WG

RÉPUBLIQUE DU BÉNIN

Fraternité-Justice-Travail

PRÉSIDENCE DE LA RÉPUBLIQUE

LOI N° 2020 – 35 DU 06 JANVIER 2021

modifiant la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

L'Assemblée nationale a délibéré et adopté en sa séance du 10 décembre 2020 ;

Le Président de la République promulgue la loi dont la teneur suit :

Article 1er : Les dispositions des articles 121, 125, 464 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin sont modifiées ainsi qu'il suit :

« **Article 121 nouveau :** Organes de l'Autorité de régulation

Les organes de l'Autorité de régulation des communications électroniques et de la poste sont le Conseil de régulation et le Secrétariat exécutif.

Le Conseil de régulation est constitué de cinq (05) conseillers.

Le Secrétariat exécutif est composé du Secrétaire exécutif et des autres membres du personnel ».

« Article 125 nouveau : Membres du Conseil de régulation

Les membres du Conseil de régulation sont désignés, à l'issue d'une procédure d'appel à candidatures, sur la base de leurs qualités morales, de leurs compétences et expériences professionnelles avérées dans le domaine des communications électroniques et de la poste aux plans technique, économique et/ou juridique.

Ils sont sélectionnés parmi des cadres ayant totalisé au moins dix (10) ans d'expérience professionnelle.

Ils sont nommés par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques, pour un mandat de cinq (05) ans, renouvelable une fois.

Les modalités de la procédure d'appel à candidatures sont fixées par décret pris en Conseil des ministres.

Avant la fin de leur mandat, les membres du Conseil de régulation ne peuvent être suspendus ou révoqués que pour faute lourde dûment constatée ».

« **Article 464 nouveau :** Composition

L'Autorité de protection des données à caractère personnel est composée de huit (08) membres ainsi qu'il suit :

- trois (03) députés désignés par l'Assemblée nationale en tenant compte de sa configuration politique ;

- deux (02) personnes qualifiées pour leur connaissance des services de communications électroniques ayant un diplôme sanctionnant au moins cinq (05) années d'études universitaires et totalisant au moins dix (10) années d'expérience, désignées par l'Assemblée nationale, en tenant compte de sa configuration politique ;

- une (01) personnalité désignée par le président de la République ;

- un (01) magistrat élu par ses pairs ;

- un (01) avocat ayant au moins quinze (15) années d'expérience, élu par ses pairs.

L'Autorité est dirigée par un Bureau composée d'un président et d'un rapporteur élus en son sein ».

Article 2 : La dénomination « ministre des Communications électroniques et de la Poste » ou « ministre chargé des Communications électroniques et de la Poste » est remplacée par celle de « ministre chargé des Communications électroniques dans toutes les dispositions de la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

Article 3 : Nonobstant les dispositions de la présente loi relatives à la composition de l'Autorité de régulation des communications électroniques et de la poste et de l'Autorité de protection des données à caractère personnel,

les membres en exercice restent en fonction jusqu'à l'installation des nouvelles mandatures.

Article 4 : La présente loi sera publiée au Journal officiel et exécutée comme Loi de l'Etat.

Fait à Cotonou, le 06 janvier 2021

Par le Président de la République,
Chef de l'État, Chef du Gouvernement,

Patrice TALON.-

Le Garde des Sceaux, Ministre de
la Justice et de la Législation,

Séverin Maxime QUENUM

Le Ministre du Numérique
et de la Digitalisation,

Aurelie I. ADAM SOULE ZOUMAROU

AMPLIATIONS : PR 6 – AN 4 – CC 2 – CS 2 – HCJ 2 – CES 2 – HAAC 2 – MJL 2 – MENC 2 – AUTRES MINISTERES 22 – SGG 4 – JORB 1.

REPUBLIQUE DU BENIN

FRATERNITE – JUSTICE - TRAVAIL

ASSEMBLEE NATIONALE

Loi n° 2017-20 portant code du numérique en République du Bénin.

L'Assemblée nationale a délibéré et adopté en sa séance du mardi 13 juin 2017, la loi dont la teneur suit:

Légi Bénin

LIVRE PRELIMINAIRE

DES DEFINITIONS ET DE L'OBJET

Article 1er : Définitions

Au sens du présent code, on entend par :

- Abonné : toute personne physique ou morale qui utilise et paie un service de communications électroniques en vertu d'un contrat, conformément aux modalités établies par l'opérateur ;

- Accès :

▪ au sens du Livre I : toute mise à disposition d'infrastructures, passives ou actives, de moyens, matériels ou logiciels, ou de services, en vue de permettre au bénéficiaire d'exploiter un réseau de communications électroniques ou de fournir des services de communications électroniques, y compris les prestations associées telle que la co-localisation ;

▪ au sens du Livre VI : pénétration directe ou indirecte dans l'intégralité ou une partie quelconque d'un système informatique. La pénétration indirecte s'entend de l'accès intervenant via un réseau de communications électroniques de quelque nature que ce soit. Le mode de communication utilisé pour ledit accès est non pertinent ;

- Accès illégal : accès sans droit à un système informatique ou tout comportement sans droit susceptible de mettre en péril ou mettant en péril la confidentialité, l'intégrité et la disponibilité de données informatiques ;

- Accès/service universel : offre minimale au public sur l'ensemble du territoire national de services de communications électroniques à un prix abordable et ce, dans le respect des principes d'égalité, de continuité et d'universalité ;

- ABSU-CEP : Agence Béninoise de Service Universel des Communications Électroniques et de la Poste définie à l'article 109 du présent code ;

- Altérer **:** modifier ;

- APDP : Autorité de Protection des Données à caractère Personnel ;

- ANSSI-BÉNIN : Agence Nationale de Sécurité des Systèmes d'Informations en charge de contrôler le niveau de sécurité des systèmes d'informations en République du Bénin ;

- Assignation d'une fréquence ou d'un canal radioélectrique : toute autorisation accordée à un opérateur d'utiliser une ou plusieurs fréquences selon des conditions spécifiées ;

- Atteinte à l'intégrité des données : tout acte intentionnel susceptible de mettre ou mettant en péril la sécurité des données ;

- Atteinte à l'intégrité d'un système **:** tout acte intentionnel entravant l'usage légitime de systèmes informatiques, y compris de systèmes de communications électroniques, en utilisant ou en influençant des données informatiques ;

- Attribution d'une bande de fréquence **:** inscription dans le tableau d'attribution des bandes de fréquences, d'une bande de fréquences déterminée, aux fins de son utilisation par un ou plusieurs services ;

- Autorisation : acte administratif de l'Autorité de régulation qui confère à un opérateur un ensemble de droits et d'obligations spécifiques en vertu desquels cet opérateur est fondé à exercer certaines activités de communications électroniques conformément aux dispositions du présent code ;

- Autorité compétente **:** autorité désignée par voie législative ou réglementaire en charge de superviser les activités de fourniture d'outils électroniques et de services de confiances conformément aux dispositions du présent code ;

- Autorité de protection des données à caractère personnel ou Autorité de contrôle **:** autorité nationale administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions du Livre V. Cette Autorité est habilitée à conduire des investigations ou engager des poursuites en cas de non-respect des dispositions précitées. Cette Autorité est dénommée Autorité de Protection des Données Personnelles (APDP) en République du Bénin ;

- Autorité de régulation **:** autorité de régulation des communications électroniques et de la poste chargée de réguler les activités de communications électroniques et de la poste ;

- Boucle locale et sous-boucle locale : Circuit physique qui relie les points de terminaison d'un réseau de communications électroniques dans les locaux des abonnés au répartiteur principal ou à toute autre installation équivalente du réseau de communications électroniques d'un opérateur ;

- Cachet électronique : données électroniques, jointes ou associées logiquement à d'autres données électroniques afin de garantir l'origine et l'intégrité de ces dernières ;

- Cachet électronique avancé : cachet électronique qui satisfait aux exigences énoncées à l'article 294 du présent code ;

- Cachet électronique qualifié : cachet électronique avancé créé à l'aide d'un dispositif de création de cachet électronique qualifié et qui repose sur un certificat qualifié de cachet électronique ;

Legibenin

- Cahier des charges : document intégrant les conditions techniques et les modalités d'exploitation imposées à tout opérateur ou fournisseur de services postaux ou de services de communications électroniques ouverts au public ;

- CEDEAO : Communauté Économique des États de l'Afrique de l'Ouest ;

- Certificat d'authentification de site Internet : attestation permettant d'authentifier un site internet et l'associant à la personne physique ou morale à laquelle le certificat est délivré ;

- Certificat de cachet électronique : attestation électronique qui associe les données de validation d'un cachet électronique à une personne morale et confirme le nom de cette personne ;

- Certificat de signature électronique : attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne ;

- Certificat qualifié d'authentification de site Internet **:** certificat d'authentification de site internet, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'article 304 ;

- Certificat qualifié de cachet électronique **:** certificat de cachet électronique délivré par un prestataire de services de confiance qualifié, et qui satisfait aux exigences fixées par voie réglementaire ;

- Certificat qualifié de signature électronique : certificat de signature électronique délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées par voie réglementaire ;

- CNIL : Commission Nationale de l'Informatique et des Libertés. Désormais connue sous la dénomination APDP

- CNUDCI : Commission des Nations-Unies pour le droit commerciale international ;

- Code : le présent code du numérique ;

- Code de conduite : chartes d'utilisation élaborées par le responsable du traitement afin d'instaurer un usage correct des ressources informatiques, de l'internet et des communications électroniques au sein de la structure concernée ;

- Code pénal : loi portant code pénal et ensemble des dispositions législatives réprimant des infractions pénales en vigueur au Bénin ;

- Collecte en temps réel : rassemblement des preuves contenues dans des communications en cours de production, lequel rassemblement est réalisé au moment de la transmission de la communication ;

- Colocalisation : prestation offerte par un opérateur à d'autres opérateurs et consistant en une mise à leur disposition d'infrastructures, y compris des locaux, afin qu'ils y installent leurs équipements.

Le terme colocalisation couvre également les prestations de colocalisation offertes dans un bâtiment aménagé à cet effet adjacent ou distant du point de terminaison objet d'un accord d'accès et/ou d'interconnexion ;

- Commerce électronique : activité économique par laquelle une personne propose ou assure par voie de communications électroniques la fourniture de biens ou de services. Entrent également dans le champ du commerce électronique les services tels que ceux consistant à

Légi-Bénin

fournir des informations en ligne, des communications commerciales et des outils de recherche, d'accès et/ou de récupération de données, d'accès à un réseau de communications ou d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent ;

- Commission cryptologie : Commission au sein de l'ANSSI-BENIN en charge de la cryptologie au Bénin ;

- Communication électronique : toute émission, toute transmission et toute réception de signes, de signaux, d'écrits, d'images, de sons ou d'informations de toute nature par fil, fibre optique, radioélectricité ou autres systèmes électromagnétiques ;

- Confidentialité : état de sécurité permettant de garantir le secret des informations et ressources stockées dans les réseaux et systèmes de communication électroniques, systèmes d'information et/ou des équipements terminaux, afin d'en prévenir la divulgation non autorisée d'informations à des tiers, par la lecture, l'écoute, la copie illicite d'origine intentionnelle ou accidentelle durant leur stockage, traitement ou transfert ;

- Consentement de la personne concernée : toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel accepte par une déclaration ou par un acte positif clair que les données à caractère personnel le concernant fassent l'objet d'un traitement ;

- Conservation des données : conservation des données dans l'état dans lequel elles se trouvent en les protégeant contre tout ce qui pourrait en modifier ou dégrader la qualité ou l'état actuel ;

- Consommateur : toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale ou libérale ;

- Coût net : différence entre les coûts d'investissement et d'exploitation nécessaires à la fourniture de l'accès/service universel et les recettes pertinentes ; les recettes pertinentes étant les recettes directes et indirectes induites par l'accès/service universel ;

- Créateur de cachet : personne morale qui crée des cachets électroniques ;

- Cryptologie : science relative à la protection et à la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation ;

- Déclaration : notification à l'Autorité de régulation faite par toute personne dans les conditions prévues à l'article 55 du présent code et contre remise d'un récépissé ;

- Dégroupage de la boucle-locale : prestation qui inclut également les prestations associées, notamment celle de colocalisation, offerte par opérateur pour permettre à un autre opérateur d'accéder à tous les éléments de la boucle locale du premier exploitant pour desservir directement ses abonnés ;

- Destinataire :

▪ personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers ;

▪ les instances administratives ou judiciaires susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une enquête particulière conformément au Livre V ne sont toutefois pas considérées comme des destinataires. Le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;

Legibenin

- Diffusion : action consistant à transmettre des données à autrui ;

- Dispositif : matériel ainsi que solutions basées sur des logiciels dans l'intention de commettre l'une des infractions visées au Livre VI du présent code. Ces dispositifs sont, sans s'y limiter :

- les éléments capables de couper l'alimentation électrique d'un système informatique ;
- les éléments de stockage, tels que les disques durs, les cartes mémoire, les disques compacts et les bandes ;

- les périphériques d'entrée, tels que les claviers, les souris, les pavés tactiles, les scanners et les appareils photo numériques ; et

- les périphériques de sortie, tels que les imprimantes et les écrans ;

- Documents administratifs : tout document reçu, produit ou détenu par un organisme public dans le cadre de ses missions ou de ses attributions, notamment les correspondances, faits, opinions, avis, mémorandums, données, statistiques, livres, dessins, plans, cartes, diagrammes, photographies et enregistrements audiovisuels ou électroniques ;

- Données à caractère personnel : toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée.

Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

- Données afférentes à la création de signature : données uniques telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique sécurisée ;

- Données biométriques : toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques ;

- Données concernant la santé : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

- Données de création de cachet électronique : données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

- Données d'identification personnelle : ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

- Données génétiques : toute information concernant les caractères génétiques héréditaires ou acquis d'une personne physique qui donnent des indications uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;

Legibenin

- Données informatiques : toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

- Données relatives aux abonnés : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

▪ le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

▪ l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

▪ toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;

- Données relatives au contenu : contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication. Il s'agit de tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic ;

- Données relatives au trafic : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

- Données sensibles : toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, à la génétique, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

- Droits de passage : droits permettant de mettre en place des infrastructures et équipements nécessaire à l'exploitation d'un réseau de communications électroniques ou à la fourniture d'un service de communications électroniques sur, au-dessus ou au-dessous de propriétés privées et/ou publiques ;

- Effacer : action de détruire des objets corporels qui en deviennent méconnaissables ;

- Emissions électromagnétiques : émissions pouvant provenir d'un ordinateur en fonctionnement. Elles ne sont pas considérées comme des données informatiques au sens des définitions ci-dessus. Cependant, des données peuvent être reconstituées à partir de telles émissions ;

- Entraver : actions de porter atteinte au bon fonctionnement du système informatique ou de tout autre équipement électronique. Elle résulte de l'introduction, du transfert, de l'endommagement, de l'effacement, de l'altération ou de la suppression de données informatiques. En relation avec un système informatique, l'entrave peut consister, sans s'y limiter, à :

- couper l'alimentation électrique d'un système informatique ;
- provoquer des interférences électromagnétiques dans un système informatique ;
- corrompre un système informatique par quelque moyen que ce soit ;

Loi Benin

▪ introduire, transmettre, endommager, effacer, détériorer, altérer ou supprimer des données informatiques ;

- Equipement terminal : tout équipement destiné à être connecté directement ou indirectement à un point de terminaison d'un réseau en vue de la transmission, de la réception, du traitement ou de la visualisation d'informations ; ne sont pas visés les équipements permettant d'accéder à des services de radiodiffusion et télévision diffusés par voie hertzienne ou distribués par câble, sauf dans les cas où ils permettent d'accéder également à des services de communications électroniques ;

- Escroquerie : le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation à décharge ;

- Etablissement principal :

▪ en ce qui concerne le responsable du traitement établi dans plusieurs pays, le lieu de son administration centrale, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal ;

▪ en ce qui concerne un sous-traitant établi dans plusieurs pays, le lieu de son administration centrale ou, si ce sous-traitant ne dispose pas d'une administration centrale, l'établissement du sous-traitant où se déroule l'essentiel des activités de traitements effectués dans le cadre des activités d'un établissement du sous-traitant, dans la mesure où le sous-traitant est soumis à des obligations spécifiques en vertu du présent code ;

- Etat : République du Bénin ;

- Etat tiers : tout Etat non membre de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) ;

- Exigences essentielles : ensemble des règles qui sont nécessaires pour garantir dans l'intérêt général :

- la sécurité des usagers et du personnel exploitant des réseaux de communications électroniques ;
- la surveillance d'éventuelles activités criminelles ;
- le respect des libertés individuelles et de la vie privée ;
- la protection des réseaux et notamment des échanges d'informations de commande et de gestion qui y sont associés ;
- la bonne utilisation du spectre radioélectrique, le cas échéant ;
- l'interopérabilité des services, des réseaux et des équipements terminaux ainsi que la protection des données, dans les cas justifiés ;

Légibenin

- la protection de l'environnement et les contraintes d'urbanisme et d'aménagement du territoire ;

- Exploitant d'infrastructures alternatives : toute personne qui détient, exploite ou assure la gestion d'infrastructures ou de droits pouvant supporter ou contribuer à supporter des réseaux de communications électroniques, sans exercer elle-même les activités d'un opérateur ;

- Fichier : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;

- Flux transfrontières de données à caractère personnel : circulation de données à caractère personnel au-delà des frontières nationales ;

- Fournisseur d'accès : toute personne physique ou morale qui fournit un service de transmission électronique de données en transmettant des informations fournies par ou à un utilisateur du service dans un réseau de communication, ou qui fournit un accès à un réseau de communication ;

- Fournisseur de cache : toute personne physique ou morale fournissant un service de transmission électronique de données par stockage automatique, intermédiaire et temporaire des informations, dans le but de rendre plus efficace la transmission des informations ;

- Fournisseur de liens hypertextes : toute personne physique ou morale qui fournit un ou plusieurs liens hypertexte ;

- Fournisseur de services en ligne : personne physique ou morale qui assure, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services. Il peut notamment s'agir de :

- d'entités publiques ou privées qui offrent aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique ;

- d'entités traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs ;

- Fréquence Radioélectrique : nombre de cycles par seconde à partir duquel un courant électrique analogique change de sens ; elle est généralement mesurée en hertz (Hz). Un hertz est égal à un cycle par seconde ;

- Gestion du spectre des fréquences : ensemble des actions administratives et techniques visant à assurer une utilisation rationnelle et efficace du spectre des fréquences radioélectriques par les utilisateurs ;

- HAAC : Haute Autorité de l'Audiovisuel et de la Communication ;

- Hébergeur : toute personne physique ou morale qui fournit un service de transmission électronique de données en stockant les informations fournies par l'utilisateur du service ;

- Horodatage électronique : données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant ;

- Horodatage électronique qualifié : horodatage électronique qui satisfait aux exigences fixées à l'article 300 du présent code ;

Légi-Bénin

- Identification électronique : processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale ;

- Information : tous signes, tous signaux, tous écrits, toutes images, tous sons ou tous enregistrements de toutes natures pouvant être véhiculés par des procédés de communications électroniques ;

- Information sur le régime des droits : toute information fournie par les titulaires de droits qui permet d'identifier l'œuvre ou tout autre objet protégé, l'auteur ou autre titulaire de droits, les informations sur les conditions et modalités d'utilisation de l'œuvre ou autre objet protégé ainsi que tout numéro ou code représentant ces informations ;

- Infrastructure alternative : toute installation ou ensemble d'installations pouvant assurer ou contribuer à assurer la transmission et/ou l'acheminement de signaux de communications électroniques ;

- Infrastructure essentielle : toute infrastructure de communications électroniques actives ou passives ou toute infrastructure alternative qui ne peut être reproduite dans des conditions économiques raisonnables et pour laquelle il n'existe pas de substitut réel ou potentiel permettant de fournir les mêmes services avec une qualité de service comparable ou des services sur un marché amont, aval ou connexe ;

- Infrastructure sensible ou critique : point, système ou partie de celui-ci, situé sur le territoire de la République du Bénin et qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, comme les centrales électriques, les réseaux de transport et les réseaux publics, et dont l'arrêt ou la destruction aurait un impact significatif sur la République du Bénin du fait de la défaillance de ces fonctions ;

- Installation de communications électroniques : tous équipements, appareils, câbles, éléments d'infrastructures et dispositifs électriques, systèmes radioélectriques ou optiques ou tout autre système technique pouvant servir aux technologies de l'information et de la communication ou à toute autre opération qui y est directement liée ;

- Intégrité : état de sécurité assurant qu'un réseau de communications électroniques, système d'information ou équipement terminal qui est demeuré intact et que les ressources et informations qui y sont stockées n'ont pas été altérées, modifiées ou détruites, d'une façon intentionnelle ou accidentelle, de manière à assurer leur exactitude, leur fiabilité et leur pérennité ;

- Interception : acquisition, prise de connaissance, saisie ou copie du contenu ou d'une partie du contenu de toute communication, y compris les données relatives au contenu, les données informatiques, les données relatives au trafic, lors de transmissions non publiques par le biais de moyens techniques. L'interception comprend, sans que cette liste soit limitative, l'écoute, le contrôle ou la surveillance du contenu des communications et l'obtention du contenu des données, soit directement, au moyen de l'accès aux systèmes d'information et de leur utilisation, soit indirectement, au moyen de l'utilisation de dispositifs d'écoute électroniques ou de dispositifs d'écoute par des moyens techniques ;

- Interconnexion : liaison physique et logique des réseaux de communications électroniques utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre, ou bien d'accéder aux services fournis par une autre entreprise ; ces services peuvent être fournis

Legibenin

par les parties concernées ou par d'autres parties qui ont accès au réseau ; l'interconnexion constitue un type particulier d'accès mis en œuvre entre opérateurs de réseaux publics. Les prestations d'interconnexion comprennent également les prestations associées telle que la colocalisation ;

- Interconnexion des données à caractère personnel : tout mécanisme de connexion consistant en la mise en relation de données traitées pour une finalité déterminée avec d'autres données traitées pour des finalités identiques ou non, ou liées par un ou plusieurs responsables de traitement ;

- Interopérabilité des équipements terminaux : aptitude d'un équipement à fonctionner, d'une part, avec le réseau auquel il est connecté et, d'autre part, avec l'ensemble des autres équipements terminaux connecté à un réseau et qui permettent d'accéder à un même service ;

- Introduction de données : manipulations à l'entrée du système de données inexactes, manipulations de programmes ou autres ingérences dans le traitement des données ;

