels pour tous les secteurs et sous-secteurs d'activité figurant à l'annexe au présent décret.

Article 6 : L'ANCy, après en avoir informé l'autorité sectorielle, met fin à la désignation des opérateurs de services essentiels qui ne satisfont plus aux critères mentionnés à l'article 3 du présent décret.

La décision mettant fin à la désignation est notifiée à l'opérateur de services essentiels.

Article 7 : L'opérateur de services essentiels désigne un point de contact pour la sécurité et en communique les données de contact à l'autorité sectorielle et à l'ANCy dans un délai de six mois à compter de la notification de la désignation comme infrastructure critique, ainsi qu'après chaque mise à jour de ces données.

Le point de contact pour la sécurité exerce la fonction de point de contact vis-à-vis de l'autorité sectorielle, de l'ANCy, des services de police pour toute question liée à la sécurité et la protection de l'infrastructure.

Le point de contact pour la sécurité est disponible à tout moment.

Section 2 : Déclaration des infrastructures essentielles

Article 8 : L'autorité sectorielle identifie, pour le secteur relevant de sa compétence, les infrastructures essentielles nationales.

Elle procède à cette identification après consultation des opérateurs de services essentiels suivant une procédure qui comporte au moins les étapes suivantes :

I. L'autorité sectorielle applique des critères sectoriels afin d'opérer une première sélection parmi les infrastructures existant au sein de son secteur. Ces critères sont établis eu égard aux caractéristiques particulières du secteur concerné en concertation avec l'ANCy.

II. L'autorité sectorielle applique la définition de l'infrastructure essentielle aux termes de l'article 2 point 57 de la loi n° 2018-026 sur la cybersécurité et la lutte contre la cybercriminalité du 07 décembre 2018 à la sélection effectuée lors de la première étape et dresse une liste des infrastructures essentielles potentielles ainsi identifiées.

III. La gravité de l'incidence est déterminée en fonction des caractéristiques du secteur concerné, sur la base des critères intersectoriels visés à l'article 3 du présent décret. Il est tenu compte de l'existence de solutions de remplacement ainsi que de la durée de l'interruption/de la reprise d'activité.

Les opérateurs de services essentiels établissent et tiennent à jour la liste des infrastructures essentielles potentielles, auxquels pourront s'appliquer les règles de cybersécurité prévues à l'article 3 de la loi n°2018-026 précitée. Cette liste comprend, le cas échéant, les infrastructures essentielles dont ils ont confié l'exploitation à un tiers lorsque lesdites infrastructures sont nécessaires à la fourniture des services essentiels concernés.

Article 9 : Dans un délai de trois (3) mois à compter de sa désignation comme opérateur de services essentiels, l'opérateur communique à l'autorité sectorielle, par voie électronique et par voie postale, en mettant en copie l'ANCy, la liste mentionnée à l'article 8 du présent décret ainsi que, pour chaque infrastructure essentielle, les informations précisées par arrêté.

L'opérateur de services essentiels communique une fois par an à l'autorité sectorielle et à l'ANCy les mises à jour de la liste et des informations mentionnées au premier alinéa. Lorsqu'il retire une infrastructure essentielle de sa liste, l'opérateur en informe sans délai l'autorité sectorielle et l'ANCy et leur fournit la justification de ce retrait.

Article 10 : L'Agence nationale de la cybersécurité, après avis des autorités sectorielles concernées, peut faire des observations aux opérateurs de services essentiels sur la liste mentionnée à l'article 8 du présent décret et les informations mentionnées à l'article 9 du présent décret.

Dans ce cas, l'opérateur de services essentiels modifie sa liste et les informations conformément à ces observations et communique à l'autorité sectorielle et à l'ANCy, la liste et les informations modifiées, dans un délai de deux (2) mois à compter de la réception des observations. L'Agence en rend compte au Premier ministre.

Section 3 : Règles de cybersécurité

Article 11 : L'Agence nationale de la cybersécurité fixe les règles de cybersécurité prévues à l'article 3 de la loi n° 2018-026 précitée que les opérateurs de services essentiels doivent respecter.

Ces règles ont pour objet de garantir un niveau de sécurité adapté au risque existant, compte tenu de l'état des connaissances.

Les opérateurs de services essentiels appliquent les règles visées à l'alinéa ci-dessus à leurs frais.