- Itinérance nationale ou national roaming : toute forme de partage d'infrastructures actives, permettant aux abonnés d'un opérateur mobile d'avoir accès au réseau et aux services offerts par un autre opérateur mobile offrant ladite itinérance dans une zone non couverte par le réseau nominal desdits abonnés ;

- Licence : tout droit attribué par décret, portant approbation d'un cahier des charges, à toute personne qui répond aux conditions prévues au présent code et qui s'engage à en respecter les dispositions ; elle définit les modalités et les conditions suivant lesquelles le titulaire de la licence est autorisé à exercer son activité de communications électroniques et fixe les droits et obligations de celui-ci ;

- Lien hypertexte : caractéristique ou propriété d'un élément tel qu'un symbole, un mot, une phrase ou une image qui contient des informations sur une autre source et qui renvoie et affiche un autre document lorsqu'elle est exécutée ;

- Limitation du traitement **:** marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur ;

- Loteries sur Internet : toutes opérations offertes au public sur internet, sous quelque dénomination que ce soit, pour faire naître l'espérance d'un gain qui serait dû, même partiellement au hasard et pour lesquelles une contrepartie financière est exigée ;

- Matériel raciste et xénophobe : tout matériel écrit, toute image ou toute autre représentation d'idées ou de théories qui préconise ou encourage la haine, la discrimination ou la violence, contre une personne ou un groupe de personnes, en raison de la race, de la couleur, de l'ascendance ou de l'origine nationale ou ethnique, ou de la religion, dans la mesure où cette dernière sert de prétexte à l'un ou l'autre de ces éléments, ou qui incite à de tels actes ;

- Mesure de sécurité : toute utilisation des procédures, des dispositifs ou des programmes informatiques spécialisés à l'aide desquels l'accès à un système informatique est limité ou interdit pour certaines catégories d'utilisateurs ;

- Mineur : toute personne âgée de moins de dix-huit (18) ans ;

- Mise à disposition : action consistant à mettre, entre autres, des dispositifs, matériels, et informations en ligne pour qu'ils soient utilisés par autrui ;

- Monétique : ensemble des techniques informatiques et électroniques appliquées à la réalisation des transactions bancaires ;

Leg-Bénin

- Moyen de stockage de données informatiques : tout objet ou support à partir duquel des informations peuvent être reproduites, avec ou sans l'aide d'un autre objet ou dispositif;

- Moyen d'identification électronique : élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour authentifier un utilisateur de services en ligne ;

- Moyens techniques : dispositifs techniques connectés aux lignes de transmission ainsi que dispositifs de collecte et d'enregistrement de communications sans fil. Ils peuvent entre autres consister en des logiciels, mots d'accès et codes ;

- MVNO ou Mobile Virtual Network Operator ou Opérateur de réseau mobile virtuel : tout opérateur de téléphonie mobile ne possédant pas d'autorisation d'utilisation de fréquences radioélectriques ni d'infrastructures de radiocommunications qui contracte avec les opérateurs de radiocommunication afin de fournir aux utilisateurs des services de communications électroniques mobiles ;

- Normes : ensemble des spécifications techniques des équipements et des protocoles associés nécessaires au fonctionnement et à l'interopérabilité d'un réseau de communications électroniques ;

- Numéro : toute chaîne de chiffres indiquant de façon univoque le point de terminaison du réseau public ; ce numéro contient l'information nécessaire pour acheminer l'appel jusqu'à ce point de terminaison. Il peut avoir un format national ou international ; le format international est connu comme le numéro de communication électronique publique internationale qui comporte l'indicatif du pays et les chiffres subséquents ;

- Opérateur : toute personne physique ou morale exploitant un réseau de communications électroniques ou fournissant un service de communications électroniques. Les opérateurs sont impérativement soumis au régime de la licence, de l'autorisation ou de l'entrée libre avec ou sans déclaration ;

- Opérateur fournissant un accès à internet : tout opérateur offrant un service permettant un accès à internet à des personnes physiques ou morales, à titre lucratif ou non ;

- Opérateur national : tout opérateur titulaire d'une licence ou d'une autorisation ou ayant réalisé une déclaration en République du Bénin, ou bénéficiant du droit d'exploiter un réseau de communications électroniques ou de fournir des services de communications électroniques au titre des articles 48, 54 et 57 du présent code ;

- Opérateur non national : tout opérateur dûment autoriséà exercer des activités de communications électroniques dans un autre État membre de la CEDEAO que la République du Bénin et ne bénéficiant pas du droit d'exploiter un réseau de communications électroniques ou de fournir des services de communications électroniques au titre des articles 48, 54 et 57 du présent code ;

- Opérateur de radiocommunication : opérateur exploitant un réseau de communications électroniques nécessitant l'utilisation de fréquences radioélectriques soumises à une autorisation préalable de l'Autorité de régulation ;

- Opérateur dominant : tout opérateur disposant sur un marché de services ou d'un groupe de services une puissance significative, équivalent au moins à 25 % du volume ou de la valeur de ce marché ;

Log-Bénin

- Ordinateur : appareil électronique capable, en appliquant des instructions prédéfinies, d'effectuer des traitements automatisés de données et d'interagir avec l'environnement grâce à des périphériques comme l'écran, le clavier, la souris etc. ;

- Organe de Contrôle : organe créé par voie légale ou réglementaire, chargé de contrôler les activités des prestataires de services de confiance, conformément aux dispositions de l'article 317 du présent code ;

- Organisme d'évaluation de la conformité : tout organisme qui effectue des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection ;

Organisme public : l'État, les collectivités territoriales et les personnes de droit public chargées d'une mission de service public ;

- Pédopornographie/pornographie enfantine :

▪ tout matériel représentant de manière visuelle un enfant se livrant à un comportement sexuellement explicite, réel ou simulé ;

▪ toute représentation des organes sexuels d'un enfant à des fins principalement sexuelles ;

▪ tout matériel représentant de manière visuelle une personne qui paraît être un enfant se livrant à un comportement sexuellement explicite, réel ou simulé, ou toute représentation des organes sexuels d'une personne qui paraît être un enfant, à des fins principalement sexuelles ; ou

▪ images réalistes d'un enfant se livrant à un comportement sexuellement explicite ou des images réalistes des organes sexuels d'un enfant à des fins principalement sexuelles ;

- Personne concernée par un traitement de données à caractère personnel : toute personne physique dont les données à caractère personnel font l'objet d'un traitement **;**

- Piratage informatique : accès sans autorisation à un système informatique. Il est utilisé pour accéder à des informations confidentielles ou encore pour altérer ou endommager les systèmes et les données qu'elles peuvent comporter. Les attaques pirates peuvent être dirigées vers tous les systèmes informatiques: ordinateur, compte de messagerie personnelle, serveur de grandes compagnies ou infrastructure de sécurité d'un Etat ;

- Plainte : toute requête écrite adressée à l'Autorité de régulation pour faire reconnaître un droit que l'auteur estime posséder ou pour manifester une insatisfaction contre un opérateur ;

- Plan national de numérotation : plan organisant la ressource constituée par l'ensemble des numéros et permettant notamment d'identifier les points de terminaison fixes ou mobiles des réseaux et services téléphoniques, d'acheminer les appels et d'accéder à des ressources internes aux réseaux ; ce plan fixe les procédures et les conditions de réservation et d'attribution des ressources de numérotation et correspond à un segment du plan de numérotation mondial E 164 ;

- Point de terminaison : point de connexion physique répondant à des spécifications techniques, nécessaires pour avoir accès à un réseau de communications électroniques et communiquer efficacement par son intermédiaire ; ce point fait partie intégrante du réseau et ne constitue pas en soi un réseau de communications électroniques. Lorsqu'un réseau de communications électroniques est connecté à un réseau étranger, les points de connexion à ce réseau sont considérés comme des points de terminaison ; en cas de réseaux de radiocommunications

LegiBenin

mobiles, les interfaces aériennes des équipements terminaux mobiles sont considérées comme points de terminaison ;

- Portabilité des numéros : possibilité pour un utilisateur d'utiliser le même numéro d'abonnement, indépendamment de l'opérateur chez lequel il est abonné et même dans le cas où il change d'opérateur ;

- Possession : détention ou jouissance d'une chose ou d'un droit qu'une personne tient ou qu'elle exerce par elle-même, ou par une autre qui la tient ou qui l'exerce en son nom ;

- Prestataire de service de confiance : personne physique ou morale qui fournit un ou plusieurs services de confiance ;

- Prestataire de service de confiance qualifié : prestataire de services de confiance qui fournit un ou plusieurs services de confiance ayant obtenu le statut qualifié ;

- Professionnel : toute personne physique ou morale qui, pour les pratiques commerciales relevant du Livre IV, agit à des fins qui entrent dans le cadre de son activité, commerciale, industrielle, artisanale ou libérale, et toute personne agissant au nom ou pour le compte d'une telle personne ;

- Professionnel des soins de santé : toute personne définie comme telle par la législation nationale ;

- Profilage : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ;

- Programme informatique : ensemble ordonné d'instructions pouvant être exécutées par l'ordinateur pour obtenir le résultat attendu ;

- Prospection directe : tout envoi de message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services ;

- Pseudonymisation : traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ;

- Radiocommunications : les communications réalisées à l'aide d'ondes radioélectriques ;

- Recel : le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. C'est aussi le fait en toute connaissance de cause, de bénéficier par tout moyen, du produit d'un crime ou d'un délit ;

- Règlement des radiocommunications : manuel publié par l'UIT contenant les recommandations relatives à la radiocommunication ; il définit le service de radiocommunication comme un service impliquant la transmission, l'émission ou la réception d'ondes radioélectriques à des fins spécifiques de télécommunications ;

Legibenin

- Représentant : toute personne physique ou morale expressément désignée par le responsable du traitement ou le sous-traitant, qui agit en lieu et place de ce dernier et peut être contactée à sa place par les autorités de contrôle et d'autres entités dans la CEDEAO, ainsi que les Autorités d'Etats tiers, en ce qui concerne les obligations du responsable du traitement en vertu du Livre V ;

- Réseau : ensemble connecté de systèmes informatiques, quel que soit leur mode de connexion. Les connexions peuvent être reliées à la terre, sans fil ou les deux. Un réseau peut être géographiquement limité à une zone peu étendue ou couvrir une zone étendue et de tels réseaux peuvent eux-mêmes être interconnectés ;

- Réseau de communications électroniques **:** toute installation ou tout ensemble d'installations de transport ou de diffusion ainsi que, le cas échéant, les autres moyens assurant l'acheminement de communications électroniques, notamment ceux de commutation et de routage ;

- Réseau indépendant : tout réseau de communications électroniques réservé à un usage privé ou partagé. Un réseau indépendant est appelé :

▪ à usage privé lorsqu'il est réservé à l'usage de la personne physique ou morale qui l'établit ;

▪ à usage partagé, lorsqu'il est réservé à l'usage de plusieurs personnes physiques ou morales constituées d'un ou de plusieurs groupes fermés d'utilisateurs, en vue d'échanger des communications électroniques au sein du même groupe.

- Réseau interne : tout réseau indépendant entièrement établi sur une même propriété, sans emprunter ni le domaine public y compris hertzien, ni l'espace atmosphérique ni une propriété tierce ;

- Réseau ouvert au public : tout réseau de communications électroniques établi et/ou exploité pour fournir des services de communications électroniques au public, y compris des capacités nationales et internationales ;

- Réseau, installation et équipement terminal radioélectriques : un réseau, une installation ou un équipement terminal sont qualifiés de radioélectriques lorsqu'ils utilisent des fréquences hertziennes pour la propagation des ondes électromagnétiques en espace ; au nombre des réseaux radioélectriques figurent notamment les réseaux utilisant les capacités des satellites ;

- Responsable du traitement : toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens ;

- Saisir : en relation avec un système informatique, sans s'y limiter :

▪ activer tout système informatique et moyen de stockage des données informatiques sur site ;

▪ faire et conserver une copie des données informatiques, en utilisant notamment l'équipement sur site ;

▪ maintenir l'intégrité de ces données informatiques stockées ;

▪ rendre inaccessible ou retirer les données informatiques du système informatique auquel on a accédé ;

▪ sortir sur imprimante les données informatiques ; ou

Registered

▪ saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un moyen de stockage des données informatiques ;

- Sans droit : le fait :

▪ d'agir sans habilitation ou sans autorisation en vertu d'une loi, d'un contrat et/ou de l'entité privée ou publique compétente ; et/ou

▪ de dépasser les limites de son habilitation ou de son autorisation ;

- Schéma d'identification électronique : système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales ;

- Sécurité de données informatiques : confidentialité, intégrité et disponibilité de données informatiques ;

- Sélection du transporteur : mécanisme qui permet à un utilisateur de choisir entre un ensemble d'exploitants d'opérateur pour acheminer une partie ou l'intégralité de ses appels ;

- Service d'envoi recommandé électronique : service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée ;

- Service d'envoi recommandé électronique qualifié : service d'envoi recommandé électronique qui satisfait aux exigences fixées à l'article 275 du présent code ;

- Service de confiance : services considérés comme essentiels à la création de la confiance en l'économie numérique et encadrés par le Livre III du présent code ;

- Service de confiance qualifié : service de confiance qui satisfait aux exigences de l'article 322 du présent code ;

- Service de radiocommunication : tout service impliquant la transmission, l'émission ou la réception de fréquences radioélectriques se propageant dans l'espace sans guide artificiel à des fins spécifiques de communications électroniques ;

- Services de communications électroniques : toutes prestations incluant l'émission, la transmission ou la réception de signes, de signaux, d'écrits, d'images, de sons ou d'informations de toute nature ou une combinaison de ces fonctions ;

- Services à valeur ajoutée : tous services de communications électroniques qui, n'étant pas des services de diffusion et utilisant des services supports ou les services de communications électroniques, ajoutent d'autres services au service support ou répondent à de nouveaux besoins spécifiques de communication ;

- Service téléphonique au public : exploitation commerciale pour le public du transfert direct de la voix en temps réel au départ et à destination de réseaux commutés ouverts au public entre utilisateurs fixes ou mobiles ;

- Servitudes : obligations grevant les propriétés privées au profit du domaine public ou dans un but d'intérêt général. Elles sont instituées notamment, en vue de la protection des centres radio électriques d'émission et de réception contre les obstacles physiques.

- Spectre de fréquences radioélectriques : désigne l'ensemble de bandes de fréquences radioélectriques ;

Hé Benin

- Signataire : toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui d'une entité ou d'une personne physique ou morale qu'elle représente ;

- Signature électronique : mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur ;

- Signature électronique qualifiée : signature électronique répondant aux exigences de l'article 285 du présent code ;

- Sous traitant : toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement ;

- Station radioélectrique : un ou plusieurs émetteurs ou récepteurs ou un ensemble d'émetteurs et de récepteurs y compris les appareils accessoires, nécessaires pour assurer un service de radiocommunication en un emplacement donné ;

- Système d'alerte professionnelle ou « whistleblowing » : tout système permettant à des individus de signaler un comportement d'un membre de leur organisation contraire, selon eux, à une législation ou à une réglementation ou aux règles primordiales établies par leur organisation ;

- Système informatique : dispositif ou groupe de dispositifs interconnectés ou reliés, dont internet, qui, au moyen d'un programme, procède au traitement automatique des données ou à l'exécution d'autres fonctions. Un système informatique est un dispositif composé de matériels et de logiciels, conçus pour le traitement automatisé des données numériques. Il peut comprendre des moyens d'acquisition, de restitution et de stockage des données. Il peut être isolé ou connecté à d'autres dispositifs similaires au sein d'un réseau ;

- Technologies de l'Information et de la Communication (TIC) : toutes techniques utilisées dans le traitement et la transmission des informations, principalement l'informatique, l'internet et les communications électroniques. Elles désignent aussi le secteur d'activité économique de technologies de l'information et de la communication ;

- TICE : Technologies de l'Information et de la Communication pour l'Enseignement ;

- Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que la limitation, le cryptage, l'effacement ou la destruction ;

- Traitement automatique ou automatisé de données informatiques : ensemble des opérations réalisées en totalité ou en partie par des moyens automatisés, relatifs à la collecte, l'enregistrement, l'élaboration, la modification, la conservation, la destruction, l'application d'opérations logiques et/ou arithmétiques l'édition des données et d'une façon générale, leur exploitation sans intervention humaine directe ;

- Transmission : tous les transferts de données, par téléphone, télécopie, courriel ou transfert de fichiers ;

- UEMOA : Union Économique et Monétaire Ouest Africaine ;

- UIT : Union Internationale des Télécommunications ;

Projet Bénin

- Utilisateur : toute personne physique ou morale qui utilise ou demande à bénéficier d'un réseau et/ou service de communications électroniques, ou d'un service en ligne ;

- Utilisateur final : utilisateur qui ne fournit pas de réseaux de communications électroniques ou de services de communications électroniques ;

- Violation de données à caractère personnel : violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation ou la consultation non autorisées de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Pour les termes non définis par le présent livre, il peut être fait recours et dans l'ordre de leur énumération, aux définitions des textes et des instruments juridiques des organisations ou organismes suivants :

- Union Economique et Monétaire Ouest-Africaine (UEMOA) ;
- Communauté Économique des États de l'Afrique de l'Ouest (CEDEAO) ;
- Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel ;
- loi type de la CNUDCI sur les signatures électroniques (2001) ;
- loi type de la CNUDCI sur le commerce électronique (1996) ;
- Union Internationale des Télécommunications (UIT).

En cas de différence entre les définitions des différents textes et instruments juridiques listés ci-dessus, les définitions prévues dans les textes et instruments juridiques mentionnés en premier dans la liste prévalent.

Article 2 : Objet

Le présent code du numérique a pour objet de régir :

- les activités qui relèvent des réseaux et services de communications électroniques ;
- les outils électroniques ;
- les services de confiance en l'économie numérique ;
- le commerce électronique ;
- la protection des données à caractère personnel ; et
- la cybercriminalité et la cybersécurité.

LegiBenin

LIVRE PREMIER: DES RESEAUX ET SERVICES DE COMMUNICATIONS ELECTRONIQUES

TITRE PREMIER: DES DISPOSITIONS GENERALES

CHAPITRE PREMIER: DU CHAMP D'APPLICATION

Article 3 : Activités concernées

Le présent Livre I régit les activités de communications électroniques conduites par toute personne physique ou morale établissant et/ou exploitant un réseau de communications électroniques ou fournissant des services de communications électroniques sur le territoire de la République du Bénin, quel que soit son statut juridique, sa nationalité, celle des détenteurs de son capital social ou de ses dirigeants, le lieu de son siège social ou de son établissement principal.

Article 4 : Exclusions

Sont exclus du champ d'application du présent Livre I :

- les installations de l'État établies pour les besoins de la sécurité publique, de la défense nationale ou utilisant, exclusivement pour les besoins propres d'une administration, des bandes de fréquences attribuées directement à cette administration. Un décret pris en Conseil des ministres fixe la réglementation applicable aux dites installations ;
- les entreprises de radiodiffusion et/ou de télévision hertzienne, pour ce qui concerne leurs activités de production et de diffusion.

Légal Bénin

Article 5 : Règlementation du secteur

La règlementation du secteur des communications électroniques et de la poste est du ressort de l'Etat. Cette prérogative est exercée par le ministère en charge des communications électroniques et de la poste.

CHAPITRE II: DES PRINCIPES GENERAUX

Article 6 : Principe de liberté d'exercice des activités de communications électroniques

Les activités de communications électroniques s'exercent librement, dans le respect des dispositions prévues au présent code.

Article 7 : Égalité de traitement, non-discrimination, transparence et libre concurrence

Les principes d'égalité de traitement, de non-discrimination des opérateurs et de transparence des procédures s'imposent à toute autorité administrative, notamment à l'Autorité de régulation, y compris dans le cadre des procédures applicables aux différents régimes juridiques concernant les activités de communications électroniques en République du Bénin.

Il est interdit à l'Autorité de régulation de prendre toute mesure ou disposition discriminatoire, notamment des mesures fondées sur la nationalité ou l'origine des opérateurs, de leurs actionnaires et de leurs dirigeants.

Les autorités administratives s'assurent que l'accès à un régime par un opérateur respecte les règles de libre concurrence.

Article 8 : Droits des opérateurs

Les opérateurs intervenant sous un même régime juridique jouissent dans les mêmes conditions de l'ensemble des droits et obligations prévus à ce régime.

Sans préjudice des dispositions de l'alinéa précédent, les conditions dans lesquelles les opérateurs peuvent faire usage de leurs droits dépendent du respect des conditions matérielles ou techniques préalablement fixées par l'Autorité de régulation. Ces conditions sont compatibles avec les règles nationales et communautaires en matière de concurrence.

Article 9 : Représentations diplomatiques, institutions étrangères et organismes jouissant de la personnalité juridique de droit international

Les activités de communications électroniques menées sur le territoire national par les représentations diplomatiques, les institutions étrangères et les organismes jouissant de la personnalité juridique de droit international, sont exercées conformément aux accords internationaux ratifiés par la République du Bénin.

Ces activités sont soumises aux dispositions du présent Livre sous réserve des stipulations contraires aux accords internationaux ratifiés par la République du Bénin.

Article 10 : Respect des conventions et accords régionaux et internationaux

Les opérateurs sont tenus de respecter les conventions ainsi que les accords régionaux et internationaux en matière de communications électroniques ratifiés par la République du Bénin.

Article 11 : Réalisation des travaux par les opérateurs

Pour la réalisation des travaux nécessaires à l'exploitation et à l'extension de leurs réseaux, les opérateurs respectent l'ensemble des dispositions législatives et réglementaires en vigueur, notamment les prescriptions en matière d'aménagement du territoire et de protection de l'environnement.

La réalisation de tels travaux est subordonnée à l'autorisation administrative préalable des autorités locales des zones concernées. Dans ce cas, les autorisations nécessaires interviennent, en tout état de cause, dans un délai de quarante-cinq (45) jours calendaires à compter de la date de réception de la demande. À défaut de réponse dans ce délai, les autorisations sont réputées être accordées.

Tout rejet d'une demande d'autorisation est dûment motivé.

Article 12 : Confidentialité des communications

Les opérateurs ainsi que les membres de leur personnel garantissent la confidentialité des communications effectuées au moyen de leurs réseaux et/ou services et celle des données relatives au trafic y afférent. Ils garantissent également le secret des correspondances des utilisateurs et la neutralité de traitement de ces communications au regard des messages transmis et des informations qui y sont liées.

Sauf autorisation accordée en application des dispositions du code de procédure pénale relatives aux interception des correspondances ou de l'article 595 du présent code, il est interdit à toute personne autre que l'émetteur ou le destinataire d'une communication électronique d'écouter, d'intercepter, de stocker les communications et données ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement préalable des utilisateurs concernés, sous peine de sanctions prévues notamment par le Livre V.

Les opérateurs mettent en place et assurent la mise en œuvre des moyens nécessaires à l'application des articles 108 et 108 bis du code de procédure pénale et de l'article 595 du présent code. Dans ce cadre, l'opérateur désigne des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie des communications électroniques.

Legibenin

Article 13 : Accès ouvert à internet

Les utilisateurs ont le droit d'accéder et de diffuser les informations et contenus légaux de leur choix, et d'utiliser et fournir des applications, services et équipements terminaux de leur choix, quel que soit le lieu où ils se trouvent et où se trouve le fournisseur, et quel que soit le lieu, l'origine ou la destination de l'information communiquée, du contenu diffusé, de l'application utilisée ou du service fourni ou utilisé.

Article 14 : Accords entre les opérateurs fournissant un accès à internet et les utilisateurs

Les accords entre les opérateurs fournissant un accès à internet et les utilisateurs sur les conditions commerciales et techniques et les caractéristiques des services d'accès à l'internet, telles que les prix, les volumes de données ou le débit, et toutes pratiques commerciales mises en œuvre par les opérateurs fournissant un accès à internet, ne limitent pas l'exercice par les utilisateurs des droits énoncés à l'article 13.

Article 15 : Egalité de traitement et non discrimination

Les opérateurs fournissant un accès à internet traitent tous trafics de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et/ou le destinataire, les contenus consultés et/ou diffusés, les applications et/ou les services utilisés ou fournis ou les équipements terminaux utilisés.

Article 16 : Mesures raisonnables de gestion du trafic

Les dispositions de l'article 15 n'empêchent pas les opérateurs fournissant un accès à internet de mettre en œuvre des mesures raisonnables de gestion du trafic. Pour être réputées raisonnables, les mesures sont transparentes, non discriminatoires et proportionnées, et elles ne sont pas fondées sur des considérations commerciales, mais sur des différences objectives entre les exigences techniques en matière de qualité de service de certaines catégories spécifiques de trafic. Ces mesures ne concernent pas la surveillance de contenus particuliers et ne sont pas maintenues plus longtemps que nécessaire.

Les opérateurs fournissant un accès à internet n'appliquent pas de mesures de gestion du trafic qui vont au-delà de celles prévues au présent article et, en particulier, s'abstiennent de bloquer, de ralentir, de modifier, de restreindre, de perturber, de dégrader ou de traiter de manière discriminatoire des contenus, des applications ou des services spécifiques ou des catégories spécifiques de contenus, d'applications ou de services, sauf si nécessaire et seulement le temps nécessaire, pour :

- se conformer aux lois et règlements applicables ou aux mesures donnant effet à ces lois et règlements, y compris les décisions des juridictions ou des autorités compétentes ;

- préserver l'intégrité et la sûreté des réseaux, des services fournis par l'intermédiaire de ces réseaux et des équipements terminaux des utilisateurs ;

- prévenir une congestion imminente du réseau et atténuer les effets d'une congestion exceptionnelle ou temporaire, pour autant que les catégories équivalentes de trafic fassent l'objet d'un traitement égal.

Article 17 : Transparence

Les opérateurs fournissant un accès à internet veillent à ce que tout contrat incluant des services d'accès à internet contienne au moins :

- une explication claire et compréhensible, pour les réseaux fixes, sur le débit minimal, normalement disponible, maximal et annoncé pour le téléchargement descendant et ascendant des services d'accès internet ou, dans le cas des réseaux mobiles, le débit maximal estimé et annoncé pour le téléchargement descendant et ascendant des services d'accès internet ;

- des informations sur la manière dont les mesures de gestion du trafic appliquées par le fournisseur concerné peuvent avoir une incidence sur la qualité des services d'accès à internet, sur le respect de la vie privée des utilisateurs et sur la protection de leurs données à caractère personnel.

Les opérateurs fournissant un accès à internet établissent des procédures transparentes, simples et efficaces pour traiter les réclamations des utilisateurs concernant les droits et les obligations énoncés à l'article 13 du présent code.

Tout écart significatif, permanent ou récurrent, entre les performances réelles des services d'accès à internet en matière de débit ou d'autres paramètres de qualité de service et les performances indiquées par l'opérateur fournissant un accès à internet conformément à l'alinéa premier du présent article est, lorsque les faits pertinents sont établis par un mécanisme de surveillance agréé par l'Autorité de régulation, réputé constituer une performance non-conforme aux fins du déclenchement des voies de recours ouvertes aux utilisateurs.

Article 18 : Surveillance

L'Autorité de régulation surveille étroitement l'application des articles 13 et 17, veille au respect de ces articles et encourage la disponibilité permanente des services d'accès à internet non-discriminatoires à des niveaux de qualité qui correspondent à l'état d'avancement des technologies.

A cette fin, l'Autorité de régulation peut imposer des exigences concernant des caractéristiques techniques, des exigences minimales de qualité du service et d'autres mesures adaptées et nécessaires à un ou plusieurs opérateurs.

A la demande de l'Autorité de régulation, les opérateurs mettent à sa disposition les informations relatives aux obligations énoncées aux articles 13 et 17, notamment les informations concernant la gestion de la capacité de leur réseau et du trafic, ainsi que les justifications de toute mesure de gestion du trafic appliquée. Ces fournisseurs communiquent les informations demandées dans les délais et selon le degré de précision exigés par l'Autorité de régulation.

Article 19 : Neutralité technologique

Dans le cadre de leurs attributions, le ministère en charge des communications électroniques et l'Autorité de régulation veillent à appliquer en toutes circonstances le principe de la neutralité technologique.

Le principe de neutralité technologique s'entend comme l'obligation générale de non discrimination légale, réglementaire, institutionnelle ou autre des technologies au regard des services fournis.

Article 20 : Autres obligations applicables aux opérateurs

Les opérateurs ne peuvent utiliser leur réseau ou sciemment en permettre l'utilisation à des fins illégales ou contraires aux dispositions légales et règlementaires en vigueur. Ils prennent toutes mesures appropriées pour s'assurer que leur réseau n'est pas utilisé à des fins illégales ou frauduleuses.

Legi-Benin

Les opérateurs doivent coopérer et contribuer activement à la lutte contre toutes formes de fraudes énoncées dans le présent code et doivent notamment communiquer à l'Autorité de régulation et à l'autorité judiciaire toutes les informations qu'elles demandent et prendre les mesures exigées par ces autorités.

En cas de non respect des dispositions du présent article, les opérateurs s'exposent aux sanctions prévues par les dispositions légales et règlementaires en vigueur, y compris celles prévues à l'article 247 de la présente loi portant code du numérique, et sont tenus responsables de toute fraude dont la réalisation aura été possible en raison de leur manquement.

L'Autorité de régulation précise les conditions dans lesquelles les dispositions du présent article sont mises en œuvre.

Les autres obligations applicables aux opérateurs seront précisées par voie règlementaire.

CHAPITRE III: DE LA PROTECTION DES UTILISATEURS, DES PERSONNES ET DE L'ENVIRONNEMENT

Article 21 : Obligations des opérateurs

Tout opérateur a l'obligation de :

- rendre disponibles à tout utilisateur les réseaux et services de communications électroniques ouverts au public qu'il fournit ;

- s'assurer que les frais, les tarifs, les pratiques et les classifications sont justes, raisonnables et disponibles de façon transparente ;

- fournir des services efficaces et conformes aux normes reconnues au plan national, international ou adoptées par l'Autorité de régulation ;

- publier par tout moyen et sans délais, les prévisions d'interruption de services, notamment pour des raisons d'installation, de réparation ou de changement d'équipement ;

- établir un mécanisme efficace de traitement des réclamations et de réparation des pannes des réseaux et/ou des services de communications électroniques.

Article 22 : Droit à la fourniture de services de communications électroniques

Sauf décision prise en application d'une législation et/ou d'une réglementation nationale, toute personne physique ou morale qui remplit les conditions contractuelles et financières proposées par un opérateur ne peut se voir refuser la fourniture de ces services, s'il en a formulé la demande.

L'opérateur peut néanmoins exiger de l'utilisateur demandeur desdits services un dépôt de garantie dont le montant est préalablement fixé et publié de manière transparente et non discriminatoire.

Tout utilisateur d'un service de communications électroniques qui respecte les conditions contractuelles et financières souscrites ne peut se voir déconnecter du réseau ou service, à moins qu'il en fasse la demande expresse, sauf en cas d'urgence ou pour des raisons de sécurité publique.

Article 23 : Publications des informations et tarifs par les opérateurs

Légi-Parl

Les informations transparentes et actualisées relatives à l'ensemble des services proposés, aux tarifs pratiqués ainsi qu'aux conditions générales de vente et/ou de services, sont régulièrement publiées et mises à la disposition des utilisateurs par les opérateurs dans leurs points de vente et sur leur site internet.

Le Ministère en charge des communications électroniques peut préciser la forme et le contenu de ces informations et documents.

Article 24 : Contrats types élaborés par les opérateurs

Tout opérateur élabore des contrats types et leurs avenants pour la fourniture de leurs services aux utilisateurs.

Les projets de contrats types ainsi que leurs avenants sont soumis à l'approbation préalable de l'Autorité de Régulation.

Le Ministère en charge des communications électroniques peut préciser quelles sont les dispositions que doivent contenir les contrats conclus avec les utilisateurs

Article 25 : Droit des utilisateurs

Aucun opérateur ne peut limiter le droit de l'utilisateur à :

- choisir un fournisseur de services de contenu ;
- relier au réseau tout appareil radio ou équipement terminal de communications électroniques bénéficiant d'un agrément à cet effet ;
- relier à un réseau de communications électroniques ouvert au public tout réseau de communications interne qui répond aux normes et exigences en la matière.

Article 26 : Modification des contrats avec les utilisateurs

Les opérateurs ne peuvent unilatéralement modifier les termes d'un contrat qui les lie aux utilisateurs que :

- pour des raisons indiquées dans les termes du contrat et conformément à ce dernier ;
- sur la base d'un changement de la législation ou d'une décision des autorités.

Tout projet de modification des conditions contractuelles de fourniture d'un service de communications électroniques est communiqué par l'opérateur aux utilisateurs par écrit ou sur un autre support durable mis à la disposition de ce dernier au moins un (01) mois avant son entrée en vigueur, assorti de l'information selon laquelle les utilisateurs peuvent, tant qu'ils n'ont pas expressément acceptés les nouvelles conditions, résilier le contrat sans pénalité de résiliation et sans droit à dédommagement, jusque dans un délai de quatre (04) mois après l'entrée en vigueur de la modification.

La modification ne prend effet qu'à l'issue de ce délai de quatre (04) mois.

Article 27 : Accès aux services fournis par les opérateurs et aux services d'urgence

Les opérateurs assurent, de manière permanente et continue, la fourniture des services de communications électroniques.

Legibenin

Les opérateurs qui fournissent un service téléphonique au public garantissent également un accès ininterrompu aux services d'urgence, conformément aux règles applicables et dans les conditions précisées par l'Autorité de régulation, sous peine de sanctions prévues aux articles 239 et 240 du présent code.

Article 28 : Réclamations des utilisateurs

Les opérateurs fournissant des services de communications électroniques aux consommateurs établissent et gèrent un système de traitement des réclamations des utilisateurs. Les réclamations sont traitées dans un délai n'excédant pas un (01) mois.

Article 29 : Prescription

La prescription est acquise :

- au profit des opérateurs dans leurs relations contractuelles avec les utilisateurs, pour toutes demandes en restitution du prix de leurs prestations présentées par un utilisateur après un délai d'un (01) an à compter du jour du paiement ;

- au profit des utilisateurs dans leurs relations contractuelles avec les opérateurs, pour les sommes dues à un opérateur au titre du paiement de ses prestations, lorsque celui-ci ne les a pas réclamées dans un délai d'un (01) an à compter de la date de leur exigibilité.

Article 30 : Protection des personnes contre les effets des champs électriques, magnétiques et électromagnétiques

Tout opérateur, tout importateur et tout distributeur est tenu de se conformer aux valeurs limites d'exposition des personnes aux champs électriques, magnétiques et électromagnétiques.

Un décret pris en Conseil des ministres sur proposition du Ministre chargé des communications électroniques fixe les valeurs limites d'exposition aux champs électriques, magnétiques et électromagnétiques.

Article 31 : Contrôle et inspection des installations et équipements radioélectriques

L'exploitation des équipements et installations radioélectriques et électroniques se fait conformément aux normes en vigueur.

Un décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques fixe les modalités de contrôle et d'inspection des équipements et installations radioélectriques.

Article 32 : Protection de l'environnement contre les déchets électroniques

En ce qui concerne les équipements et installations électroniques, tout équipementier, opérateur, importateur et distributeur est astreint au respect des normes environnementales.

Un décret pris en Conseil des ministres sur proposition du Ministre chargé des communications électroniques précise les modalités de gestion et de traitement des déchets électroniques.

CHAPITRE IV: DES DONNEES PERSONNELLES DES UTILISATEURS

Article 33 : Effacement ou anonymisation des données techniques

Légibénin

Sans préjudice des dispositions du Livre V et de l'article 120 du présent code, les articles 33 à 37 s'appliquent au traitement des données à caractère personnel dans le cadre de l'exploitation de réseaux de communications électroniques et de la fourniture de services de communications électroniques. Ils s'appliquent notamment aux réseaux et services qui comportent un dispositif de collecte de données et d'identification.

Les opérateurs et les fournisseurs de services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des articles 34 à 37.

Les opérateurs et les fournisseurs de services de communication au public en ligne établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès à un réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables en vertu du présent article.

Article 34 : Exception à l'effacement ou l'anonymisation des données techniques

Suivant les modalités et dans les conditions prévues au code de procédure pénale relatives à l'interception et à l'accès aux données par les autorités administratives ainsi qu'à l'article 595 du présent code, il peut être différé pour une durée maximale d'un (01) an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques en vue de leur communication aux autorités judiciaires et administratives visées à ces articles.

Un arrêté du ministre chargé des communications électroniques, pris après avis de l'APDP, détermine, dans les limites fixées par l'article 37, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications.

Article 35 : Utilisation des données techniques pour les besoins de la facturation et du paiement et pour la commercialisation des services

Pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre à des tiers concernés directement par la facturation ou le recouvrement, les catégories de données techniques qui sont déterminées, dans les limites fixées par l'article 37, selon l'activité des opérateurs et la nature de la communication, par un arrêté du ministre chargé des communications électroniques pris après avis de l'APDP.

Les opérateurs peuvent en outre réaliser un traitement de données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si les utilisateurs y ont préalablement et expressément consenti, et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour la fourniture ou la commercialisation de ces services. Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux.

Article 36 : Données permettant de localiser l'équipement terminal de l'utilisateur

Sans préjudice des dispositions des articles 34 et 35 sous réserve des nécessités d'enquêtes judiciaires et de police, ou pour les besoins de la sécurité publique ou de la défense nationale, les données permettant de localiser l'équipement terminal de l'utilisateur ne peuvent ni être utilisées pendant la communication à des fins autres que son acheminement, ni être conservées

Projet Bénin

ou traitées après l'achèvement de la communication qu'avec le consentement de l'utilisateur, dûment informé des catégories de données en cause, de la durée du traitement, de ses fins et du fait que ces données seront ou non transmises à des tiers.

L'utilisateur peut suspendre ou retirer son consentement à tout moment par un moyen simple et gratuit, hormis les coûts liés à la transmission du retrait ou de la suspension.

Tout appel destiné à un service d'urgence vaut consentement de l'utilisateur au sens de l'alinéa premier du présent code jusqu'à l'aboutissement de l'opération de secours qu'il déclenche et seulement pour en permettre la réalisation.

Article 37 : Nature des données conservées

Les données conservées et traitées dans les conditions définies aux articles 34 à 36 portent exclusivement sur l'identification des utilisateurs, sur les caractéristiques techniques des communications assurées par les opérateurs et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions du Livre V du présent code, relatives à la protection des données à caractère personnel.

Les opérateurs de réseaux et/ou services de communications électroniques ouverts au public prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues aux articles 33 à 36 du présent code.

Legibenin

Article 38 : Identification des utilisateurs

Les opérateurs procèdent à l'identification de tous les utilisateurs de leurs services de communications électroniques au moment de la souscription aux services qu'ils fournissent. Les conditions dans lesquelles les opérateurs procèdent à l'identification des utilisateurs sont précisées par voie règlementaire.

Les opérateurs mobiles mettent en place les moyens et procédures nécessaires afin de garantir l'intégrité de leur réseau de distribution. Ils demeurent responsables des agissements de leurs distributeurs et sous-traitants

Article 39 : Vols de terminaux

Les opérateurs sont tenus de mettre en œuvre les dispositifs techniques destinés à interdire, à l'exception des numéros d'urgence, l'accès à leurs communications émises au moyen de terminaux mobiles, identifiés et qui leur ont été déclarés volés. Ces terminaux sont bloqués sans délai, dès la réception par l'opérateur concerné de la déclaration officielle de vol, transmise par les services de police, l'autorité judiciaire ou le propriétaire du terminal, dont l'identité aura préalablement été confirmée par l'opérateur.

Les services de police judiciaire peuvent toutefois après accord du Procureur de la République ou du Juge d'Instruction, déroger à l'application du premier alinéa.

Article 40 : Identification de l'appelant

A sa demande, tout utilisateur peut, sauf pour une raison liée au fonctionnement des services d'urgence ou à la tranquillité de l'appelé, s'opposer à l'identification par ses correspondants de son numéro de téléphone.

TITRE II: DES COMMUNICATIONS ELECTRONIQUES

CHAPITRE PREMIER: DES REGIMES JURIDIQUES

SECTION I: DES DISPOSITIONS GENERALES

Article 41 : Prohibition et abrogation des droits exclusifs

Toutes dispositions antérieures de quelque nature que ce soit accordant des droits exclusifs sont abrogées.

Article 42 : Régimes applicables

Les régimes juridiques applicables aux activités de communications électroniques sont :

- le régime de la licence ;
- le régime de l'autorisation ;
- le régime de l'entrée libre avec ou sans déclaration préalable.

Article 43 : Octroi des licences et des autorisations et réalisation des déclarations

Les modalités d'octroi des licences, des autorisations et les conditions de réalisation de la déclaration font l'objet d'un décret pris en Conseil des ministres sur avis conforme de l'Autorité de régulation. Le décret qui le constate est publié au Journal officiel.

Article 44 : Modifications affectant les activités de communications électroniques

Les droits, les procédures et les conditions attachés aux différents régimes juridiques doivent être précisés par voie règlementaire. Ils ne peuvent faire l'objet de modification qu'en respect des procédures énoncées à l'alinéa 2 du présent article.

Avant de modifier les régimes, les procédures, les droits et les obligations attachés à l'exercice des activités de communications électroniques, l'Autorité de régulation consulte et recueille les avis des acteurs du secteur. Les modifications opérées ne sont pas rétroactives.

Article 45 : Coordination avec les autorités régionales et les autorités de régulation nationales

L'Autorité de régulation se coordonne avec les autorités régionales de la CEDEAO et de l'UEMOA ainsi qu'avec les autres autorités de régulation nationale des États membres de la CEDEAO et de l'UEMOA en ce qui concerne la délivrance de licences ou d'autorisations ou la réalisation de déclaration pour l'exercice de certaines activités de communications électroniques.

SECTION II: DE LA LICENCE

Article 46 : Activités soumises au régime de la licence

La licence est exigée :

- pour l'exploitation de réseaux ouverts au public ;

Droit Béninois

- lorsque pour des raisons de politique nationale concernant notamment l'ordre public, la défense, les bonnes mœurs, la sécurité et/ou la santé publique, l'État décide que le service concerné soit soumis au régime de la licence.

L'exploitation de réseaux ouverts au public qui ne requiert pas l'utilisation de fréquences radioélectriques identifiées par décret pris en Conseil des ministres peut être soumise à un régime d'autorisation ou de déclaration par décret pris en Conseil des ministres.

La licence est octroyée par décret pris en Conseil des ministres sur proposition du Ministre chargé des communications électroniques à toute personne morale suivant un cahier des charges qui en fixe les conditions.

Le décret d'octroi de la licence approuve les termes du cahier des charges.

Article 47 : Appel à la concurrence

Les licences délivrées pour l'établissement et l'exploitation de réseaux ouverts au public et/ou la fourniture de services de communications électroniques au public qui nécessitent l'utilisation de fréquences radioélectriques identifiées par décret pris en Conseil des ministres sont octroyées à la suite d'une procédure d'appel à la concurrence.

L'Autorité de régulation est chargée de conduire la procédure de mise en concurrence jusqu'à la désignation de l'attributaire.

Le candidat déclaré attributaire est celui dont l'offre est jugée la mieux disante par rapport aux exigences prévues dans le dossier d'appel d'offres, notamment celles du cahier des charges, des conditions générales d'établissement et d'exploitation et des dispositions de la présente section qu'il s'engage à respecter.

L'attribution de la licence à la suite d'un appel à concurrence fait l'objet d'un rapport présenté par le ministre chargé des communications électroniques sur avis conforme de l'Autorité de régulation au Conseil des ministres qui prend la décision d'octroi de la licence par décret.

Les modalités d'attribution des licences sont précisées par décret pris en Conseil des ministres.

Article 48 : Opérateurs non nationaux

Sous réserve des engagements souscrits par le Bénin et comportant une clause de réciprocité applicable au secteur des communications électroniques, l'exercice de toute activité soumise au régime de la licence ne peut être autorisé qu'à des entreprises de droit béninois.

Article 49 : Modification des licences

La licence est attribuée à titre personnel et individuel. Elle ne peut être attribuée, renouvelée, modifiée, retirée ou transférée que par décret pris en Conseil des ministres, sur avis conforme de l'Autorité de régulation.

Toute modification unilatérale de licence est passible de sanction.

Article 50 : Règles applicables aux activités soumises au régime de la licence

Les règles applicables et les exigences essentielles relatives aux activités soumises au régime de la licence sont précisées par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques.