Les règles prévues au second alinéa du présent article visent notamment à s'assurer que les opérateurs de services essentiels identifient les risques qui menacent la sécurité des réseaux et systèmes d'informations nécessaires à la fourniture des services essentiels et prennent les mesures techniques et organisationnelles appropriées pour gérer ces risques, pour prévenir les incidents qui compromettent la sécurité desdits réseaux et systèmes d'information ainsi que pour en limiter l'impact, de manière à garantir la continuité de leurs services.

Ces règles définissent les mesures appropriées dans chacun des domaines suivants :

1- la gouvernance de la sécurité des réseaux et systèmes d'information ;
2- la protection des réseaux et systèmes d'information ;
3- la défense des réseaux et systèmes d'information ;
4- la résilience des activités.

Elles peuvent également prescrire le recours à des dispositifs matériels ou logiciels ou à des services informatiques dont la sécurité a été certifiée par l'ANCy.

Un arrêté conjoint du ministre chargé de l'économie numérique et du ministre chargé de la sécurité, complète en tant que de besoin, les dispositions de cet article.

Section 4 : Plan de sécurité d'opérateurs (PSO)

Article 12 : Les opérateurs de services essentiels se dotent de plans de sécurité d'opérateurs (PSO) ou de mesures équivalentes visant à prévenir, à atténuer et à neutraliser les risques d'interruption du fonctionnement ou de destruction de l'infrastructure essentielle par la mise au point de mesures matérielles et organisationnelles internes.

Un plan de sécurité d'opérateurs comprend au minimum :

1° des mesures internes de sécurité permanentes, applicables en toutes circonstances ;

2° des mesures internes de sécurité graduelles à appliquer en fonction de la menace.

La procédure d'élaboration d'un PSO recense les mesures de sécurité appliquées ou en cours de mise en œuvre pour la protection des services essentiels. La procédure d'élaboration du PSO comprend au moins les étapes suivantes :

1. l'inventaire et la localisation des points de l'infrastructure qui, s'ils étaient touchés, pourraient causer l'interruption de son fonctionnement ou sa destruction ;
2. une analyse des risques, consistant en une identification des principaux scénarios de menaces potentielles pertinents d'actes intentionnels visant à interrompre le fonctionnement de l'infrastructure essentielle ou à la détruire ;
3. une analyse des vulnérabilités de l'infrastructure essentielle et des impacts potentiels de l'interruption de son fonctionnement ou de sa destruction en fonction des différents scénarios retenus ;
4. pour chaque scénario de l'analyse de risques, l'identification, la sélection et la désignation par ordre de priorité des mesures de sécurité internes.

L'opérateur de services essentiels élabore le PSO dans un délai d'un an à compter de la notification de la désignation de son infrastructure comme infrastructure essentielle.

L'opérateur de services essentiels est responsable d'organiser des exercices et d'actualiser le PSO, en fonction des enseignements des exercices ou de toute modification de l'analyse des risques.

L'ANCy apprécie si chaque infrastructure classée comme essentielle établie sur le territoire est doté d'un PSO ou a mis en place des mesures équivalentes répondant aux exigences du présent article. Si l'ANCy estime qu'un PSO ou une mesure équivalente existe est mis à jour régulièrement, aucune autre mesure d'exécution n'est nécessaire.

L'ANCy s'assure qu'un PSO ou une mesure équivalente est établi et que, dans un délai d'un (1) an à compter de la désignation de l'infrastructure comme essentiel, il fait l'objet d'un réexamen. Ce délai peut être prorogé dans les circonstances exceptionnelles.

Article 13 : Sans préjudice des compétences des autorités judiciaires pour prendre des mesures de police judiciaire, l'ANCy peut solliciter des services de police des mesures externes de protection des infrastructures essentielles, sur la base d'une analyse de la menace réalisée à sa demande.

Article 14 : L'ANCy et les services de police récoltent les informations utiles pour la prise de mesures externes de protection des infrastructures critiques.

L'opérateur de services essentiels, son point de contact pour la sécurité, l'autorité sectorielle, l'ANCy et les services de police collaborent en tout temps, par un échange adéquat d'informations concernant la sécurité et la protection de l'infrastructure

essentielle, afin de veiller à une concordance entre les mesures internes de sécurité et les mesures externes de protection.