Article 51 : Contenu du cahier des charges de la licence

Le cahier des charges prévoit, a minima, des dispositions relatives :

Légi Bénin

- au respect d'une concurrence loyale ;
- à l'obligation de tenir une comptabilité analytique autonome pour chaque réseau et service exploité ;
- aux conditions de confidentialité et de neutralité du service au regard des messages transmis ;
- aux prescriptions exigées par la défense nationale et la sécurité publique et les prérogatives de l'autorité judiciaire ;
- aux modalités de contribution aux missions générales de l'Etat et en particulier aux missions et charges du service universel ;
- à l'obligation de respecter les accords et les conventions internationaux ratifiés par la République du Bénin ;
- à l'obligation d'acheminer gratuitement les appels d'urgence ;
- à la contribution à la recherche, à la formation et à la normalisation en matière de communications électroniques.

SECTION III: DE L'AUTORISATION

Article 52 : Activités de communications électroniques soumises au régime de l'autorisation

Une autorisation est exigée pour la fourniture de services de communications électroniques au public et pour l'exploitation de réseaux ouverts au public dispensés du régime de la licence par décret pris en Conseil des ministres, conformément aux dispositions de l'article 46 du présent code.

Article 53 : Règles applicables aux activités soumises au régime de l'autorisation

Les règles applicables aux activités soumises au régime de l'autorisation sont précisées par arrêté du ministre en charge des communications électroniques.

Article 54 : Obtention des autorisations

Les décisions d'octroi ou de refus de délivrance d'une autorisation par l'Autorité de régulation interviennent dans un délai maximum d'un (01) mois à compter de la date de notification de la demande par le demandeur. Ce délai peut être prorogé d'un (01) mois, notamment en raison de la complexité technique des réseaux et/ou services objets de l'autorisation sollicitée.

Toute décision de refus de délivrance d'une autorisation par l'Autorité de régulation, est motivée. La décision de refus de l'Autorité de régulation est susceptible de recours devant la chambre administrative de la cour d'appel de Cotonou dans un délai d'un (01) mois.

SECTION IV: DE LA DECLARATION

Article 55 : Activités de communications électroniques soumises au régime de la déclaration

L'établissement et/ou l'exploitation de tout réseau de communications électroniques et/ou la fourniture de tout service de communications électroniques ne relevant pas des régimes de la licence ou de l'autorisation est libre, sur simple déclaration préalable auprès de l'Autorité de régulation, et sous réserve du respect des dispositions légales et règlementaires en vigueur.

Par exception aux dispositions du présent article, sous réserve de la conformité de leurs équipements, les réseaux internes, les réseaux indépendants à usage privé et les dispositifs exclusivement composés d'appareils de faible puissance et de faible portée ne requièrent aucune

Legi-Benin

déclaration auprès de l'Autorité de régulation et ne sont pas soumis aux obligations applicables aux opérateurs, sauf lorsque les textes légaux et règlementaires le prévoient spécifiquement.

En tant que de besoin, l'Autorité de régulation fixe les seuils d'émission, de portée et les bandes de fréquences utilisées par d'appareils de faible puissance et de faible portée.

Article 56 : Règles applicables aux activités soumises au régime de la déclaration

Les règles applicables aux activités soumises au régime de la déclaration sont précisées par l'Autorité de régulation.

Article 57 : Règles applicables aux déclarations

Un récépissé est remis par l'Autorité de régulation à toute personne déposant un dossier complet de déclaration le jour même du dépôt du dossier. Dès la remise de ce récépissé, l'activité objet de la déclaration peut être exercée par le déclarant.

Les opérateurs dûment autorisés à exercer des activités de communications électroniques dans un autre Etat membre de la CEDEAO qui relèvent, en République du Bénin, du régime de la déclaration, sont autorisés à déclarer leurs activités en République du Bénin dans des conditions identiques aux entreprises nationales.

L'Autorité de régulation ne peut refuser une déclaration, sauf en cas de dossier incomplet, pour des raisons de sécurité publique ou si les réseaux exploités ou les services fournis sont contraires aux dispositions légales ou règlementaires applicables ou contraires à l'ordre public.

Les éléments constitutifs de la déclaration, les procédures de réalisation de la déclaration et les conditions particulières d'exploitation sous le régime de la déclaration sont fixés par un arrêté du ministre chargé des communications électroniques après avis de l'Autorité de régulation.

Legibenin

SECTION V: DES CONTREPARTIES FINANCIERES, CONTRIBUTIONS ET REDEVANCES

Article 58 : Contrepartie financière des opérateurs titulaires d'une licence

L'octroi de licence est soumis au paiement d'une contrepartie financière dont les modalités sont précisées dans le cahier des charges.

Article 59 : Contribution au titre de la formation et de la normalisation

La contribution des opérateurs titulaires de licence et d'autorisation au titre de la formation et de la normalisation au profit du ministère en charge des communications électroniques et de l'Autorité de régulation est fixée à un pourcentage de leur chiffre d'affaires réalisé au titre des activités de communications électroniques, objet de la licence et/ou de l'autorisation.

Ce pourcentage est fixé par décret pris en Conseil des ministres sur proposition du Ministre chargé des communications électroniques et du ministre chargé des finances.

Le montant de la contribution est payé directement au trésor public sur le compte de l'Autorité de régulation.

Article 60 : Contribution au titre de l'aménagement numérique du territoire, du service universel et du fonctionnement de l'Autorité de régulation

La contribution des opérateurs titulaires de licence et d'autorisation au titre de l'aménagement numérique du territoire, du service universel et du fonctionnement de l'Autorité de régulation est fixée à un pourcentage de leur chiffre d'affaire réalisé au titre des activités de communications électroniques objet de la licence et de l'autorisation.

Ce pourcentage est fixé par décret pris en Conseil des ministres sur proposition du Ministre chargé des communications électroniques et du ministre chargé des finances.

Article 61 : Contribution au titre de la recherche

La contribution des opérateurs titulaires de licence et d'autorisation au titre de la recherche est fixée à un pourcentage du chiffre d'affaires précité.

Ce pourcentage est fixé par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques et du ministre chargé des finances.

Le montant de la contribution est payé sur un compte d'affectation spécial pour la recherche créé conformément à la législation en vigueur.

Sont libérés de cette contribution les opérateurs qui réalisent, pour un montant équivalent, des programmes de recherche dans le cadre de conventions approuvées par le ministre chargé des communications électroniques à passer avec des organismes de recherche dont la liste sera fixée par arrêté du ministre chargé des communications électroniques.

Article 62 : Frais et redevances

Sur proposition de l'Autorité de régulation et sans préjudice des contreparties financières, des contributions prévues dans la présente Section et des contributions au financement de l'accès/service universel auxquelles sont assujetties les opérateurs conformément aux dispositions du présent code, l'État instaure, en cas de besoin, dans les conditions de transparence et de non-discrimination, des taxes, frais et des redevances destinés à couvrir les charges inhérentes à l'exercice des activités de régulation et de règlementations.

Les modalités d'affectation desdits frais et redevances sont déterminées par arrêté du Ministre chargé des communications électroniques.

Les frais et les redevances ainsi créés sont publiés, chaque année, au Journal Officiel et par toutes voies d'annonces légales.

CHAPITRE II: DE L'ACCES ET DE L'INTERCONNEXION

SECTION I: DES DISPOSITIONS GENERALES RELATIVES A L'ACCES ET A L'INTERCONNEXION

Article 63 : Droit d'accès et d'interconnexion

Les opérateurs nationaux bénéficient d'un droit d'accès et d'interconnexion aux réseaux de communications électroniques, aux infrastructures passives et actives et aux infrastructures alternatives dans les conditions prévues à la présente section et dans leur cahier des charges.

Les opérateurs non nationaux bénéficient d'un droit d'accès et d'interconnexion limité aux réseaux, infrastructures et services couverts par le présent Chapitre dans les conditions qui seront précisées par décret pris en Conseil des ministres.

Tout opérateur bénéficiant d'un accès aux réseaux d'un autre opérateur ne peut revendre en l'état les capacités disponibles sur ce réseau, y compris les capacités nationales et internationales à d'autres opérateurs ou à ses utilisateurs.

Article 64 : Demandes d'accès et d'interconnexion présentées par des opérateurs nationaux

Log-Bénin

Les opérateurs nationaux et non-nationaux et les exploitants d'infrastructures alternatives font droit dans des conditions objectives, transparentes et non discriminatoires, aux demandes d'accès et d'interconnexion des autres opérateurs présentées en vue d'exploiter des réseaux et/ou fournir des services de communications électroniques, pour autant que ceux-ci soient techniquement réalisables.

Article 65 : Mise en œuvre de l'accès et de l'interconnexion

Toute demande d'accès ou d'interconnexion ne peut être refusée si elle est justifiée au regard, d'une part, des besoins du demandeur et d'autre part, des capacités de l'opérateur à la satisfaire. Elle peut être refusée si elle est techniquement impossible à satisfaire, notamment au regard de l'interopérabilité des équipements et systèmes.

Toute décision de refus d'accès ou d'interconnexion opposée par un opérateur doit être motivée. Elle est notifiée au demandeur et portée à la connaissance de l'Autorité de régulation, ainsi qu'à l'autorité de régulation nationale du pays dans lequel est établi l'opérateur non national, le cas échéant.

A la demande des parties, l'Autorité de régulation peut les assister dans les négociations des accords d'accès et d'interconnexion.

Article 66 : Conditions techniques et tarifaires de l'accès et de l'interconnexion

L'Autorité de régulation peut préciser les conditions techniques et tarifaires de l'interconnexion et de l'accès aux infrastructures actives et/ou passives et aux infrastructures alternatives entre opérateurs et entre opérateurs et exploitants d'infrastructures alternatives.

L'Autorité de régulation peut notamment décider que la fourniture de certaines prestations d'accès et d'interconnexion visées à l'alinéa précédent doivent être orientées vers les coûts ou doivent être publiées dans un catalogue d'accès et d'interconnexion dans les conditions prévues à l'article 70 du présent code.

Article 67 : Opérateurs contrôlant l'accès aux utilisateurs finaux

Les opérateurs qui contrôlent l'accès aux utilisateurs finaux peuvent se voir imposer des obligations en vue d'assurer le bon fonctionnement et l'interconnexion de leurs réseaux ainsi que l'accès aux services fournis sur d'autres réseaux.

Article 68 : Conventions d'accès et d'interconnexion

L'accès et l'interconnexion font l'objet d'une convention de droit privé entre les parties concernées. Cette convention détermine, dans le respect des dispositions du présent Chapitre et des actes règlementaires pris pour son application, les conditions techniques et financières relatives à ces prestations.

Les conventions d'accès et d'interconnexion sont communiquées, pour approbation, à l'Autorité de régulation, qui peut en demander la modification dans un délai d'un (01) mois suivant leur réception. Toute modification de ces conventions par les parties doit être notifiée à l'Autorité de régulation.

Un décret pris en Conseil des ministres fixe les modalités d'application de la présente section, notamment les conditions générales et les principes de tarification applicables aux accords d'accès et d'interconnexion.

Article 69 : Fourniture d'informations et cartographie

Projet

Les opérateurs, les exploitants d'infrastructures alternatives et les exploitants d'infrastructures essentielles visés à l'article 82 du présent code communiquent à l'Autorité de régulation, dans les conditions, la périodicité et les formats demandés par celle-ci, l'ensemble des informations pertinentes relatives à leur réseau de communications électroniques, leurs infrastructures passives et actives, leurs infrastructures alternatives et à toutes autres informations pertinentes exigées par l'Autorité de régulation.

La nature et les conditions dans lesquelles ces informations sont communiquées à l'Autorité de régulation font l'objet d'une décision de l'Autorité de régulation.

Sur la base de ces informations, l'Autorité de régulation élabore une base de données et une cartographie :

- des réseaux et infrastructures actives et passives des opérateurs ouverts à l'accès et à l'interconnexion et offrant la possibilité aux autres opérateurs de s'y colocaliser ;
- des infrastructures alternatives détenues par les exploitants d'infrastructures alternatives ;
- des infrastructures essentielles.

A cet égard, des obligations spécifiques peuvent être imposées aux opérateurs désignés comme dominants en application de l'article 144 du présent code.

Article 70 : Catalogue d'interconnexion

Tous les opérateurs titulaires d'une licence et les autres opérateurs s'ils sont désignés comme dominants par l'Autorité de régulation en application de l'article 144 du présent code sont tenus de publier et de lui communiquer un catalogue d'accès et d'interconnexion dans lequel figurent l'ensemble des offres techniques et tarifaires proposées au titre de l'accès et de l'interconnexion, y compris les prestations de colocalisation.

L'Autorité de régulation peut également imposer à tout autre opérateur non visé à l'alinéa précédent, aux exploitants d'infrastructures alternatives et aux exploitants d'infrastructures essentielles visées à l'article 82 du présent code de publier un catalogue d'accès et/ou d'interconnexion en précisant les prestations et les dispositions qui doivent y figurer.

L'Autorité de régulation peut imposer des modifications aux offres figurant dans leurs catalogues d'interconnexion.

Les prestations et dispositions que doivent contenir les catalogues d'accès et d'interconnexion et leur niveau de détail, ainsi que les conditions d'approbation et de publication de ces catalogues, sont précisées par décret pris en Conseil des ministres sur avis de l'Autorité de régulation.

Article 71 : Obligations imposées spécifiquement aux opérateurs dominants

L'Autorité de régulation peut imposer les obligations prévues à la présente Section uniquement aux opérateurs désignés comme dominants en application de l'article 144 du présent code.

SECTION II

DU PARTAGE D'INFRASTRUCTURES ET AUTRES FORMES PARTICULIERES

D'ACCES ET D'INTERCONNEXION

Légiburkina

Article 72 : Partage d'infrastructures

L'Autorité de régulation encourage le partage d'infrastructures actives et passives et l'accès aux infrastructures alternatives dans des conditions d'équité, de non-discrimination et d'égalité d'accès.

Lorsque le partage d'infrastructures est rendu nécessaire pour satisfaire aux objectifs de concurrence, d'aménagement du territoire ou de protection de l'environnement ou du patrimoine, l'Autorité de régulation peut imposer aux opérateurs et aux exploitants d'infrastructures alternatives des obligations de partage des infrastructures passives ou actives y compris les infrastructures alternatives, qu'elles soient existantes ou à construire, notamment les poteaux, les fourreaux et les points hauts, particulièrement dans les zones peu denses afin de mutualiser les investissements d'infrastructures des operateurs ainsi qu'aux endroits où l'accès à de telles capacités est limité.

Article 73 : Dégroupage de la boucle locale et de la sous-boucle locale

En fonction de l'évolution des marchés, des réseaux et des services de communications électroniques et après consultation des parties prenantes, l'Autorité de régulation pourra, sur la base d'une analyse sur l'opportunité de mettre en œuvre le dégroupage de la boucle locale ou de la sous-boucle locale, proposer au Ministre chargé des communications électroniques les dispositions nécessaires à la mise en œuvre d'un tel dégroupage.

Sur la base de cette proposition, le Ministre chargé des communications électroniques prend un arrêté précisant les conditions techniques et tarifaires dans lesquelles le dégroupage de la boucle-locale doit être mis en œuvre par les opérateurs.

Cet arrêté précise les dispositions à mettre en œuvre afin que :

- les opérateurs puissent accéder à la boucle locale d'autres opérateurs sur la base d'un calendrier prédéfini ;
- les opérateurs souhaitant accéder à la boucle locale d'autres opérateurs soient tenus, de par leur cahier des charges, à un déploiement minimal d'infrastructure ;
- les opérateurs de boucle locale fournissent aux autres opérateurs l'accès à leurs infrastructures ainsi que la possibilité de colocalisation dans leurs propres locaux pour faciliter le dégroupage dans des conditions objectives, transparentes et non discriminatoires, dans le respect du principe d'orientation des prix en fonction des coûts ;
- l'offre technique et tarifaire de dégroupage qui devra être publiée par les opérateurs de boucle locale comprenNE la liste exhaustive des services offerts, qui devra faire l'objet d'une approbation par l'Autorité de régulation dans les conditions prévues à l'article 70 du présent code.

Article 74 : Prestations d'itinérance nationale

Sans préjudice des dispositions prévues dans la Section 1, les opérateurs de radiocommunications doivent faire droit dans des conditions objectives, transparentes et non discriminatoires aux demandes de prestations d'itinérance nationales qui leur sont présentées par d'autres opérateurs de radiocommunication dans les zones les moins denses du territoire qui sont déterminées par l'Autorité de régulation.

Lorsqu'un nouvel opérateur de radiocommunication intègre le marché en République du Bénin ou lorsque la mise en œuvre d'une prestation d'itinérance nationale est rendue nécessaire pour satisfaire aux objectifs de concurrence ou d'aménagement numérique du territoire ou de

Log-Bénin

protection de l'environnement ou du patrimoine, l'Autorité de régulation impose aux opérateurs de radiocommunications de fournir une prestation d'itinérance nationale sur des zones définies ou sur l'ensemble du territoire national.

Pour garantir l'égalité des conditions de concurrence ou l'interopérabilité des services, l'Autorité de régulation peut demander aux parties à une convention d'itinérance nationale la modification des accords d'itinérance déjà conclus.

Article 75 : Prestations d'itinérance internationale

Les opérateurs de radiocommunications sont libres de conclure des contrats d'itinérance avec des opérateurs étrangers en vue de la fourniture de services de communications électroniques aux abonnés de ces opérateurs étrangers lorsqu'ils sont au Bénin et de la fourniture de services de communications électroniques à leurs abonnés par ces opérateurs étrangers lorsqu'ils sont à l'étranger.

L'Autorité de régulation peut :

- enquêter sur les prix d'itinérance pratiqués dans la région ;
- procéder à des consultations avec les acteurs concernés en vue d'arriver à des tarifs raisonnables permettant à un maximum d'itinérants dans la région de pouvoir utiliser les réseaux aux meilleurs prix et qualité ;
- identifier les opérateurs pratiquant des tarifs abusifs ;
- demander, le cas échéant, l'avis du conseil de la concurrence ;
- permettre aux abonnés des services prépayés de bénéficier du service d'itinérance et à des tarifs raisonnables ;
- informer clairement et de façon transparente et détaillée les clients des tarifs appliqués pour l'itinérance.

Leg-Bénin

Article 76 : Accès des opérateurs mobiles virtuels

Sans préjudice des dispositions prévues dans la Section 1, les opérateurs de radiocommunications doivent faire droit dans des conditions objectives, transparentes et non discriminatoires aux demandes d'accès et d'interconnexion présentées par des opérateurs de réseaux mobiles virtuels (MVNO) dûment autorisés en vue de fournir des services de communications électroniques aux utilisateurs.

Article 77 : Accès aux capacités sur les câbles sous-marins

Sans préjudice des dispositions prévues dans la Section 1, tout exploitant et/ou gestionnaire de câble sous-marin et/ou de station d'atterrissement de câble sous-marin sur le territoire national est soumis aux obligations suivantes :

- fournir à tout opérateur qui le demande un accès à sa station d'atterrissement de câble sous-marin ainsi que des prestations de colocalisation, y compris virtuelle ;
- fournir à tout opérateur une prestation de liaison d'interconnexion entre le point de présence de l'opérateur situé sur le territoire national et la station d'atterrissement du câble ;
- fournir à tout opérateur national une prestation d'interconnexion avec les capacités internationales qu'il détient sur un câble sous-marin raccordé à sa station d'atterrissement ainsi qu'avec toutes les capacités détenues par des opérateurs tiers sur l'ensemble des câbles sous-marins connectés à la station ;

- permettre à tout exploitant et/ou gestionnaire de câble sous-marin d'atterrir à ladite station.
- publier les conditions techniques et tarifaires de ces prestations dans une offre d'interconnexion et d'accès de référence relative à l'accès aux capacités internationales sous-marines dans les conditions prévues à l'article 70 du présent code.

L'accès aux capacités sur les câbles sous-marins se fait dans des conditions équitables, non discriminatoires et de façon transparente.

Article 78 : Demandes d'accès et d'interconnexion

Toute demande relative à des prestations visées aux articles 73, 74, 76 et 77 du présent code ne peut être refusée si elle est justifiée au regard, d'une part, des besoins du demandeur et d'autre part, des capacités de l'opérateur à la satisfaire. Elle peut être refusée si elle est techniquement impossible à satisfaire, notamment au regard de l'interopérabilité des équipements et systèmes.

Toute décision de refus d'accès ou d'interconnexion opposée par un opérateur doit être motivée. Elle est notifiée au demandeur et portée à la connaissance de l'Autorité de régulation, ainsi que, le cas échéant, à l'autorité de régulation nationale du pays dans lequel est établi l'opérateur non national.

A la demande des parties, l'Autorité de régulation peut les assister dans les négociations des accords conventions prévues à la présente Section.

Article 79 : Obligations imposées par l'Autorité de régulation

Dans son appréciation du caractère proportionné des obligations de partage d'infrastructures et d'itinérance nationale qu'elle peut imposer en application des articles 72 et 74 du présent code, l'Autorité de régulation prend notamment en compte les éléments suivants :

- la viabilité technique et économique de l'utilisation partagée des infrastructures envisagées ;
- le degré de faisabilité technique du partage des infrastructures existantes compte tenu des capacités disponibles et
- l'investissement initial réalisé par le propriétaire des ressources, sans négliger les risques inhérents à l'investissement.

Article 80 : Conditions techniques et tarifaires et conventions d'accès et d'interconnexion

L'Autorité de régulation peut imposer des obligations techniques et/ou tarifaires applicables aux prestations visées aux articles 73, 74, 76 et 77 du présent code, et peut notamment décider que la fourniture de certaines de ces prestations doit être orientée vers les coûts.

L'Autorité de régulation peut également imposer que les prestations visées articles 73, 74 et 76 du présent code soient publiées dans un catalogues d'accès et d'interconnexion dans les conditions prévues à l'article 70 du présent code.

Les conventions conclues en application des articles 73, 74, 76 et 77 du présent code sont communiquées, pour approbation, à l'Autorité de régulation, qui peut en demander la modification dans les conditions prévues à l'article 70 du présent code. Toute modification de ces conventions par les parties doit être notifiée à l'Autorité de régulation.

Un décret pris en Conseil des ministres fixe les modalités d'application de la présente Section.

Article 81 : Obligations imposées spécifiquement aux opérateurs dominants

Le Bénin

L'Autorité de régulation peut imposer les obligations prévues à la présente Section uniquement aux opérateurs désignés comme dominants en application de l'article 144 du présent code.

SECTION III

DU PARTAGE D'INFRASTRUCTURES ESSENTIELLES

Article 82 : Infrastructures essentielles

Toute personne établissant et ou ayant établi une infrastructure essentielle fait droit dans des conditions objectives, transparentes et non discriminatoires aux demandes raisonnables d'accès auxdites infrastructures et aux moyens qui y sont associés présentées par les opérateurs nationaux dans les conditions prévues à l'article 65 du présent code.