Section 5 : Contrôles de sécurité et accréditations

Article 15 : L'Agence nationale de la cybersécurité ou des prestataires de service chargés du contrôle qualifiés par l'agence peuvent soumettre les opérateurs de services essentiels à des contrôles destinés à vérifier le respect des obligations prévues au présent décret et par les décisions de l'ANCy, ainsi que le niveau de sécurité des infrastructures essentielles.

Les contrôles sont effectués, sur pièce et sur place. Le coût des contrôles est à la charge des opérateurs de services essentiels.

Les opérateurs de services essentiels communiquent à l'Agence nationale de cybersécurité ou au prestataire de service prévu au premier alinéa du présent article les informations et éléments nécessaires pour réaliser le contrôle, et leur permettre d'accéder aux infrastructures essentielles faisant l'objet du contrôle afin d'effectuer des analyses et des relevés d'informations techniques.

L'opérateur de services essentiels communique en application de l'alinéa précédent les informations suivantes :

1. les informations nécessaires pour évaluer la sécurité de ses infrastructures essentielles, notamment la documentation technique des équipements et des logiciels utilisés dans ses systèmes ainsi que le cas échéant les codes sources de ces logiciels ;

2. les moyens nécessaires pour accéder à ses infrastructures essentielles et à l'ensemble de leurs composants afin de permettre au prestataire de réaliser des analyses sur les systèmes, notamment des relevés d'informations techniques.

L'opérateur de services essentiels conclut une convention le prestataire de service chargé d'effectuer le contrôle. Cette convention précise :

1. les infrastructures essentielles qui font l'objet du contrôle ;
2. les objectifs et le périmètre du contrôle ;
3. les modalités de déroulement du contrôle, notamment les conditions d'accès aux sites et aux infrastructures essentielles de l'opérateur ;
4. les informations nécessaires à la réalisation du contrôle, fournies par l'opérateur, et les conditions de leur protection ;
5. les modalités selon lesquelles sont effectuées les analyses techniques sur les infrastructures essentielles de l'opérateur.

La convention est conclue dans des délais compatibles avec le délai fixé pour la réalisation du contrôle. Une copie de la convention signée est adressée sans délai par l'opérateur à l'Agence nationale de la cybersécurité.

Le prestataire ayant réalisé le contrôle rédige un rapport exposant ses constatations, au regard de l'objectif du contrôle, sur le niveau de sécurité des infrastructures essentielles contrôlées et le respect des règles de sécurité prévues par le décret n° 2019-022/PR du 13 février 2019 portant attributions et organisation et fonctionnement de l'ANCy. Les vulnérabilités et les manquements aux règles de sécurité constatés lors du contrôle sont indiqués dans le rapport, qui formule le cas échéant des recommandations pour y remédier. Le rapport est couvert par le secret professionnel.

Après avoir mis l'opérateur en mesure de faire valoir ses observations, le prestataire remet, dans le délai fixé pour la réalisation du contrôle, le rapport à l'Agence nationale de la cybersécurité.

L'Agence nationale de la cybersécurité peut auditionner, dans un délai de deux (2) mois à compter de la remise du rapport, le prestataire ayant réalisé le contrôle, le cas échéant en présence de l'opérateur, aux fins d'examiner les constatations et les recommandations figurant dans le rapport. Elle peut inviter les autorités sectorielles concernées à assister à cette audition.

L'Agence nationale de la cybersécurité communique aux autorités sectorielles concernées les conclusions du contrôle.

Les agents de l'ANCy et les prestataires de services auxquels elle a recours sont astreints à des règles de confidentialité à l'égard des informations auxquelles ils ont accès dans le cadre des opérations de contrôle.

En cas de manquement constaté à l'occasion d'un contrôle, l'ANCy peut mettre en demeure l'opérateur de services essentiels concerné de se conformer, dans un délai qu'elle fixe, aux obligations qui lui incombent. Le délai est déterminé en tenant compte des conditions de fonctionnement de l'opérateur et des mesures à mettre en œuvre.

Si le contrôle confirme le respect par l'opérateur de services essentiels contrôlé des obligations qui lui incombent, l'ANCy lui délivre une accréditation.

Les conditions financières de réalisation des contrôles et de délivrance des accréditations sont fixées par décision de l'ANCy après avis de l'autorité de tutelle.

En cas de non-conformité à l'issue du délai fixé par la mise en demeure, l'ANCy peut prononcer à l'encontre de l'opérateur de services essentiels défaillant, des astreintes ou sanctions, y compris les sanctions pécuniaires prévues à l'article 19 du présent décret.