Sont notamment considérées comme des infrastructures essentielles :

- les câbles sous-marins ;
- les stations d'atterrissement de câbles sous-marins ;
- les points d'atterrissements virtuels ;
- les points d'échanges internet ;
- les réseaux de transport nationaux ;
- les boucles locales et sous-boucles locales.

L'Autorité de régulation peut identifier toute autre infrastructure comme infrastructure essentielle sur décision motivée.

Article 83 : Principe de non thésaurisation et de non spéculation

Les ressources et/ou capacités issues d'infrastructures essentielles ne peuvent faire l'objet de spéculation ou de thésaurisation de la part des opérateurs qui les exploitent ou qui y ont accès.

Article 84 : Demande d'accès aux infrastructures essentielles

Toute demande d'accès à des ressources et/ou capacités issues d'infrastructures essentielles ne peut être refusée si elle est justifiée au regard, d'une part, des besoins du demandeur et d'autre part, des capacités de l'exploitant de l'infrastructure essentielle à la satisfaire. Elle peut être refusée si elle est techniquement impossible à satisfaire, notamment au regard de l'interopérabilité des équipements et systèmes.

Toute décision de refus opposée par un exploitant d'infrastructure essentielle doit être motivée. Elle est notifiée au demandeur et portée à la connaissance de l'Autorité de régulation, ainsi que, le cas échéant, à l'autorité de régulation nationale du pays dans lequel est établi l'opérateur non national.

A la demande des parties, l'Autorité de régulation peut les assister dans les négociations des accords et conventions prévues à la présente Section.

Article 85 : Mise à disposition des infrastructures essentielles

Toutes ressources et/ou capacités issues des infrastructures essentielles doivent être octroyées dans des conditions techniques et financières raisonnables et équitables.

Legi Bénin

L'Autorité de régulation peut imposer des obligations techniques et/ou tarifaires à l'accès à ces infrastructures, et notamment imposer que la fourniture de certaines prestations doit être orientée vers les coûts.

L'Autorité de régulation peut également imposer que ces infrastructures essentielles soient publiées dans un catalogue d'accès et d'interconnexion dans les conditions prévues à l'article 70 du présent code.

Les conventions conclues en application du présent article sont communiquées, pour approbation, à l'Autorité de régulation, qui peut en demander la modification dans les conditions prévues à l'article 70 du présent code. Toute modification de ces conventions par les parties doit être notifiée à l'Autorité de régulation.

Article 86 : Obligations imposées spécifiquement aux opérateurs dominants

L'Autorité de régulation peut imposer les obligations prévues à la présente Section uniquement aux opérateurs désignés comme dominants en application de l'article 144 du présent code.

SECTION IV

DU DROIT DE PASSAGE ET SERVITUDE SUR LE DOMAINE PUBLIC

ET LES PROPRIETES PRIVEES

Article 87 : Droits de passage et servitudes

Les opérateurs et les exploitants d'infrastructures alternatives bénéficient, moyennant une juste et préalable indemnisation, de droits de passage et de servitudes sur le domaine public et de droits de passage et de servitudes sur les propriétés privées nécessaires :

- à l'installation et à l'exploitation des installations de communications électroniques ;
- à la suppression et à la prévention des perturbations électromagnétiques ou des obstacles susceptibles de perturber la propagation et la réception des ondes électromagnétiques ;
- à la conservation et au fonctionnement normal des réseaux de communications électroniques.

L'Autorité de régulation peut préciser les conditions techniques et tarifaires applicables aux droits de passages sur les propriétés privées.

Sauf dispositions légales contraires, les opérateurs peuvent bénéficier des servitudes et droits de passage dont bénéficient déjà tout autre opérateur ou exploitant d'infrastructures alternatives en République du Bénin, sous réserve de ne pas aggraver significativement ces servitudes ou droits de passage au détriment de la personne publique ou privée propriétaire ou gestionnaire du domaine public ou de la propriété privée concernée.

Article 88 : Prérogatives en matière d'installation des lignes

Lorsqu'un opérateur est privé de l'accès à des propriétés publiques ou privées du fait de la nécessité de la protection de l'environnement, de la santé et de la sécurité publique ou de la réalisation d'objectifs d'urbanisme ou d'aménagement du territoire, l'Autorité de régulation peut imposer le partage d'infrastructures ou de biens fonciers, y compris la colocalisation physique, à un opérateur déjà établi, ou prendre des mesures visant à faciliter la coordination

Légi-Bénin

des travaux, après que les parties intéressées ont eu la possibilité de donner leur avis dans un délai maximum d'un (01) mois.

Les accords de partage d'infrastructures, de biens fonciers, de coordination de travaux publics ou privés précisent les règles de répartition des coûts de partage.

Article 89 : Travaux de voirie

Les opérateurs titulaires de licence ou d'autorisation peuvent exécuter sur le sol ou le sous-sol des voies publiques tous travaux nécessaires à l'établissement, l'entretien et l'extension des lignes de communications électroniques, à condition d'avoir obtenu les autorisations nécessaires à cet effet et de remettre en état les tracés utilisés. Ils déterminent le tracé de ces lignes en accord avec l'autorité responsable de la voie. Les travaux nécessaires à l'établissement et à l'entretien des lignes et ouvrages de communications électroniques sont exécutés conformément aux règlements de la voirie.

Le propriétaire d'un immeuble bâti ou non bâti ou son mandataire ne peut s'opposer à l'installation d'une ligne de communications électroniques demandée par son locataire ou un occupant de bonne foi.

Toute personne établissant des infrastructures alternatives, notamment dans les secteurs de l'énergie, des transports ou encore de l'eau, peut se voir imposer des obligations en matière d'installation d'infrastructures passives de communications électroniques. Les conditions dans lesquelles ces obligations sont imposées et mises en œuvre sont précisées par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques.

Article 90 : Résolution des différends

L'Autorité de régulation est compétente pour trancher l'ensemble des différends liés à la mise en œuvre des dispositions du présent Chapitre II dans les conditions prévues au Titre V du présent Livre du code en cas de litiges graves, les tribunaux de commerce sont compétents.

legibenin

CHAPITRE III

DE L'ACCES/SERVICE UNIVERSEL

SECTION I

DES PRINCIPES GENERAUX

Article 91 : Politique nationale de développement des communications électroniques et de la poste

La politique nationale de développement des communications électroniques intègre l'accès/service universel et les ressources humaines.

Article 92 : Droit à la fourniture de l'accès/service universel de qualité

Toute personne a droit aux services des communications électroniques et aux services postaux.

L'Agence béninoise de service universel visée à l'article 109 du présent code veille à la fourniture de l'accès/service universel de qualité à des conditions tarifaires accessibles à tous.

Article 93 : Élaboration de la politique nationale d'accès/service universel

La politique nationale d'accès/service universel est élaborée par le ministre chargé des communications électroniques et de la poste qui :

- identifie les objectifs d'accès/service universel appropriés et réalistes qui tiennent compte des spécificités de l'accès universel, de l'accès public aux Technologies de l'Information et de la Communication (TIC), du service universel et des services postaux et financiers de base ;

- élabore la réglementation et les pratiques d'accès/service universel afin de prendre, pour le secteur privé, des mesures incitatives visant l'atteinte des objectifs de l'accès universel aux services de communication ;

- réalise régulièrement des études afin d'identifier les besoins et de modifier en conséquence la politique, la réglementation et les pratiques d'accès/service universel.

Article 94 : Cadre règlementaire de l'accès/service universel

Le cadre règlementaire de l'accès/service universel mis en place par le ministre chargé des communications électroniques et de la poste doit :

- être juste et transparent ;

- promouvoir l'accès aux TIC et aux services postaux et financiers ;

- promouvoir des pratiques d'attribution de licences technologiquement neutres qui permettent aux fournisseurs de services d'utiliser la technologie la plus rentable ;
- permettre de définir un cadre de l'interconnexion transparent et non discriminatoire pour orienter les tarifs d'interconnexion vers les coûts ;

- réduire le poids de la réglementation pour faire baisser les coûts de fourniture des services aux utilisateurs finaux ;

- promouvoir la concurrence pour la fourniture d'une gamme complète de services TIC et postaux afin de favoriser la disponibilité et l'accès de ces services, l'accessibilité financière, la disponibilité et l'utilisation des TIC.

Article 95 : Objectifs et contenu de la politique d'accès/service universel

Le ministre chargé des communications électroniques et de la poste, en élaborant la politique d'accès/service universel, veille à :

- assurer la promotion de l'accès à l'interconnectivité large bande à bas coût aux niveaux local et international en impliquant les pouvoirs publics, les entreprises et les organisations non gouvernementales ;

- adopter des cadres réglementaires qui favorisent l'offre de services numériques à la population ;

LégiBenin

- adopter des politiques, pour augmenter l'accès à l'internet et aux services large bande, basées sur leur propre structure de marché et pour que de telles politiques reflètent la diversité des cultures, des langues et des intérêts sociaux ;
- adopter une réglementation qui facilite l'utilisation de tous les moyens de support, que ce soit par lignes fixes ou mobiles, courant porteur, câble métallique ou optique, technologie hertzienne ou toute autre technologie ;

- proposer les initiatives encourageant l'accès public à l'internet et aux services large bande dans les écoles, les bibliothèques et autres centres communautaires.

Article 96 : Promotion des services innovants à des prix abordables

Pour faciliter l'accès aux infrastructures d'information et de communication, le Ministre chargé des communications électroniques et de la poste veille à :

- promouvoir, dans un cadre concurrentiel, transparent et non discriminatoire, l'introduction des services innovants mettant en œuvre de nouvelles technologies qui offrent des options à des prix abordables ;

- promouvoir des équipements des TIC à des prix abordables en tenant compte du pouvoir d'achat des populations.

Article 97 : Demandes de raccordement

Le ministre chargé des communications électroniques et de la poste, avec l'appui de l'Autorité de régulation, s'assure que les demandes de raccordement à un réseau de communications électroniques sont satisfaites sur l'ensemble du territoire national par au moins un opérateur.

Article 98 : Annuaire et services d'informations téléphoniques

L'Autorité de régulation veille à ce que :

- un annuaire regroupant l'ensemble des coordonnées des abonnés y compris les numéros de téléphonie fixe et mobile, soit mis à la disposition des utilisateurs sous une forme électronique ;

- des services d'informations téléphoniques à la clientèle couvrant l'ensemble des abonnés répertoriés soient accessibles à tous les utilisateurs y compris aux utilisateurs de postes téléphoniques publics ;

- les entreprises, proposant les services décrits ci-dessus, appliquent le principe de non-discrimination au traitement et à la présentation des informations qui leur ont été fournies par les opérateurs.

Article 99 : Données à caractère personnel

L'Autorité de régulation s'assure du respect des dispositions législatives et réglementaires applicables en matière de protection des données à caractère personnel et relatives à la vie privée. En particulier, les coordonnées des abonnés qui s'y opposent expressément ne sont pas publiées dans les annuaires.

Article 100 : Appels d'urgence

Légibenin

L'Autorité de régulation veille à ce qu'il soit possible de procéder gratuitement à des appels d'urgence à partir de tout poste fixe ou mobile y compris les points d'accès de services payants de communications électroniques.

Article 101 : Points d'accès

L'Autorité de régulation veille à ce que les opérateurs installent des points d'accès de services payants de communications électroniques ouverts au public, dans des conditions raisonnables, en termes de nombre et de répartition géographique.

Ils permettent l'accès auxdits services à tous les utilisateurs, notamment à ceux qui ne sont pas abonnés.

Le calendrier de déploiement des points d'accès fait partie des obligations imposées aux opérateurs.

Article 102 : Accès des personnes handicapées

Le ministère en charge des communications électroniques prend des mesures particulières pour garantir aux utilisateurs handicapés et aux utilisateurs ayant des besoins sociaux spécifiques un accès équivalent aux services de communications électroniques ouverts au public y compris les services d'urgence et d'annuaires, à un coût abordable.

Article 103 : Évaluation du service universel

Le ministre chargé des communications électroniques et de la poste évalue périodiquement la portée du service universel, en prenant en compte, entre autres, les évolutions sociales, économiques et technologiques. Il propose les mesures correctives subséquentes.

L'évaluation effectuée une fois tous les deux (02) ans, fait l'objet d'un rapport soumis à l'approbation du Conseil des ministres.

LegiBénin

SECTION II

DE LA MISE EN ŒUVRE DE L'ACCES/SERVICE UNIVERSEL

Article 104 : Coopération entre les acteurs

Dans la mise en œuvre et la gestion de l'accès/service universel, la coopération est obligatoire entre les différents acteurs notamment :

- le secteur privé et les collectivités locales, pour cerner les besoins du marché et son développement ;
- les collectivités locales, les pouvoirs publics et le secteur privé, pour s'assurer que le différentiel d'accès est traité de manière pertinente pour les communautés locales ;
- les départements ministériels, pour s'assurer que l'accroissement des bénéfices des TIC profite à tous les secteurs d'activités.

Article 105 : Détermination de l'approche pour assurer la mise en œuvre du service universel

Le ministre chargé des communications électroniques et de la poste détermine l'approche la plus efficace et la plus adaptée pour assurer la mise en œuvre du service universel sur proposition du Conseil national d'orientation.

Article 106 : Objectifs de performance

L'Agence béninoise de service universel établit des objectifs de performance pour les entreprises assumant des obligations de service universel dans le respect des procédures qu'elle définit.

Les objectifs de desserte de zone, de performance et de qualité en matière d'accès/service universel sont contenus dans un cahier des charges.

Ces objectifs sont contrôlés annuellement par l'Agence béninoise de service universel.

L'incapacité notoire d'une entreprise à atteindre les objectifs de performance et les niveaux de qualité prévus pour la mise en œuvre de l'accès/service universel entraîne des sanctions imposées par l'Agence béninoise de service universel conformément aux dispositions des articles 239 et 240 du présent code.

L'Agence béninoise de service universel a le droit d'exiger une vérification indépendante de la réalisation des obligations des opérateurs ou fournisseurs de l'accès/service universel.

SECTION III

DE LA POLITIQUE D'ACCES/SERVICE UNIVERSEL

Article 107 : Subvention pour la fourniture de l'accès/service universel

Lorsque la fourniture de l'accès/service universel représente une charge injustifiée pour les entreprises désignées comme fournisseurs, l'Agence béninoise de service universel détermine la subvention à accorder pour la fourniture de l'accès/service universel.

Le calcul du coût net des obligations de service universel est soumis à la vérification de l'Autorité de régulation.

Article 108 : Mécanismes d'octroi des subventions

Les subventions sont accordées au titre du service universel par le biais de différents mécanismes dont :

- un mécanisme d'approche globale orientée vers le marché ;
- des enchères concurrentielles de subvention minimum pour réduire le montant du financement nécessaire aux projets d'accès publics ;

- un mécanisme d'analyse permettant d'arriver rapidement à un équilibre financier, particulièrement lorsque l'on accorde de l'importance aux technologies peu coûteuses et innovantes.

SECTION IV

DE L'AGENCE BENINOISE DE SERVICE UNIVERSEL DES COMMUNICATIONS ELECTRONIQUES ET DE LA POSTE (ABSU-CEP)

Légibénin

Article 109 : Création de l'Agence Béninoise de Service Universel des Communications Electroniques et de la Poste (ABSU-CEP)

Il est créé une Agence Béninoise du Service Universel des Communications Electroniques et de la Poste, en abrégé ABSU-CEP. Elle est placée sous la tutelle du ministère en charge des communications électroniques et de la poste.

Article 110 : Siège de l'ABSU-CEP

Le siège de l'ABSU-CEP est fixé à Cotonou. Toutefois il peut être transféré en tout autre lieu du territoire national si les circonstances l'exigent, par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques et de la poste après avis du Conseil National d'Orientation.

Article 111 : Mission de l'ABSU-CEP

L'ABSU-CEP est administrée par le Conseil National d'Orientation qui a pour missions :

- d'élaborer les cahiers des charges des programmes de Service Universel des communications électroniques et de la poste ;
- d'assurer la mise en œuvre des programmes de Service Universel des communications électroniques et de la poste, pour le compte de l'État ;
- d'assurer le financement des programmes de Service Universel des communications électroniques et de la poste ;
- d'assurer la gestion des opérations d'investissement financées par l'Etat dans le domaine du Service Universel des communications électroniques et de la poste ;
- et de concourir au renforcement des capacités des ressources humaines conformément à la politique de développement des communications électroniques et de la poste.

Article 112 : Organes de gestion, personnel et contrôle de l'ABSU-CEP

L'Agence est dirigée par une direction générale et un Conseil National d'Orientation.

Le personnel de l'Agence est constitué d'agents recrutés conformément à la législation du travail en vigueur et des fonctionnaires et agents de l'Etat en position de détachement.

La gestion administrative et financière de l'ABSU-CEP est soumise à un contrôle interne et à un contrôle externe de la juridiction des comptes de l'État.

La composition, l'organisation et les modalités de fonctionnement de l'ABSU-CEP sont déterminées par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques et de la poste.

CHAPITRE IV

DE L'AUTORITE DE REGULATION DES COMMUNICATIONS ELECTRONIQUES ET DES POSTES

LégiBénin

SECTION I

DES ATTRIBUTIONS DE L'AUTORITE DE REGULATION

Article 113 : Autorité de régulation

Il est créé en République du Bénin, une autorité de Régulation des communications électroniques et de la poste ayant pour sigle "ARCEP BENIN", ci-après dénommée Autorité de régulation.

L'Autorité de régulation est une structure administrative indépendante dotée de la personnalité juridique, de l'autonomie financière et de gestion. Elle exerce ses missions de manière indépendante, impartiale, équitable et transparente.

Article 114 : Siège de l'Autorité de régulation

Le siège de l'Autorité de régulation est fixé à Cotonou. Toutefois, il peut être transféré en tout autre lieu du territoire national si les circonstances l'exigent, par décret pris en Conseil des ministres, sur proposition du ministre chargé des communications électroniques, après avis de l'Autorité de régulation.

Article 115 : Attributions de l'Autorité de régulation

L'Autorité de régulation a pour attributions, entre autres :

- de contribuer à l'élaboration, à la demande du ministre chargé des communications électroniques ou sur son initiative :

  ▪ des propositions visant à adapter le cadre juridique, économique et sécuritaire dans lequel s'exercent les activités de communications électroniques ;

  ▪ des projets de lois, de décrets et d'arrêtés relatifs au régime des activités des différents opérateurs intervenant dans le secteur des communications électroniques ;

- de préparer, à la demande du ministère en charge des communications électroniques, les cahiers des charges assortis aux licences ;

- d'instruire, à la demande du ministère en charge des communications électroniques, les demandes de licences et de donner son avis, positif ou négatif, sur les demandes de licences ;

- de proposer et d'instruire, à la demande du ministère en charge des communications électroniques, les procédures d'attribution de licences par appel à la concurrence ;

- d'instruire les demandes d'autorisation qui lui sont présentées et, le cas échéant, de les délivrer ;

- de préparer les cahiers des charges fixant les droits et obligations des titulaires d'autorisation et de les adapter à l'évolution du secteur ;

- de recevoir les déclarations préalables pour les activités de communications électroniques ne relevant pas du régime des licences ou des autorisations ;

Legi-Bénin

- de préparer les conditions d'établissement et d'exploitation que doivent respecter les exploitants de réseaux de communications électroniques et les fournisseurs de services de communications électroniques soumis au régime de la déclaration et de les adapter à l'évolution du secteur. Ces spécifications et règles ne sont opposables aux tiers qu'après leur publication au Journal officiel ;

- de fixer les spécifications techniques et administratives d'agrément des équipements terminaux et des installations radioélectriques ;

- d'apporter son appui à la mise en œuvre de la politique de développement du service universel des communications électroniques conformément aux dispositions du présent code ;

- de participer, aux côtés du ministre chargé des communications électroniques, aux réunions internationales traitant de la gestion du spectre des fréquences radioélectriques et de la réglementation des communications électroniques, ainsi que de participer aux travaux des organismes nationaux ou étrangers ayant pour objet l'étude et l'amélioration de la réglementation et de la gestion des communications électroniques ;

- d'assurer le respect des dispositions légales et règlementaires applicables par les opérateurs titulaires de licences et d'autorisation, par les opérateurs soumis au régime de la déclaration et par les titulaires d'agrément ;

- d'assurer le suivi du respect :

  ▪ des termes des licences et des autorisations ainsi que des cahiers des charges associés à ces licences et autorisations ;

  ▪ des conditions d'établissement et d'exploitation par les opérateurs titulaires de licences et d'autorisation et par les opérateurs soumis au régime de la déclaration ;

  ▪ des spécifications techniques et administratives des titulaires d'agrément des équipements terminaux et des installations radioélectriques ;

- de veiller au respect des règles de libre concurrence, et en particulier de veiller au respect de la concurrence loyale dans le secteur des communications électroniques et de trancher les litiges afférents aux pratiques anticoncurrentielles;

- d'assurer la veille technologique du secteur des communications électroniques ;

- de mettre en place les procédures rapides, transparentes et non discriminatoires des règlements de différends ;

- de gérer et de surveiller, dans le respect des contraintes liées à la sécurité publique et à la défense nationale, les ressources rares, et notamment les ressources en fréquences, les ressources en numérotation et les noms de domaine ;

Legi Benin

- de tenir à jour l'ensemble des documents relatifs à l'emploi des fréquences. A cet effet, l'ensemble des administrations et autorités affectataires lui transmettent les données nécessaires, dans le respect des dispositions relatives à la protection du secret-défense ;
- de coordonner les assignations de fréquences dans les bandes en partage et d'être informée des projets d'assignation de nouvelles fréquences dans les bandes exclusives avec dérogation sur lesquelles elle peut émettre un avis ;

- de procéder à la notification des assignations nationales au fichier international des fréquences de l'Union Internationale des Télécommunications dont elle est, pour ce domaine, l'interlocuteur unique ;

- d'assurer les fonctions de bureau centralisateur prévu par le Règlement des Radiocommunications de l'Union Internationale des Télécommunications ;

- d'assurer la coordination internationale des fréquences aux frontières et de celle des systèmes de communications électroniques par satellites ;

- d'établir, en liaison avec l'ensemble des affectataires, le plan national d'attribution des bandes de fréquences radioélectriques ;

- d'organiser et de coordonner le contrôle de l'utilisation des fréquences, sans préjudice des compétences de contrôles spécifiques exercées par les administrations et les autorités affectataires. Elle peut être saisie, par ces dernières ou par des tiers, des cas de brouillage qu'elle instruit. Elle transmet son rapport d'instruction à l'administration ou à l'autorité affectataire concernée.