Article 16 : Les systèmes de détection ainsi que les prestataires qui exploitent ces systèmes doivent être qualifiés dans les conditions prévues par décision de l'ANCy.

Un opérateur de services essentiels peut agir comme prestataire de service exploitant des systèmes de détection au profit d'autres opérateurs de services essentiels ou pour ses propres besoins sous réserve d'être qualifié dans les conditions prévues à l'alinéa précédent.

Section 6 : Déclaration des incidents de sécurité

Article 17 : Les opérateurs de services essentiels déclarent, sans délai, après en avoir eu connaissance, à l'Agence nationale de la cybersécurité les incidents affectant les infrastructures essentielles, lorsque ces incidents ont ou sont susceptibles d'avoir, compte tenu notamment du nombre d'utilisateurs et de la zone géographique touchés ainsi que de la durée de l'incident, un impact significatif sur la continuité de ces services.

Après avoir consulté l'opérateur concerné, l'ANCy peut informer le public, les agences de cybersécurité d'autres Etats et les organismes de cybersécurité d'un incident mentionné au précédent alinéa, lorsque cette information est nécessaire pour prévenir ou traiter un incident.

Lorsqu'elle informe le public, les agences de cybersécurité des autres Etats ou les organismes de cybersécurité d'incidents, l'ANCy tient compte des intérêts économiques de ces opérateurs et veille à ne pas révéler d'informations susceptibles de porter atteinte à leur sécurité et au secret en matière commerciale et industrielle.

Article 18 : Après chaque incident mentionné à l'article 17 du présent décret, l'Agence nationale de la cybersécurité transmet au Premier ministre et aux ministres concernés une synthèse des informations recueillies.

CHAPITRE III - SANCTIONS ADMINISTRATIVES

Article 19 : Est puni de cinquante millions (50 000 000) à cent millions (100 000 000) de francs CFA d'amende le fait, pour un opérateur de services essentiels, de ne pas se conformer aux règles de sécurité qui lui incombent en vertu du présent décret et des décisions de l'ANCy à l'issue du délai fixé par la mise en demeure qui lui a été adressée en application de l'article 15 du présent décret.

Est puni de trente millions (30 000 000) de francs CFA d'amende le fait, pour un opérateur de services essentiels, de faire obstacle aux opérations de contrôle mentionnées à l'article 15 du présent décret.

Est puni de quinze millions (15 000 000) de francs CFA d'amende le fait, pour un opérateur de services essentiels, de ne pas satisfaire à l'obligation de déclaration d'incident prévue à l'article 17 du présent décret.

Article 20 : Les décisions de l'ANCy peuvent faire l'objet de recours devant une juridiction administrative.

CHAPITRE IV - DISPOSITIONS FINALES

Article 21 : Sont abrogées toutes les dispositions contraires au présent décret.

Article 22 : Le ministre des postes, de l'économie numérique et des innovations technologiques, le ministre de la sécurité et de la protection civile et le ministre de la défense et des anciens combattants sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret qui est publié au Journal officiel de la République togolaise.

Fait à Lomé, le 08 JUIL 2019

Le Président de la République

SIGNE

Faure Essozimna GNASSINGBE

Le Premier ministre

SIGNE

Selom Komi KLASSOU

Le ministre de la sécurité
et de la protection civile

SIGNE

Damehame YARK

Le ministre des postes, de l'économie
numérique et des innovations
technologiques

SIGNE

Cina LAWSON

Pour ampliation,
le Secrétaire général
de la Présidence de la République

Daté Patrick TEVI-BENISSAN

- **ANNEXE**

LISTE DES SERVICES ESSENTIELS AU FONCTIONNEMENT DE LA SOCIÉTÉ OU DE L'ÉCONOMIE

SECTEUR --- Sous-secteur	SERVICES ESSENTIELS
REGALIEN ---- Administration Publique	Activités civiles de l'Etat
	Activités fiscales de l'Etat
	Activités judiciaires
	Activités militaires de l'Etat
	Réseau e-gouvernement
	Messagerie professionnelle de l'administration publique
	Identification biométrique
ÉNERGIE --- Electricité	Vente ou revente d'électricité aux particuliers et entreprises (vente d'électricité aux consommateurs finaux, vente d'électricité aux fournisseurs d'électricité, exploitation d'une bourse de l'électricité)
	Distribution d'électricité (conduite et supervision du réseau de distribution, gestion des raccordements des consommateurs, pilotage des compteurs des consommateurs)
	Transport d'électricité (conduite et supervision du réseau de transport, équilibrage de l'offre et de la demande, gestion des interconnexions)
ÉNERGIE --- Pétrole	Exploitation d'oléoducs (conduite et supervision d'oléoducs)
	Production (conduite et supervision d'installations de production) Raffinage (conduite et supervision de raffineries) Stockage (conduite et supervision d'installations de stockage) Transport hors oléoducs (planification des transports, exploitation d'une flotte de navires ou camions)