Article 116 : Enquêtes, vérifications, analyses et communication de documents

L'Autorité de régulation est également une structure d'enquêtes de vérifications et d'analyses.

A ce titre, elle peut, de sa propre initiative, procéder aux enquêtes, vérifications et demandes de documents et d'informations, sur place et sur pièces, auprès des opérateurs et auprès de la clientèle, afin d'identifier des dysfonctionnements, d'en déterminer les causes et les responsabilités et d'exiger les corrections nécessaires.

Les opérateurs doivent faire droit à toute demande d'informations et de documents qui leur est adressée par l'Autorité de régulation, et doivent notamment communiquer, selon une périodicité définie par l'Autorité de régulation, les informations nécessaires :

- à la collecte des taxes, redevances et autres contributions sectorielles ;
- à l'établissement par l'Autorité de régulation de bilans comparatifs dans l'intérêt des utilisateurs, relatifs à la qualité de service et aux prix ;
- à la conduite des analyses des marchés prévues aux articles 143 et suivants du présent code, et notamment :
  - la description de l'ensemble des services offerts ;
  - les tarifs et conditions générales de leurs offres ;
  - les données statistiques de trafic ;
  - les données de chiffre d'affaires ;
  - les données de parcs de clients ;

Legibénin

- les prévisions de croissance de leur activité ;
- les informations relatives au déploiement de leur réseau ;
- les informations comptables et financières pertinentes.

A la demande de l'Autorité de régulation, les opérateurs doivent également lui communiquer toute information et document qu'elle exige de façon ponctuelle. Ces documents et informations sont précisés par voie règlementaire.

Article 117 : Expertises extérieurs

Dans le cadre de l'accomplissement de sa mission, l'Autorité de régulation peut faire appel, en cas de nécessité, à toutes compétences et expertises extérieures, notamment sur le plan juridique, économique et technique.

Article 118 : Objectifs visés par l'Autorité de régulation

L'Autorité de régulation prend, dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées en vue d'atteindre les objectifs suivants :

- l'application et le respect des dispositions législatives et réglementaires en vigueur ;
- l'application du principe de la neutralité technologique en vue de la fourniture des services ;
- le maintien d'un marché ouvert et concurrentiel pour les réseaux et services de communications électroniques ;
- l'application à tous les opérateurs d'un traitement équitable et non-discriminatoire ;
- le respect du principe du contradictoire et des droits de la défense en mettant les parties à même de présenter leurs observations ;
- le respect par les opérateurs de la protection des données à caractère personnel, du secret des correspondances et du principe de neutralité vis-à-vis du contenu des messages transmis ;
- l'intégrité et la sécurité des réseaux de communications électroniques ouverts au public et le respect, par les opérateurs, de l'ordre public et des obligations de défense et de sécurité publique ;
- la protection des droits et des intérêts des consommateurs et des utilisateurs des services de communications électroniques, y compris ceux handicapés, personnes âgées ou ayant des besoins sociaux spécifiques ;
- le développement de l'investissement, de l'innovation et de la compétitivité dans le secteur des communications électroniques ;
- la mise en place des mécanismes transparents de consultation, de publication et d'information des acteurs du secteur sous réserve des clauses de confidentialité ;
- la contribution à la préparation des études et des actes réglementaires relatifs au secteur des communications électroniques.

Article 119 : Obligation de transparence

Legi-Benin

L'Autorité de régulation doit publier, dans un délai maximal de cinq (05) jours ouvrés suivant leur adoption ou finalisation, l'ensemble des décisions qu'elle adopte, son règlement intérieur, les licences, autorisations et cahiers des charges assortis des opérateurs, la liste des opérateurs déclarés, le plan national de fréquence à jour, le plan national de numérotation ainsi que son rapport d'activité annuel.

Article 120 : Recours contre les décisions de l'Autorité de régulation

Sauf lorsque le présent code prévoit d'autres voies ou d'autres modalités de recours, les décisions adoptées par l'Autorité de régulation peuvent faire l'objet d'un appel devant la chambre administrative de la Cour Suprême et par toute partie intéressée dans un délai d'un (01) mois suivant :

- sa notification aux intéressées pour les décisions individuelles ;
- sa publication sur le site internet de l'Autorité pour les autres décisions.

SECTION II

DES ORGANES DE L'AUTORITE DE REGULATION

Article121 : Le Conseil de régulation et le Secrétariat exécutif

Les organes de l'Autorité de régulation sont le Conseil de régulation et le Secrétariat exécutif.

Le Conseil de régulation est constitué de neuf (09) conseillers.

Le Secrétariat exécutif est composé du Secrétaire exécutif et des autres membres du personnel.

Article 122 : Le Conseil de régulation

Le Conseil de régulation est l'organe de délibération et de décision de l'Autorité de régulation.

Il a pour missions de :

- superviser les activités de l'Autorité de régulation en application des orientations et de la politique dans le domaine des communications électroniques et de la poste ;
- veiller au bon exercice des fonctions et attributions statutaires de l'Autorité de régulation.

Article 123 : Délibérations du Conseil de régulation

Le Conseil de régulation délibère sur :

- les plans stratégiques à court, moyen et long termes de l'Autorité de régulation élaborés par le Secrétaire exécutif pour la mise en œuvre de l'ensemble des éléments constitutifs de la politique nationale dans le domaine des communications électroniques et de la poste ;
- les budgets ou comptes prévisionnels annuels ;
- les états et comptes financiers de fin d'exercice ;
- le plan des comptes de l'Autorité de régulation ;
- les programmes pluriannuels d'actions et d'investissements de l'Autorité de régulation ;
- les rapports annuels d'activités du Secrétaire exécutif ;
- le statut ou l'accord collectif d'établissement du personnel de l'Autorité de régulation ;
- la rémunération et les avantages à accorder au Secrétaire exécutif de l'Autorité de régulation ;

LegiBénin

- les acquisitions et les aliénations de patrimoine de l'Autorité de régulation.

Article 124 : Avis et recommandations du Conseil de régulation

Le Conseil de régulation est chargé, sur saisine du Secrétaire exécutif de l'Autorité de régulation, d'émettre des avis motivés et de faire des recommandations sur :

- les projets de décisions réglementaires élaborés par le Secrétariat exécutif ;
- le règlement des appels à la concurrence, les dossiers d'instruction afférents à l'octroi de licences y compris les textes des cahiers des charges fixant les droits et obligations des titulaires de licences et d'autorisations ;
- les dossiers d'instruction des demandes de modification des tarifs des services des communications électroniques et de la poste ;

- les dossiers d'instruction relatifs à l'approbation du catalogue d'interconnexion des opérateurs ;

- les procédures de règlement des différends et de conciliation entre opérateurs et les plaintes des utilisateurs ;

- toute autre question afférente aux missions de l'Autorité de régulation définies par le présent code.

Lég-Bénin

Article 125 : Membres du Conseil de régulation

Les neuf (09) membres du Conseil de régulation sont retenus en raison de leurs qualités morales, de leurs compétences et expériences professionnelles avérées dans le domaine des communications électroniques et de la poste aux plans technique, économique et/ou juridique. Ils sont des cadres ayant totalisé au moins dix (10) ans d'expériences professionnelles.

Ils sont nommés par décret pris en Conseil des ministres pour un mandat de cinq (05) ans renouvelable une fois à l'issue d'une procédure transparente d'appel à candidature; sur proposition du ministre chargé des communications électroniques et de la poste à l'issue d'une procédure transparente d'appel à candidatures.

Les modalités de la procédure d'appel à candidatures sont fixées par décret pris en Conseil des ministres.

Avant la fin de leur mandat, les membres du Conseil de régulation ne peuvent être suspendus ou révoqués que pour faute lourde dûment constatée.

Article 126 : Serment

Avant leur entrée en fonction, les membres du Conseil de régulation prêtent serment au cours d'une cérémonie solennelle devant la Cour Suprême du siège de l'Autorité de régulation.

La formule du serment est la suivante :

« *Je jure solennellement de bien et fidèlement remplir mes fonctions de membre de l'Autorité de régulation des communications électroniques et de la poste, en toute indépendance et en toute impartialité, de façon digne et loyale et de garder le secret des délibérations, même après la cessation de mes fonctions* ».

Le parjure de ce serment est sanctionné conformément à la législation en vigueur.

Article 127 : Président et vice-président du Conseil de régulation

Les membres du Conseil de régulation élisent en leur sein un président et un vice-président selon les modalités prévues au règlement intérieur.

Article 128 : Incompatibilités

La qualité de conseiller est incompatible avec celle de membre du Gouvernement, avec l'exercice de tout mandat électif et de tout intérêt personnel lié au secteur des communications électroniques ou de la poste, à l'exception des activités d'enseignement et/ou de recherche.

Article 129 : Le Secrétariat exécutif

Le Secrétariat exécutif est l'organe exécutif de l'Autorité de régulation. Il exécute les délibérations du Conseil de régulation.

Il a à sa tête un Secrétaire exécutif nommé pour un mandat de cinq (05) ans renouvelable une fois par décret pris en Conseil des ministres, sur proposition du ministre chargé des communications électroniques et de la poste, au terme d'une procédure de sélection par appel à candidatures conduite par le Conseil de régulation.

Le Secrétaire exécutif est choisi en raison de ses compétences et qualifications dans le domaine des communications électroniques et de la poste.

Article 130 : Pouvoirs et responsabilité du Secrétaire exécutif

Le Secrétaire exécutif dispose de tous les pouvoirs pour assumer ses fonctions dans la limite des missions et attributions de l'Autorité de régulation.

A cet effet, il est chargé notamment :

- d'exécuter les délibérations du Conseil de régulation ;
- de soumettre au Conseil de régulation pour approbation avant adoption les plans stratégiques, les plans d'actions et les programmes budgétaires ;
- d'exécuter ces plans et programmes ;
- d'assurer le respect strict des procédures internes de passation des marchés, contrats et conventions ;
- de représenter l'Autorité de régulation en justice et d'intenter toutes les actions judiciaires ayant pour objet la défense des intérêts de l'Autorité de régulation ;
- d'assister aux réunions du Conseil de régulation au sein duquel, sans droit de vote, il assure le secrétariat ;
- d'assurer la préparation technique des dossiers à soumettre à l'approbation du Conseil de régulation.

Dans le cadre de ses fonctions, la responsabilité civile et pénale du secrétaire exécutif peut être engagée conformément à la législation en vigueur.

Article 131 : Révocation du Secrétaire exécutif

Legi-Bénin

Le Secrétaire exécutif peut être révoqué pour l'un des motifs suivants :

- Incapacité dûment constatée ;
- Faute lourde ;
- Agissements incompatibles avec ses fonctions.

La décision de révocation du Secrétaire exécutif est prise dans les mêmes conditions que celles de sa nomination.

Article 132 : Budget de l'Autorité de régulation

Le Secrétaire exécutif est l'ordonnateur du budget de l'Autorité de régulation.

A ce titre, il :

- ordonne et met en recouvrement les ressources ou recettes établies au profit de l'Autorité de régulation ;

- ordonne les dépenses de l'Autorité de régulation.

Article 133 : Rapport d'activités

Le Secrétaire exécutif établit, le 31 mars au plus tard de chaque année, un rapport sur les activités de l'Autorité de régulation de l'année précédente qu'il soumet au Conseil de régulation pour approbation et transmission au Gouvernement.

Article 134 : Personnel du Secrétariat exécutif

Outre le Secrétaire exécutif, le personnel du Secrétariat exécutif est constitué :

- des agents recrutés selon les règles du code du travail ;
- des fonctionnaires et agents de l'Etat en position de détachement.

Article 135 : Organisation et fonctionnement du Conseil de régulation et du Secrétariat exécutif

Les modalités d'organisation et de fonctionnement du Conseil de régulation et du Secrétariat exécutif sont déterminées par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques et de la poste.

L'Autorité de régulation adopte son règlement intérieur.

SECTION III

DES RESSOURCES HUMAINES, MATERIELLES ET FINANCIERES DE L'AUTORITE DE REGULATION

Article 136 : Recrutement du personnel de l'Autorité de régulation

Le Secrétaire exécutif recrute le personnel de l'Autorité de régulation dans le respect des dispositions législatives et réglementaires en vigueur.

Article 137 : Règles relatives au personnel de l'Autorité de régulation

Log-i-Ren-in

Les fonctionnaires et agents de l'État en détachement auprès de l'Autorité de régulation sont soumis, pendant la durée de l'emploi, aux textes régissant l'Autorité de régulation et à la législation du travail.

Les employés de l'Autorité de régulation sont interdits, dans tous les cas, d'être salariés ou de bénéficier de rémunérations d'un autre établissement public ou privé. Ils sont également interdits d'avoir un quelconque intérêt direct ou indirect dans les entreprises des secteurs régulés.

Article 138 : Missions et pouvoirs du personnel de l'Autorité de régulation

Le personnel de l'Autorité de régulation chargé d'effectuer les missions de contrôle, de vérification, d'enquête et d'information est assermenté.

A ce titre, il procède au contrôle des équipements, à la saisie des matériels et à la fermeture des locaux, conformément au présent code.

Article 139 : Ressources financières de l'Autorité de régulation

Les ressources financières de l'Autorité de régulation comprennent :

- le produit des redevances perçues à l'occasion de l'étude des dossiers et de l'octroi ou du renouvellement des licences et des autorisations, du traitement des déclarations, du traitement des demandes d'assignation des fréquences radioélectriques et de numéros ;
- le produit de toutes redevances en relation avec les missions de l'Autorité de régulation ;
- un pourcentage sur le produit de la contrepartie financière versée par les opérateurs à l'occasion d'une opération de cession ou de renouvellement de licence. Ce pourcentage est fixé par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques après avis conforme de l'Autorité de régulation ;
- les produits et les revenus provenant des biens mobiliers et immobiliers ;
- les avances ou prêts remboursables du Trésor, d'organismes publics ou privés ;
- les emprunts autorisés conformément à la législation en vigueur ;
- les produits des placements ;
- les subventions, dons et legs ;
- toutes autres recettes en rapport avec ses activités statutaires.

Article 140 : Charges de l'Autorité de régulation

Les charges de l'Autorité de régulation comprennent les dépenses de fonctionnement et les dépenses d'investissement.

Article 141 : Contrôle de la gestion administrative et financière de l'Autorité de régulation

La gestion administrative et financière de l'Autorité de régulation est soumise à un contrôle interne et à un contrôle externe.

Le contrôle externe est assuré par la juridiction des comptes de l'État.

Article 142 : Communication des rapports de contrôle externes

Les rapports établis à la suite des contrôles externes sont communiqués simultanément au ministre chargé des finances et au ministre chargé des communications électroniques.

Le Droit Privé

CHAPITRE V

DE LA DOMINANCE ET DE LA CONCURRENCE

SECTION I

DE LA REGULATION DES OPERATEURS DOMINANTS

SOUS-SECTION I

DE L'IDENTIFICATION DES MARCHES PERTINENTS, DE LA DESIGNATION DES OPERATEURS DOMINANTS ET DETERMINATION DES OBLIGATIONS APPLICABLES A CES OPERATEURS

Article 143 : Identification des marchés pertinents

L'Autorité de régulation détermine, au regard notamment des obstacles au développement d'une concurrence effective, les marchés du secteur des communications électroniques pertinents, en vue de l'application des articles 151 et suivants du présent code.

Article 144 : Désignation des opérateurs dominants

Après avoir analysé l'état et l'évolution prévisible de la concurrence sur les différents marchés, l'Autorité de régulation établit la liste des opérateurs dominants sur chacun de ces marchés.

Article 145 : Appréciation de la position dominante

Tout opérateur disposant sur un marché de services ou d'un groupe de services d'une puissance significative, équivalent au moins à 25 % du volume ou de la valeur de ce marché peut être déclaré dominant.

La position dominante de l'opérateur est appréciée sur la base des critères suivants :

- sa capacité à influencer le marché ;
- son chiffre d'affaires par rapport à la taille du marché ;
- le contrôle qu'il exerce sur les moyens d'accès à l'utilisateur final ou
- sa capacité à agir indépendamment de ses concurrents, de ses clients et des consommateurs.

L'Autorité de régulation identifie et publie annuellement, dans les conditions spécifiées par arrêté du ministre chargé des communications électroniques, la liste des opérateurs dominants.

Elle fixe, pour chaque opérateur concerné, les contraintes liées à cette position dans le but de garantir une concurrence saine.

Les obligations que doivent respecter les opérateurs dont les parts de marché sur un marché du secteur des communications électroniques sont supérieures à un pourcentage déterminé par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques sont précisées dans ce décret.

LegiBenin

Article 146 : Détermination des obligations applicables aux opérateurs dominants

L'Autorité de régulation précise, en les motivant, les obligations des opérateurs dominants sur un marché du secteur des communications électroniques.

Ces obligations qui s'appliquent pendant une durée limitée fixée par l'Autorité de régulation, pour autant qu'une nouvelle analyse du marché concerné, effectuée en application du présent article ne les rende pas caduques.

Toute autre obligation résultant des dispositions du droit de la CEDEAO et de l'UEMOA qui sont d'application directe en République du Bénin peut être appliquée à un opérateur dominant.

Article 147 : Typologie d'obligations qui peuvent être imposées aux opérateurs dominants

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer des obligations :

- de transparence ;
- de non-discrimination ;
- de séparation comptable ;
- d'accès aux réseaux de communications électroniques, aux ressources spécifiques associées à ces réseaux et aux infrastructures passives, y compris les infrastructures alternatives ;
- de contrôle des prix et d'obligations relatives au système de comptabilisation des coûts ;
- de séparation fonctionnelle.

Le cas échéant, l'Autorité de régulation peut également imposer la mise en œuvre d'un mécanisme de sélection ou de présélection du transporteur. Dans ce cas, les modalités de mise en œuvre de cette mesure sont précisées par voie règlementaire.

Article 148 : Critère d'évaluation des obligations imposées aux opérateurs dominants

Lorsqu'elle examine s'il y a lieu d'imposer les obligations visées au présent Chapitre, et en particulier lorsqu'elle évalue si ces obligations seraient proportionnées aux objectifs énoncés à l'article 118 du présent code, l'Autorité de régulation prend notamment en considération les éléments suivants :

- la viabilité technique et économique de l'utilisation ou de la mise en place de ressources concurrentes, compte tenu du rythme auquel le marché évolue et de la nature et du type d'interconnexion et d'accès concerné ;
- le degré de faisabilité de la fourniture d'accès proposée, compte tenu de la capacité disponible ;
- l'investissement initial réalisé par le propriétaire des ressources, sans négliger les risques inhérents à l'investissement ;
- la nécessité de préserver la concurrence à long terme ;
- les éventuels droits de propriété intellectuelle ;
- l'établissement de réseaux de communications électroniques et la fourniture de services de communications électroniques régionaux et panafricains.

SOUS-SECTION II

DES OBLIGATIONS EN MATIERE DE TRANSPARENCE

Légi-Bénin

ET DE NON-DISCRIMINATION

Article 149 : Obligations de transparence

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer des obligations de transparence concernant l'interconnexion et/ou l'accès en vertu desquelles les opérateurs doivent rendre publiques des informations bien définies, telles que les informations comptables, les spécifications techniques, les caractéristiques du réseau, les modalités et conditions de fourniture et d'utilisation et les prix.

Article 150 : Obligation de non-discrimination

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer des obligations de non-discrimination.

Lorsqu'un opérateur est soumis à des obligations de non-discrimination, l'Autorité de régulation peut notamment imposer que l'offre de référence qu'il publie :

- soit suffisamment détaillée pour garantir que les bénéficiaires de cette offres ne sont pas tenus de payer pour des ressources qui ne sont pas nécessaires pour le service demandé ;
- comprenne une description des offres pertinentes réparties en divers éléments selon les besoins du marché ;
- soit accompagnée des modalités et conditions correspondantes, y compris des prix.

LégiBénin

SOUS-SECTION III

DES OBLIGATIONS EN MATIERE DE SEPARATION COMPTABLE

Article 151 : Obligation de séparation comptable

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer des obligations de séparation comptable en ce qui concerne certaines activités de communications électroniques.

Elle peut, notamment, obliger un opérateur intégré verticalement à rendre ses prix de gros et ses prix de transferts internes transparents, entre autres pour garantir le respect de l'obligation de non-discrimination prévue à l'article 150 du présent code ou, en cas de nécessité, pour empêcher des subventions croisées abusives.

L'Autorité de régulation peut spécifier le format et les méthodologies comptables à utiliser.

Dans ce cas, la comptabilité de l'opérateur est auditée annuellement à ses frais par un organisme indépendant sélectionné par l'Autorité de régulation.

Article 152 : Communication des documents comptables

L'Autorité de régulation peut, afin de faciliter la vérification du respect des obligations de transparence, de non-discrimination et de séparation comptable, exiger que les documents comptables, y compris les données concernant les recettes provenant de tiers, lui soit fournis si elle en fait la demande.

L'Autorité de régulation peut publier ces informations dans la mesure où elles contribuent à l'instauration d'un marché ouvert et concurrentiel, dans le respect de la réglementation nationale et communautaire sur la confidentialité des informations commerciales.

SOUS-SECTION IV

DES OBLIGATIONS RELATIVES A L'ACCES A DES RESSOURCES DE RESEAU SPECIFIQUES ET A LEUR UTILISATION

Article 153 : Obligation de faire droit à certaines demandes spécifiques

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer à des opérateurs l'obligation de satisfaire les demandes raisonnables d'accès à des éléments de réseau spécifiques et à des ressources associées et d'en autoriser l'utilisation, notamment lorsqu'elle considère qu'un refus d'octroi de l'accès ou des modalités et conditions déraisonnables ayant un effet similaire empêcheraient l'émergence d'un marché de détail concurrentiel durable ou risqueraient d'être préjudiciables à l'utilisateur final.

Les opérateurs peuvent notamment se voir imposer :

- d'accorder à des tiers l'accès à des éléments et/ou ressources de réseau spécifiques, y compris l'accès dégroupé à la boucle locale ;
- de fournir des prestations d'itinérance nationales ;
- de fournir des prestations d'accès à son réseau nécessaires aux opérateurs mobiles virtuels ;
- de négocier de bonne foi avec les opérateurs qui demandent un accès ;
- de ne pas retirer l'accès aux ressources lorsqu'il a déjà été accordé ;
- d'offrir des services particuliers en gros en vue de la revente à des tiers ;
- d'accorder un accès ouvert aux interfaces techniques, protocoles ou autres technologies clés qui revêtent une importance essentielle pour l'interopérabilité des services ou des services de réseaux virtuels ;
- de fournir une possibilité de colocalisation ou d'autres formes de partage des ressources, y compris le partage des gaines, des bâtiments ou entrées de bâtiments, des antennes ou pylônes, des trous de visite et boîtiers situés dans la rue ;

- de fournir les services spécifiques nécessaires pour garantir aux utilisateurs l'interopérabilité des services de bout en bout, notamment en ce qui concerne les ressources destinées aux services de réseaux intelligents ou permettant l'itinérance sur les réseaux mobiles ;

- de fournir l'accès à des systèmes d'assistance opérationnelle ou à des systèmes logiciels similaires nécessaires pour garantir l'existence d'une concurrence loyale dans la fourniture des services ;

- d'interconnecter des réseaux ou des ressources de réseau ;

- de donner accès à des services associés comme ceux relatifs à l'identité, l'emplacement et l'occupation.

Texte Officiel

L'Autorité de régulation peut associer à ces obligations des conditions concernant le caractère équitable ou raisonnable de ces prestations et le délai de fourniture de ces prestations.

Article 154 : Conditions techniques ou opérationnelles imposées aux opérateurs dominants

Lorsque l'Autorité de régulation impose à un opérateur l'obligation de fournir un accès conformément aux dispositions de la présente Section, elle peut fixer, de façon objective, transparente, proportionnée et non discriminatoire, des conditions techniques ou opérationnelles auxquelles le fournisseur et/ou les bénéficiaires de l'accès doivent satisfaire pour assurer le fonctionnement normal du réseau. L'obligation de respecter certaines normes ou spécifications techniques doit être compatible avec les normes et spécifications en vigueur.

SOUS-SECTION IV

DU CONTROLE DES PRIX ET DES OBLIGATIONS RELATIVES AU SYSTEME DE COMPTABILISATION DES COUTS

LegiBénin

Article 155 : Tarifs de détail

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer aux opérateurs dominants des obligations d'information et des obligations de nature tarifaire relatives à leurs offres et leurs tarifs de détail visant à empêcher ou limiter :

- toute différenciation tarifaire on-net/off-net ;
- tout effet de ciseau tarifaire ;
- tout effet d'éviction ;
- toute subvention croisée d'une activité de communications électroniques par une autre activité.

A cet effet, l'Autorité de régulation peut imposer aux opérateurs dominants un contrôle *ex ante* de leurs offres et tarifs y compris promotionnels sur le marché de détail.

Article 156 : Orientation des prix en fonction des coûts et systèmes de comptabilisation des coûts

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer des obligations de nature tarifaire, y compris les obligations concernant l'orientation des prix en fonction des coûts et les obligations concernant les systèmes de comptabilisation des coûts, pour la fourniture de types particuliers d'interconnexion et/ou d'accès, lorsqu'une analyse du marché indique que l'opérateur concerné pourrait, en l'absence de concurrence efficace, maintenir les prix à un niveau excessivement élevé ou comprimer les prix.

L'Autorité de régulation tient compte des investissements réalisés par l'opérateur et lui permet une rémunération raisonnable du capital adéquat engagé, compte tenu des risques encourus.

Article 157 : Méthodologies de tarification

L'Autorité de régulation veille à ce que les méthodologies de tarification qui seraient rendues obligatoires visent à promouvoir l'efficacité économique, à favoriser une concurrence durable et à optimiser les avantages pour le consommateur.

A cet égard, l'Autorité de régulation peut également prendre en compte les prix en vigueur sur les marchés concurrentiels comparables.

Article 158 : Preuve du respect des obligations de nature tarifaire

Lorsqu'un opérateur est soumis à une obligation de nature tarifaire, notamment une obligation d'orientation des prix en fonction des coûts, il lui incombe de prouver que ses tarifs sont déterminés en fonction des coûts, en tenant compte d'un retour sur investissements raisonnable.

Afin de calculer les coûts de la fourniture d'une prestation efficace, l'Autorité de régulation peut utiliser des méthodes de comptabilisation des coûts distinctes de celles appliquées par l'opérateur.

L'Autorité de régulation peut demander à un opérateur de justifier intégralement ses prix et, si nécessaire, en exiger l'adaptation.

Article 159 : Système de comptabilisation des coûts

Lorsque la mise en place d'un système de comptabilisation des coûts est rendue obligatoire dans le cadre d'un contrôle des prix, l'Autorité de régulation veille à ce que soit mise à la disposition du public une description du système de comptabilisation des coûts faisant apparaître au moins les principales catégories au sein desquelles les coûts sont regroupés et les règles appliquées en matière de répartition des coûts.

Le respect du système de comptabilisation des coûts est vérifié par un organisme compétent indépendant. Une attestation de conformité est publiée annuellement.

Article 160 : Asymétrie tarifaire

L'Autorité de régulation peut décider de l'application de tarifs asymétriques au bénéfice d'un nouvel opérateur qui intègre un marché, ou en cas de déséquilibre significatif des ressources en fréquences au détriment d'un opérateur. Une telle mesure doit être justifiée et doit être limitée dans le temps.

LegiBenin

SOUS-SECTION VI

DE LA SEPARATION FONCTIONNELLE

Article 161 : Obligation de création d'une entité économique fonctionnellement indépendante

L'Autorité de régulation peut, conformément aux dispositions de l'article 143 du présent code, imposer à un opérateur verticalement intégrée l'obligation de confier ses activités de fourniture en gros de produits d'accès à une entité économique fonctionnellement indépendante.

Cette entité économique fournit des produits et services d'accès à tous les opérateurs, y compris aux autres entités économiques au sein de la société mère, aux mêmes échéances et conditions, y compris en termes de tarif et de niveaux de service et à l'aide des mêmes systèmes et procédés.

Article 162 : Justification de la mesure

Lorsque l'Autorité de régulation entend imposer une obligation de séparation fonctionnelle, elle doit démontrer que l'imposition d'obligations appropriées, parmi celles recensées dans le présent Chapitre, pour assurer une concurrence effective à la suite d'une analyse coordonnée des marchés pertinents conformément à la procédure en vigueur a échoué et échouerait

systématiquement pour atteindre cet objectif et qu'il existe des problèmes de concurrence ou des défaillances du marché importants et persistants sur plusieurs de ces marchés de produits.

L'Autorité de régulation doit en outre réaliser une analyse de l'effet de la mesure escomptée :

- sur l'opérateur et sa motivation à investir dans son réseau ;
- sur la concurrence entre infrastructures ;
- pour les consommateurs.

Article 163 : Contenu de la mesure

Le projet de mesure comporte les éléments suivants :

- la nature et le degré précis de séparation et, en particulier, le statut juridique de l'entité économique distincte ;
- la liste des actifs de l'entité économique distincte ainsi que des produits ou services qu'elle doit fournir ;
- les modalités de gestion visant à assurer l'indépendance du personnel employé par l'entité économique distincte et les mesures incitatives correspondantes ;
- les règles visant à assurer le respect des obligations ;
- les règles visant à assurer la transparence des procédures opérationnelles, en particulier pour les autres parties intéressées ;
- un programme de contrôle visant à assurer la conformité et comportant la publication d'un rapport annuel.

Article 164 : Autres obligations applicables aux opérateurs soumis à une mesure de séparation fonctionnelle

Un opérateur auquel a été imposée la séparation fonctionnelle peut être soumis à toute autre obligation visée dans le présent Chapitre sur tout marché particulier où il a été désigné comme dominant conformément à l'article 144 du présent code ou à toute autre obligation résultant du droit de la CEDEAO et de l'UEMOA directement applicable.

SECTION II

DE LA CONCURRENCE

Article 165 : Compétences en matière de droit de la concurrence

L'Autorité de régulation veille au respect de la concurrence dans le secteur des communications électroniques et tranche les litiges y afférents, notamment ceux relatifs aux pratiques anticoncurrentielles.

L'Autorité de régulation informe le Conseil National de la Concurrence des décisions prises en vertu de la présente Section.

Les modalités de mise en œuvre des dispositions de la présente Section sont fixées par voie réglementaire.

Article 166 : Enquêtes

Legi-Bénin

Les agents assermentés de l'Autorité de régulation peuvent procéder aux enquêtes nécessaires. Ils sont astreints au secret professionnel.

Les agents assermentés de l'Autorité de régulation peuvent accéder à tous locaux, terrains ou moyens de transport à usage professionnels, demander la communication des livres, des factures et tous autres documents professionnels et en prendre copie et recueillir, sur convocation ou sur place, les renseignements et justifications.

Ces opérations de visites et saisies ne peuvent être réalisées qu'en présence du procureur de la République, ou en présence des officiers de police judiciaire qu'il a désignés. Elles ne peuvent commencer avant six heures ou après vingt et une heure et sont effectuées en présence de l'occupant des lieux ou de son représentant. En cas de refus ou d'impossibilité, l'officier de police judiciaire requiert à cet effet deux témoins pris en dehors du personnel relevant de son autorité et de celui de l'Autorité de régulation.

Il est procédé à un inventaire des pièces saisies. Le cas échéant, celles-ci peuvent être mises sous scellés.

Il est dressé procès-verbal des opérations de visites et saisies.

Les agents assermentés de l'Autorité de régulation peuvent, sans se voir opposer le secret professionnel, accéder à tout document ou élément d'information détenu parles administrations, les établissements et les autres personnes morales de droit public.

Article 167 : Communication des pièces et convocation

L'Autorité de régulation peut demander la communication de toutes pièces ou documents et convoquer toute personne ou toute entreprise.

En cas de refus de se rendre à une convocation ou de communiquer une pièce ou un document, ou en cas d'obstruction à l'instruction ou à l'enquête, notamment en fournissant des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou dénaturées, l'Autorité de régulation peut :

- prononcer une astreinte, dans la limite et suivant les modalités prévues à l'article 172 ;
- infliger à l'intéressé une sanction pécuniaire dont le montant ne peut excéder 1 % du montant du chiffre d'affaires mondial hors taxes le plus élevé réalisé au cours d'un des exercices clos depuis l'exercice précédent celui au cours duquel les pratiques ont été mises en œuvre.

Article 168 : Mesures à adopter par l'Autorité de régulation

Lorsqu'elle constate des pratiques anticoncurrentielles, l'Autorité de régulation prend l'une ou l'autre des mesures suivantes :

- ordonne des mesures conservatoires qui lui sont demandées ou qui apparaissent nécessaires, telles que la suspension de la pratique concernée ou encore une injonction de revenir à l'état antérieur ;
- ordonne aux intéressés de mettre fin aux pratiques anticoncurrentielles dans un délai déterminé ;
- impose aux intéressés des conditions particulières ;
- accepter et rendre obligatoire un engagement pris par les intéressés au cours de la procédure afin de mettre un terme aux préoccupations de concurrence susceptibles de constituer des pratiques anticoncurrentielles ;

Legi-Benin

- prononce une sanction pécuniaire conformément aux dispositions des articles 170 et 171 du présent code ;
- prononce une astreinte conformément aux dispositions de l'article 172 du présent code ;
- ordonne la publication, la diffusion ou l'affichage de sa décision ou d'un extrait de celle-ci selon les modalités qu'elle précise aux frais de l'intéressé.

Article 169 : Pratiques non sanctionnées

Ne sont pas sanctionnées les pratiques :

- qui résultent de l'application d'un texte législatif ou d'un texte règlementaire pris pour son application ;

- dont les auteurs peuvent justifier qu'elles ont pour effet de contribuer au progrès économique et/ou technique, y compris par la création ou le maintien d'emplois, et qu'elles réservent aux utilisateurs une partie équitable du profit qui en résulte, sans donner aux entreprises intéressées la possibilité d'éliminer la concurrence pour une partie substantielle des biens, produits et services en cause. Ces pratiques ne doivent imposer des restrictions à la concurrence que dans la mesure où elles sont indispensables pour atteindre cet objectif de progrès.

Article 170 : Sanctions pécuniaires

Lorsqu'elle constate des pratiques anticoncurrentielles, l'Autorité de régulation peut imposer aux intéressés des sanctions pécuniaires dont le montant peut atteindre :

- pour une personne physique, deux cent cinquante millions (250 000 000) de francs CFA ;
- pour une entreprise, 10 % du montant du chiffre d'affaires hors taxes, national ou mondial consolidé, le plus élevé réalisé au cours d'un des derniers exercices clos depuis l'exercice précédent celui au cours duquel les pratiques ont été mises en œuvre.

En cas de récidive dans un délai de cinq (05) ans, le montant maximum de la sanction pécuniaire peut être porté au double.

Article 171 : Exonération des sanctions pécuniaires

Une exonération totale ou partielle des sanctions pécuniaires peut être accordée à une entreprise ou à un organisme qui, avec d'autres, a mis en œuvre une pratique anticoncurrentielle s'il a contribué à établir la réalité de la pratique prohibée et à identifier ses auteurs, en apportant des éléments d'information dont l'Autorité de régulation ou l'administration ne disposaient pas antérieurement.

Article 172 : Astreinte

Lorsqu'elle constate des pratiques anticoncurrentielles, l'Autorité de régulation peut prononcer une astreinte dans la limite de 5 % du chiffre d'affaires journalier moyen hors taxes, par jour de retard à compter de la date fixée pour exécuter une décision ayant ordonné des mesures conservatoires, ayant ordonné de mettre fin aux pratiques anticoncurrentielles ou ayant imposé des conditions particulières.

Le chiffre d'affaires pris en compte est calculé sur la base des comptes de l'entreprise relatifs au dernier exercice clos à la date de la décision ou, en l'absence de chiffre d'affaires, peut atteindre trois cent mille (300 000) francs CFA.

Legi-Bénin

L'astreinte est liquidée par l'Autorité de régulation, qui en fixe le montant définitif.

Article 173 : Recours

Les décisions prises par l'Autorité de régulation dans le cadre de la présente Section peuvent faire l'objet d'un appel devant la chambre administrative de la Cour suprême dans un délai d'un (01) mois.

Article 174 : Coopération avec les autorités régionales de concurrence

L'Autorité de régulation coopère avec les autorités de régulation régionales, les autorités chargées de l'application du droit de la concurrence et celles chargées de l'application des mesures de protection des consommateurs établies dans les autres États Membres de la CEDEAO et de l'UEMOA.

L'Autorité de régulation peut demander ou recevoir des informations aux autorités mentionnées au présent article. Elle doit assurer la confidentialité des informations envoyées et reçues qui relèvent du secret des affaires.

TITRE III

DE LA GESTION DES RESSOURCES RARES

CHAPITRE I

DES DISPOSITIONS GENERALES

Article 175 : Typologie des ressources rares

Les ressources rares sont :

- les numéros ;
- les adresses ;
- les noms du domaine internet national ;
- le spectre des fréquences radioélectriques.

Leur gestion est du domaine exclusif de l'Etat.

Article 176 : Règles de gestion des ressources rares

Les règles de gestion des ressources rares s'inscrivent dans le cadre de l'ouverture du marché national à la libre concurrence et à son intégration au marché sous régional.

Elles tiennent compte :

- de la politique nationale ;
- des conventions et des accords régionaux et internationaux ratifiés par la République du Bénin ;
- de l'efficacité économique par l'attribution des ressources rares en fonction des besoins des opérateurs et de l'utilisation desdites ressources par ceux-ci, de l'augmentation de la valeur procurée par ces ressources, de la souplesse et de la rapidité de réponse à l'évolution du marché ;

LégiBénin

- de l'efficacité technique pour une optimisation de l'utilisation intensive des disponibilités limitées, dans le respect des contraintes techniques.

Article 177 : Droit d'utiliser des ressources rares

L'utilisation de ressources rares qui font l'objet d'une attribution par l'Autorité de régulation, sous quelque forme que ce soit, requiert l'obtention d'une licence, d'une autorisation ou la réalisation d'une déclaration, sauf dans les cas où le présent code en dispose autrement.

En cas de non respect des dispositions relatives à l'attribution ou à l'utilisation de ces ressources rares, celles-ci peuvent être retirées par l'Autorité de régulation dans les conditions prévues aux articles 239 et suivants du présent code.

En cas d'annulation, de retrait, d'abandon, d'expiration, ou de toute autre forme de perte d'une licence ou d'une autorisation ou de radiation d'une déclaration, les ressources utilisées dans le cadre de la licence, de l'autorisation ou de la déclaration sont automatiquement retirées. Il en est de même en cas d'interdiction d'exercer une activité de communications électroniques.

CHAPITRE II

DES FREQUENCES RADIOELECTRIQUES

SECTION I

DES DISPOSITIONS GENERALES ET DE LA GESTION DU SPECTRE

Article 178 : Gestion du spectre de fréquences radioélectriques

Le spectre des fréquences radioélectriques fait partie du domaine public de l'Etat.

L'Autorité de régulation assure, pour le compte de l'État, la gestion du spectre des fréquences radioélectriques.

Elle veille à ce que tous les utilisateurs, quelle que soit la catégorie considérée, soient incités ou amenés, en cas de nécessité, à optimiser les fréquences ou les bandes de fréquences qu'ils exploitent.

Elle gère le spectre des fréquences radioélectriques selon des modalités favorisant la souplesse tout en restant conformes aux traités et accords régionaux et internationaux ratifiés par la République du Bénin.

Un décret pris en Conseil des ministres fixe les conditions d'utilisation et de gestion des fréquences radioélectriques ainsi que les redevances et taxes s'y rapportant.

En application de la présente loi, et en cas de nécessité, il est procédé à des modifications des assignations de fréquences existantes.

Article 179 : Fréquences soumises à une autorisation préalable

L'Autorité de régulation fixe les cas dans lesquels l'utilisation des fréquences ou des bandes de fréquences est soumise à une autorisation préalable d'utilisation :

LégiBenin

- en ce qui concerne les fréquences ou les bandes de fréquences dont l'utilisation est soumise à une autorisation préalable, l'Autorité de régulation détermine :

  - les conditions d'obtention des autorisations d'utilisation des fréquences ;
  - les cas dans lesquels l'autorisation d'utilisation des fréquences ou des bandes de fréquences est subordonnée à l'obtention d'une licence ou d'une autorisation ou à la réalisation d'une déclaration ;
  - les conditions techniques d'utilisation des fréquences ou des bandes de fréquences.

- en ce qui concerne les fréquences ou les bandes de fréquences dont l'utilisation n'est pas soumise à l'obtention d'une autorisation préalable, l'Autorité de régulation précise les conditions techniques d'utilisation des fréquences ou des bandes de fréquences.

Article 180 : Frais, redevances et taxes

L'assignation et l'utilisation de fréquences radioélectriques peuvent être soumises au paiement de frais, des redevances et des taxes conformément à la réglementation en vigueur.

Article 181 : Règles générales de gestion du spectre de fréquences radioélectriques

Les directives générales relatives à la gestion du spectre des fréquences radioélectriques sont définies par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques.

Article 182 : Comité national de coordination du spectre des fréquences radioélectriques

La coordination nationale de l'utilisation du spectre est assurée par un Comité national de coordination du spectre des fréquences radioélectriques.

Le Comité national de coordination est un organe consultatif, constitué des représentants des principaux organismes de l'Etat en charge de la gestion du spectre ainsi que des principales parties non gouvernementales intéressées.

La composition, les attributions, l'organisation et le fonctionnement du Comité sont fixés par décret pris en Conseil des ministres.

Article 183 : Non thésaurisation et utilisation optimale des ressources en fréquences

En application du principe de non thésaurisation et d'utilisation optimale du spectre de fréquences radioélectriques, l'Autorité de régulation peut procéder au retrait de toute fréquence qui ne serait pas exploitée par un opérateur dans un délai de douze (12) mois suivant son assignation, sous réserve des fréquences qui lui sont nécessaires pour faire face à l'évolution prévisible de son activité dans les deux (02) années à venir.

Article 184 : Plan national des fréquences

La gestion du spectre des fréquences radioélectriques fait l'objet d'un plan national des fréquences établi par l'Autorité de régulation et approuvé par décret pris en Conseil des ministres sur proposition du ministère en charge des communications électroniques.

Le plan établi par l'Autorité de régulation est conforme au plan international des bandes de fréquences de l'Union Internationale des Télécommunications.

Le plan national d'attribution des bandes de fréquences radioélectriques contient :

Tech-Benin

- la répartition des bandes de fréquences radioélectriques entre les besoins exclusifs de la défense nationale et de la sécurité publique d'une part et les besoins communs d'autre part. Par besoins communs, sont visées les bandes de fréquences pouvant être utilisées à la fois pour des applications civiles et de la défense nationale ;

- la répartition des bandes de fréquences radioélectriques attribuées aux besoins civils sur les différentes utilisations, en respectant en particulier les besoins pour l'exploitation des réseaux de communications électroniques ouverts au public.

Article 185 : Attribution des fréquences radioélectriques spécifiques

Les bandes de fréquences radioélectriques attribuées pour les besoins de la défense nationale et de la sécurité publique sont exclusivement gérées par les ministres chargés de la défense nationale et de la sécurité publique. Elles ne peuvent être utilisées que pour ces besoins.

- **Article 186 :** Caducité des bandes de fréquences spécifiquement attribuées à la défense nationale et à la sécurité publique

Lorsqu'il n'existe pas de besoins du Gouvernement dans les bandes de fréquences spécifiquement attribuées à la défense nationale et à la sécurité publique ou lorsque ces besoins sont négligeables, lesdites fréquences sont attribuées à titre temporaire ou permanent pour des utilisations civiles, après renonciation provisoire ou définitive par le Gouvernement.

La renonciation est faite par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques et sur demande de l'Autorité de régulation.

Article 187 : Missions de l'Autorité de régulation

Conformément aux dispositions du Chapitre IV du Titre II du présent code, l'Autorité de régulation :

- tient à jour l'ensemble des documents relatifs à l'emploi des fréquences, notamment le fichier national des fréquences qui récapitule les assignations de fréquences. A cet effet, l'ensemble des administrations et autorités affectataires lui transmettent les données nécessaires, dans le respect des dispositions relatives à la protection du secret-défense ;
- coordonne les assignations de fréquences dans les bandes en partage et est informée des projets d'assignation de nouvelles fréquences dans les bandes exclusives avec dérogation sur lesquelles elle émet un avis ;
- procède à la notification des assignations nationales au fichier international des fréquences de l'Union Internationale des Télécommunications dont elle est, pour ce domaine, l'interlocuteur unique ;
- assure les fonctions de bureau centralisateur prévues par le Règlement des Radiocommunications de l'Union Internationale des Télécommunications ;

- est responsable de la coordination internationale des fréquences aux frontières et de celle des systèmes de télécommunications par satellite ;

- organise et coordonne le contrôle de l'utilisation des fréquences, sans préjudice des compétences de contrôles spécifiques exercés par les administrations et autorités affectataires.