	Service de transfert de données logistiques numérisées entre opérateurs pétroliers, et entre les opérateurs pétroliers et les autorités publiques
ÉNERGIE --- Gaz	Vente ou revente de gaz aux particuliers et entreprises (vente de gaz aux consommateurs finaux, vente de gaz aux fournisseurs de gaz, exploitation d'une bourse du gaz)
	Distribution de gaz (conduite et supervision du réseau de distribution, gestion des raccordements des consommateurs, pilotage des compteurs des consommateurs)
	Transport de gaz (conduite et supervision du réseau de transport, équilibrage de l'offre et de la demande, gestion des interconnexions)
	Stockage de gaz (conduite et supervision d'installations de stockage)
	Liquéfaction de gaz (conduite et supervision d'installations de liquéfaction) Déchargement et regazéification (conduite et supervision d'installations de déchargement, conduite et supervision d'installations de regazéification)
	Fourniture, distribution, transport, stockage et traitement de gaz
	Raffinage (conduite et supervision d'installations de raffinage) Traitement (conduite et supervision d'installations de traitement)
TRANSPORTS --- Transport aérien	Transport de passagers (enregistrement et embarquement des passagers, exploitation des aéronefs) Transport de fret (enregistrement et embarquement du fret, exploitation des aéronefs)
	Exploitation d'installations aéroportuaires (inspection-filtrage, enregistrement et embarquement du fret, gestion des passagers et des bagages) Avitaillement et armement des aéronefs

	Contrôle et régulation de la navigation aérienne en route Contrôle et régulation des aérodromes
	Maintenance et réparation aéronautiques
	Gestion des flux de passagers
TRANSPORTS --- Transport ferroviaire	Contrôle et gestion du trafic ferroviaire (supervision et régulation du trafic, signalisation, gestion des aiguillages, planification du trafic, gestion des sillons)
	Maintenance de l'infrastructure ferroviaire
	Transport de marchandises et de matières dangereuses (exploitation des matériels roulants) Transport de passagers (exploitation des matériels roulants, information et accueil des passagers, gestion des flux de passagers)
	Maintenance des matériels roulants
TRANSPORTS --- Transport guidé	Transport de passagers (exploitation des matériels de transports guidés, information et accueil des passagers)
TRANSPORTS --- Transport par voie d'eau	Transport de passagers (gestion des flux de passagers) Transport de marchandises et de matières dangereuses (réservation, enregistrement des marchandises) Planification des trajets
	Maintenance des navires
	Exploitation des infrastructures de transport par voie d'eau
	Service aux marchandises (chargement, déchargement, entreposage, gardiennage, gestion de conteneurs) Accueil des navires (pilotage, remorquage, lamanage, avitaillement) Information, accueil, inspection-filtrage, embarquement-débarquement des passagers Gestion des ouvrages portuaires
	Service de trafic maritime

	Service de trafic fluvial
TRANSPORTS --- Transport routier	Gestion de routes (entretien, signalisation, gestion des infrastructures, régulation et surveillance du trafic)
	Gestion de routes (entretien, signalisation, gestion des infrastructures, régulation et surveillance du trafic)
	Gestion centralisée d'une flotte de véhicules Aide à la gestion du trafic Information aux passagers Aide à l'exploitation
	Transport de marchandises et de matières dangereuses
	Gestion des flux de passagers Exploitation
TRANSPORTS	Organisation de transports Affrètement de transporteurs
TRANSPORT AERIEN	Protection des installations aéroportuaires (Systèmes de surveillance de contrôle d'accès et d'alarme de gestion de la riposte, systèmes de surveillance par télévision en circuit fermé) Transport de fret (gestion des bases de données d'agents habilités et/ ou d'expéditeurs connus) Coordination des activités de sûreté (systèmes de commandement, de contrôle et de répartition de la sûreté
LOGISTIQUE	Gestion de plateforme logistique
BANQUES	Gestion des dépôts Octroi de crédits Service de paiement Service d'investissement
INFRASTRUCTURES DE MARCHÉS FINANCIERS	Exploitation de plateformes de négociation d'instruments financiers
	Service de contrepartie centrale pour les transactions sur les marchés financiers (chambres de compensation)

	Tenue de registre Gestion des garanties (collatéral) Règlement-livraison de titres
SERVICES FINANCIERS	Service de paiement Emission de titres spéciaux
	Planification et exploitation des transports de fonds Gestion des demandes de collecte et d'approvisionnement
ASSURANCE	Assurance vie Assurance non vie Réassurance
SOCIAL	Calcul et paiement des prestations sociales (assurance maladie, vieillesse, allocations familiales et chômage) Gestion du recouvrement et de la trésorerie des organismes sociaux
EMPLOI ET FORMATION PROFESSIONNELLE	Calcul et paiement des aides à l'emploi
SANTÉ --- Etablissements de soins de santé (y compris les hôpitaux et les cliniques privées)	Service concourant aux activités de prévention, de diagnostic ou de soins
	Réception et régulation des appels Service mobile d'urgence et réanimation
SANTÉ --- Produits pharmaceutiques	Distribution pharmaceutique
FOURNITURE ET DISTRIBUTION D'EAU POTABLE	Fourniture d'eau en bouteille (puisage, embouteillage, planification, logistique, contrôle de la qualité de l'eau) Production d'eau courante (conduite, supervision et maintenance des installations de captation, de transport, de traitement et de stockage, contrôle de la qualité de l'eau) Distribution d'eau courante (conduite, supervision et maintenance des installations de distribution d'eau, logistique, contrôle de la qualité de l'eau)

TRAITEMENT DES EAUX NON POTABLES	Collecte des eaux usées Traitement des eaux usées
	Collecte et évacuation d'eaux pluviales
INFRASTRUCTURES NUMÉRIQUES	Services de communications électroniques au public Services de communications électroniques à haut et très haut débit Service d'interconnexion par appairage pour l'échange de trafic internet
	Enregistrement et gestion de noms de domaine Hébergement de noms de domaine
	Hébergement de zones de premier niveau
ÉDUCATION	Gestion d'affectations en parcours scolaire ou étudiant Organisation d'examens nationaux
	Gestion des bourses
RESTAURATION	Gestion des commandes Gestion de l'approvisionnement, de la logistique, du stockage et de la distribution
AVIATION CIVILE	Transport de passagers (enregistrement, contrôle des documents de voyages, embarquement et débarquement des passagers, exploitation des aéronefs) Transport de fret (enregistrement, contrôle des documents, chargement et déchargement du fret, exploitation des aéronefs)
	Exploitation d'installations aéroportuaires (Contrôle d'accès des personnes et des véhicules, Inspection-filtrage, enregistrement, chargement et déchargement du fret, gestion des passagers et des bagages) Avitaillement et armement des aéronefs Explosion d'aéronefs avec déversement de marchandises dangereuses dans le réseau public d'eau Interférence avec les systèmes de télécommunication aéronautiques sol-sol

	Contrôle et régulation de la navigation aérienne en route Contrôle et régulation des aérodromes Contrôles de l'évolution des aéronefs télé pilotés, drones (RPAS) au voisinage d'aéronefs dans les phases de décollage, atterrissage et phase en route Intégration des RPAS dans un espace aérien non réservé Interférence avec les systèmes de télécommunication aéronautiques air —sol Contrôle et gestion de l'information aéronautique Toute autre question émergente pouvant avoir des répercussions sur la sécurité et la régularité du système de navigation aérienne
	Maintenance et réparation aéronautique Protection des aides à la navigation aérienne (VOR ; ILS, DME) Rupture brusque du circuit électrique du balisage lumineux Interférences et perturbation des fréquences aéronautiques
	Gestion des flux des passagers (mécanisme d'enregistrement et de contrôle des bagages)
Port Autonome de Lomé	Le câblage électrique et informatique du PAL Le système de télésurveillance du PAL Le système VTS/AIS pour la communication avec les navires La couverture WI-FI du PAL La liaison WI-FI du PAL avec son partenaire technique ACL (installé dans la zone portuaire) La liaison radio avec la plateforme du Guichet Unique pour le Commerce Extérieur (GUCE) La plateforme du GUCE Le Datacenter local du PAL