Legi-Bénin

Elle est saisie par ces dernières ou par des tiers des cas de brouillage, qu'elle instruit et transmet son rapport d'instruction à l'administration ou à l'autorité affectataire concernée ;

- prévoit les mesures découlant de la loi sur l'organisation de la défense nationale et aide à leur mise en œuvre ;

- Conseille le ministre chargé des communications électroniques en cas de nécessité.

Article 188 : Conditions à respecter par les stations radioélectriques concernées

L'établissement et l'exploitation d'une installation ou d'une station radioélectrique allouée aux besoins civils en vue d'assurer soit l'émission, soit à la fois l'émission et la réception d'informations et de correspondances exigent :

- l'assignation d'une ou plusieurs fréquences radioélectriques par l'Autorité de régulation sauf pour les fréquences qui ne sont pas soumises à une autorisation d'utilisation préalable conformément aux dispositions de l'article 179 du présent code ;

- l'obtention d'une autorisation d'implantation, de transfert ou de modification des stations radioélectriques prévues à l'article 189 du présent code auprès de l'Autorité de régulation ;

- le respect des conditions liées à l'autorisation et notamment celles en matière d'exigences essentielles déterminées par l'Autorité de régulation ;

- l'exclusion des émissions des signaux radioélectriques parasites susceptibles de perturber d'autres services, réseaux, installations et stations radioélectriques.

Les stations radioélectriques d'émission ne doivent être la cause d'aucune gêne pour les postes récepteurs voisins.

Article 189 : Implantation, transfert et modification des stations radioélectriques

Afin d'assurer une utilisation optimale des sites disponibles permettant d'atteindre la meilleure compatibilité électromagnétique d'ensemble, les décisions d'implantation, de transfert ou de modification des stations radioélectriques, à l'exception de celles des entreprises exploitant des installations destinées exclusivement à la radiodiffusion ou à la télévision hertzienne, sont prises après avis conforme de l'Autorité de régulation.

L'accord de l'Autorité de régulation est obligatoire dans tous les autres cas d'utilisation civile et commune à l'exception des dérogations spécifiées dans un décret d'application.

Article 190 : Dispense d'autorisation

Sont dispensées des autorisations prévues à l'article 188 ci-dessus :

- les stations exclusivement composées d'appareils de faible puissance et de faible portée dont les catégories et les conditions techniques d'exploitation sont déterminées par voie réglementaire ;

- les stations temporairement installées en République du Bénin appartenant à des catégories déterminées par voie réglementaire.

Legibenin

Article 191 : Contrôle de l'Autorité de régulation

L'Autorité de régulation exerce un contrôle permanent sur les conditions techniques et d'exploitation des stations radioélectriques publiques et privées de toutes catégories.

A cet effet, ses représentants peuvent, chaque fois que les circonstances l'exigent et après avoir informé la Haute Autorité de l'Audiovisuel et de la Communication (HAAC) pour ce qui concerne les autorisations d'exercice délivrées par elle, pénétrer dans les stations émettrices.

Article 192 : Brouillages

En cas de brouillages causés par les stations radioélectriques d'émission, l'Autorité de régulation prescrit toute disposition technique pour y remédier.

Article 193 : Servitudes radioélectriques

L'Autorité de régulation est consultée sur tous les projets de servitudes radioélectriques dans les conditions prévues dans le présent code. Elle constitue, tient à jour et publie la documentation relative aux servitudes établies dans ce domaine au titre des différents ministères.

En liaison avec les services et organismes compétents, elle établit et publie les documents, les répertoires et les fichiers relatifs aux installations radioélectriques et aux zones de groupement des installations radioélectriques.

Article 194 : Règles et normes de bonne utilisation des systèmes radioélectriques

L'Autorité de régulation fixe les règles de compatibilité électromagnétique, d'ingénierie du spectre de fréquences radioélectriques et de normes propres à assurer une bonne utilisation des systèmes radioélectriques.

Article 195 : Relations de l'Autorité de régulation et des autorités affectataires

L'Autorité de régulation, à la demande des administrations et des autorités affectataires, dans le cadre de conventions conclues avec elles :

- assure tout ou partie de la gestion de leurs plans de fréquences et de leurs assignations ;
- instruit les demandes d'autorisation ;
- délivre les documents administratifs découlant de ces autorisations ;
- effectue les contrôles nécessaires.

Sa comptabilité permet de déterminer et de suivre le coût d'exécution de chaque convention.

SECTION II

DES SERVITUDES

SOUS-SECTION I

DES SERVITUDES DE PROTECTION DES CENTRES RADIOELECTRIQUES D'EMISSION ET DE RECEPTION CONTRE LES OBSTACLES

Legi-Bénin

Article 196 : Servitudes administratives pour protéger la propagation des ondes radioélectriques

Dans un but d'intérêt général, il peut être institué des servitudes administratives pour protéger la propagation des ondes radioélectriques contre l'occultation.

Article 197 : Conséquences des servitudes

Lorsque les servitudes entraînent la suppression ou la modification d'un immeuble, il est procédé, à défaut d'accord amiable, à l'expropriation pour cause d'utilité publique, conformément à la législation en vigueur.

SOUS-SECTION II

DES SERVITUDES DE PROTECTION DES CENTRES DE RECEPTION RADIOELECTRIQUES CONTRE DES PERTURBATIONS ELECTROMAGNETIQUES

Le Gabonais

Article 198 : Servitudes administratives en raison des perturbations électromagnétiques

Afin d'assurer le bon fonctionnement des réceptions radioélectriques effectuées dans tout centre exploité ou contrôlé dans un but d'intérêt général, il est institué des servitudes administratives en raison des perturbations électromagnétiques.

Article 199 : Prescriptions en vue de faire cesser les perturbations

Tout propriétaire ou tout usager d'une installation radioélectrique, même située hors des zones de servitudes, produisant ou propageant des perturbations gênant l'exploitation d'un centre de réception radioélectrique public ou privé, est tenu de se conformer aux dispositions qui lui sont prescrites, en vue de faire cesser lesdites perturbations. Il se prête notamment aux investigations demandées et réalise les modifications indiquées afin de maintenir les installations en bon état de fonctionnement.

Lorsque les propriétaires ou les usagers ne procèdent pas d'eux-mêmes aux modifications qui leur sont prescrites, il y est procédé d'office à leurs frais et risques.

SOUS-SECTION III

DES SERVITUDES DE PROTECTION DES CABLES ET LIGNES DE RESEAUX DE COMMUNICATIONS ELECTRONIQUES EN RAISON D'OBSTACLES OU D'EXECUTION DE TRAVAUX

Article 200 : Servitudes pour la protection des câbles et des lignes desdits réseaux

Afin d'assurer la conservation et le fonctionnement normal des réseaux de communications électroniques, il peut être institué des servitudes pour la protection des câbles et des lignes desdits réseaux.

Article 201 : Indemnisation

Les servitudes visées à l'article précédent donnent droit à indemnisation s'il en résulte un dommage. Le montant de l'indemnisation, à défaut de règlement à l'amiable, est fixé par la juridiction compétente.

Sous peine de forclusion, la demande d'indemnisation parvient au bénéficiaire des servitudes dans un délai de deux (02) ans à compter de la date de notification aux intéressés des sujétions dont ils sont l'objet.

CHAPITRE III

DE LA NUMEROTATION ET NOMS DE DOMAINES

SECTION I

DE LA GESTION DU PLAN NATIONAL DE NUMEROTATION

ET D'ADRESSAGE

LégiBenin

Article 202 : Compétences de l'Autorité de régulation

L'établissement du plan national de numérotation et d'adressage, la maîtrise de l'assignation de toutes les ressources nationales de numérotation et d'adressage ainsi que la gestion du plan national de numérotation et d'adressage sont de la compétence de l'Autorité de régulation.

L'Autorité de régulation peut imposer aux opérateurs la portabilité des numéros fixes et mobiles. Les modalités de mise en œuvre de la portabilité des numéros sont définies par l'Autorité de régulation.

Article 203 : Plan national de numérotation

L'Autorité de régulation veille à ce que les numéros, les adresses et les séries de numéros et d'adresses adéquats soient prévus, dans le plan national de numérotation, pour tous les services de communications électroniques accessibles au public.

Les principaux éléments définis à l'alinéa précédent du présent article sont publics et publiés sur le site internet de l'Autorité de régulation.

Toutefois, la capacité de numérotation destinée à des fins de défense nationale et de sécurité publique n'est pas rendue publique.

Article 204 : Procédure d'attribution

La procédure d'attribution de la capacité de numérotation et d'adressage se déroule conformément aux dispositions de l'article 7 du présent code. Il en est de même des principes de sa réservation et de son retrait éventuel.

Article 205 : Non thésaurisation et utilisation optimale des ressources en numérotation

En application du principe de non thésaurisation et d'utilisation optimale des ressources en numérotation, l'Autorité de régulation peut procéder au retrait de toute ressource en numérotation qui ne serait pas exploitée par un opérateur dans un délai de douze (12) mois suivant son assignation, sous réserve des ressources qui lui sont nécessaires pour faire face à l'évolution prévisible de son activité dans les douze (12) mois à venir

Article 206 : Attribution par l'Autorité de régulation

Les adresses, les numéros et les blocs de numéros ne peuvent devenir la propriété des demandeurs ou des utilisateurs finaux. Ils sont attribués par l'Autorité de régulation.

La durée de validité correspond à la durée d'exploitation du service ou de l'application.

Article 207 : Règles et procédures de gestion du plan national de numérotation et d'adressage

Un arrêté du ministre chargé des communications électroniques précise les procédures de gestion du plan national de numérotation et d'adressage. Il définit notamment les règles et les procédures relatives aux points ci-après :

- la réservation de capacité de numérotation et d'adressage ;
- l'attribution de capacité de numérotation et d'adressage ;
- la mise à disposition d'un opérateur tiers d'une capacité de numérotation et d'adressage ;
- le transfert de capacité de numérotation et d'adressage ;
- le montant et les modalités de paiement des frais, droits et redevances.

Article 208 : Frais, redevances et taxes

L'attribution et l'utilisation de ressources en numérotation peuvent être soumises au paiement de frais, des redevances et taxes conformément à la réglementation en vigueur.

Legibenin

SECTION II

DES NOMS DE DOMAINE

Article 209 : Compétence de l'Autorité de régulation

La maîtrise des noms de domaine, de l'assignation de toutes les ressources nationales d'adressage ainsi que la gestion du plan national d'adressage sont de la compétence de l'Autorité de régulation.

Article 210 : Rôle du Registre

L'attribution et la gestion des noms de domaine rattachés à chaque domaine de premier niveau du système d'adressage par domaines de l'internet correspondant aux codes pays du territoire national « .bj » ou d'une partie de celui-ci sont centralisées par un organisme unique dénommé « Registre ».

Le Registre établit chaque année un rapport d'activité qu'il soumet à l'Autorité de régulation.

Article 211: Règles de gestion des noms de domaine

Les noms de domaine sont attribués et gérés dans l'intérêt général selon des règles non discriminatoires et transparentes, garantissant le respect de la liberté de communication, de la liberté d'entreprendre et des droits de propriété intellectuelle.

Les noms de domaine sont attribués pour une durée limitée et renouvelable.

L'enregistrement des noms de domaine s'effectue sur la base des déclarations faites par le demandeur et sous sa responsabilité.

L'Autorité de régulation précise les règles de gestion des noms de domaine.

TITRE IV

DES EQUIPEMENTS

Article 212 : Agrément des équipements terminaux

Les équipements terminaux destinés à être connectés à un réseau de communications électroniques font l'objet d'un agrément de l'Autorité de régulation.

Article 213 : Agrément des équipements et installations radioélectriques

Aucun appareil radioélectrique servant à l'émission, à la réception ou à l'émission et la réception de signaux et de correspondances ne peut être fabriqué, importé ou commercialisé en vue de son utilisation en République du Bénin s'il n'a fait l'objet d'un agrément de l'Autorité de régulation. Cette disposition ne s'applique pas aux stations expérimentales destinées à des essais d'ordre technique ou pédagogique et à des études scientifiques relatives à la radioélectricité.

Un appareil agréé ne peut être modifié qu'avec l'accord de l'Autorité de régulation.

Les agents de l'Autorité de régulation dûment habilités peuvent procéder à toute vérification afin de s'assurer que les appareils détenus par les constructeurs, les importateurs, les commerçants, les utilisateurs sont agréés et conformes à la réglementation en vigueur.

Article 214 : Procédure d'agrément

L'Autorité de régulation détermine la procédure d'agrément des équipements et des laboratoires nationaux et internationaux ainsi que les conditions de reconnaissance des normes et spécifications techniques.

Article 215 : Valeur de l'agrément

L'agrément atteste que l'équipement qui en est l'objet respecte les exigences essentielles.

Il vaut autorisation de connexion à un réseau de communications électroniques.

Une fois attribué pour un modèle d'équipements terminaux, l'agrément est valable pour toute unité du modèle correspondant.

Article 216 : Demandes d'agréments

Les demandes d'agréments sont présentées à l'Autorité de régulation qui dispose d'un délai de soixante (60) jours à partir de la date du dépôt, attestée par un accusé de réception de la demande, pour faire connaître sa décision.

Article 217 : Redevance

L'agrément fait l'objet d'une décision motivée. Son octroi est subordonné au paiement d'une redevance au profit de l'Autorité de régulation, destinée à couvrir les coûts de la délivrance, de la gestion et de la surveillance de cet agrément.

Legi-Benin

Le montant de cette redevance est fixé par décret pris en Conseil des ministres sur proposition du ministère en charge des communications électroniques.

Article 218 : Refus d'agrément

L'agrément ne peut être refusé qu'en cas de non-conformité aux exigences essentielles et/ou aux normes et spécifications techniques reconnues en République du Bénin. Le refus d'agrément doit être motivé.

En cas de contestation, l'avis d'un laboratoire agréé est requis.

Article 219 : Interdictions

Les équipements terminaux soumis à l'agrément ne peuvent être fabriqués pour le marché intérieur, ni être importés pour la mise à la consommation ou détenus en vue de la vente, ni être distribués à titre gratuit ou onéreux, ni être connectés à un réseau ouvert au public ou faire l'objet de publicité que s'ils ont été soumis à cet agrément et demeurent en permanence conformes à celui-ci.

TITRE V

DU REGLEMENT DES DIFFERENDS

CHAPITRE I

DES COMPETENCES DE L'ARCEP

Article 220 : Parties autorisées à saisir l'Autorité de régulation

L'Autorité de régulation peut être saisie d'une demande de règlement de différend par :

- les opérateurs titulaires d'une licence ou d'une autorisation ou soumis au régime de la déclaration en République du Bénin ;
- les exploitants d'infrastructures alternatives ;
- les opérateurs non nationaux.

L'Autorité de régulation peut également être saisie d'une demande de règlement de différend par une autre autorité de régulation compétente dans un État membre de l'UEMOA ou de la CEDEAO, conformément aux dispositions de l'article 222 du présent code.

Article 221 : Différends relevant de la compétence de l'Autorité de régulation

1- L'Autorité de régulation peut être saisie d'un différend portant sur :

- les conditions techniques et financières de l'interconnexion et de l'accès prévus aux articles 63 et suivants du présent code, y compris le partage d'infrastructures et les formes particulières d'accès et d'interconnexion ;

- les conditions réciproques techniques et financières de mise à disposition de fibre noire et d'acheminement du trafic national et international ;

- les conditions techniques et financières du dégroupage de la boucle locale et de la sous-boucle locale prévu à l'article 73 du présent code ;

Legibenin

- les conditions techniques et financières de l'accès aux capacités sur les câbles sous-marins prévu à l'article 77 du présent code ;

- les conditions techniques et financières du partage d'infrastructure prévu à l'article 72 du présent code, y compris le partage d'infrastructures essentielles non réplicables prévu aux articles 82 et suivants du présent code ;

- les conditions techniques et financières de l'itinérance nationale et internationale prévue aux articles 74 et 75 du présent code ;

- les conditions techniques et financières de l'accès des opérateurs mobiles virtuels au réseau et aux infrastructures des opérateurs de radiocommunication prévu à l'article 76 du présent code ;

- les possibilités et les conditions techniques et financières de l'accès aux infrastructures alternatives, y compris l'utilisation partagée des infrastructures de génie civil, et notamment:

  ▪ les possibilités et les conditions techniques et financières de l'accès aux installations existantes situées sur, en dessous ou au-dessus du domaine public ;

  ▪ les possibilités et les conditions techniques et financières de l'accès aux installations existantes situées sur, en dessous ou au-dessus d'une propriété privée ;

  ▪ les possibilités et les conditions techniques et financières d'octroi, d'exercice ou de refus des servitudes et des droits d'occupation sur le domaine public ou des servitudes et droits de passage sur les propriétés privées prévus aux articles 86 et suivants du présent code ;

  ▪ l'exercice de droits exclusifs par un opérateur.

2- L'Autorité de régulation peut également être saisie d'un différend relatif à l'interprétation, l'exécution ou la violation :

- des dispositions légales ou réglementaires applicables dans le secteur des communications électroniques, y compris les stipulations des licences, autorisations, cahiers des charges ou encore conventions d'exploitations applicables ;

- des termes des catalogues d'accès ou d'interconnexion ;

- des conventions d'accès ou d'interconnexion, y compris celles relatives aux formes particulières d'accès et d'interconnexion telles que le dégroupage de la boucle locale et de la sous-boucle locale, l'accès aux capacités sur les câbles sous-marins, le partage d'infrastructures, le partage d'infrastructures essentielles non réplicables, l'itinérance nationale et internationale, l'accès des opérateurs mobiles virtuels au réseau et aux infrastructures des opérateurs de radiocommunication, l'accès aux infrastructures alternatives ou encore les conventions d'occupation du domaine public et de droit de passage et de servitude sur les propriétés privées ;

- du procès-verbal de conciliation mentionné à l'article 225 du présent code.

3- Toute clause contractuelle qui, directement ou indirectement, tend à écarter ou à restreindre la compétence territoriale et matérielle de l'Autorité de régulation est nulle et de nul effet.

Legi-Bénin

Article 222 : Différend avec un opérateur non national

L'Autorité de régulation peut être saisie d'un différend entre un opérateur national et un opérateur non national, par l'une ou l'autre des parties.

Le cas échéant, l'Autorité de régulation est tenue d'informer les autorités de régulation compétentes du ou des autres États membres de l'UEMOA ou de la CEDEAO, de coordonner ses efforts avec elles et de leur communiquer les informations nécessaires à la résolution du différend. L'Autorité de régulation assure la confidentialité des informations envoyées et reçues qui relèvent du secret des affaires.

En l'absence de réaction des autorités de régulation du ou des autres États membres de l'UEMOA ou de la CEDEAO ou de coordination entre ces autorités, l'Autorité de régulation saisit la Commission de l'UEMOA ou de la CEDEAO et adresse une copie de la saisine à l'autre partie et aux autorités de régulation compétentes des autres États membres de l'UEMOA ou de la CEDEAO.

Si, à l'issue d'un délai de douze (12) mois suivant la saisine de l'Autorité de régulation, aucune décision permettant la résolution du différend n'a été adoptée, la partie la plus diligente peut elle-même saisir la Commission de l'UEMOA ou de la CEDEAO. Dans ce cas, elle adresse une copie de la saisine à l'autre partie et aux autorités de régulation compétentes des autres Etats membres de l'UEMOA ou de la CEDEAO.

Article 223 : Saisine de l'Autorité de régulation par une autre Autorité de régulation

Lorsqu'elle est saisie ou informée par une autorité de régulation compétente d'un autre État membre de l'UEMOA ou de la CEDEAO dans le cadre d'un différend entre un opérateur national et un opérateur non national, l'Autorité de régulation doit coordonner ses efforts avec elle et lui communiquer les informations nécessaires à la résolution du différend. L'Autorité de régulation doit assurer la confidentialité des informations envoyées et reçues qui relèvent du secret des affaires.

En outre, lorsqu'elle est saisie d'une demande de règlement de différend par une autorité de régulation compétente d'un autre État membre de l'UEMOA ou de la CEDEAO conformément aux dispositions de l'article 220 du présent code, l'Autorité de régulation peut adopter une décision de règlement de différend à l'égard d'un ou plusieurs opérateurs nationaux conformément aux dispositions prévues aux articles 221 et suivants en ce qui concerne les différends entre opérateurs nationaux, qui s'appliquent mutatis mutandis.

CHAPITRE II

DES PROCEDURES DEVANT L'AUTORITE DE REGULATION

Article 224 : Types de procédures

Les parties peuvent décider de saisir l'Autorité de régulation de tout différend relevant de sa compétence à la demande de l'une ou l'autre des parties, l'Autorité de régulation peut ouvrir une procédure de conciliation dont l'objectif est de parvenir à une solution à l'amiable qui fera l'objet d'un procès-verbal de conciliation.

En cas d'échec de la procédure de conciliation, ou en cas de non respect par une partie des termes du procès-verbal de conciliation, l'une ou l'autre partie peut saisir l'Autorité de régulation d'une procédure de règlement de différend.

Tech Bénin

Article 225 : La procédure de conciliation

La procédure de conciliation s'achève :

- par l'élaboration d'un procès-verbal de conciliation signé sans réserve par toutes les parties et l'Autorité de régulation. Dans ce cas, le procès-verbal signé à force exécutoire et ne peut être remis en cause par les parties ;

- par l'échec de la conciliation dans un délai de soixante (60) jours suivant la saisine de l'Autorité de régulation si aucun procède-verbal de conciliation n'a été signé sans réserve par toutes les parties et l'Autorité de régulation.

Les règles et procédures applicables à la procédure de conciliation sont précisées par décret pris en Conseil des ministres.

Article 226 : Communication des documents et informations

Dans le cadre d'une procédure de règlement de différend, l'Autorité de régulation peut exiger des parties qu'elles fournissent toute information ou document utile à la résolution du différend.

Le cas échéant, l'Autorité de régulation peut mettre en demeure les parties concernées de lui fournir toute information ou document utile à la résolution du différend.

Article 227 : Expertises techniques, économiques et juridiques

L'Autorité de régulation peut procéder à des consultations ou faire appel à des expertises techniques, économiques ou juridiques. Elle veille dans ce cas au respect de la confidentialité de la procédure et des informations et documents communiqués par les parties.

Les frais engendrés par ces consultations et expertises peuvent être mis à la charge de la partie perdante, sauf si les circonstances particulières du différend justifient qu'ils soient mis à la charge d'une autre partie ou partagés entre les parties.

Article 228 : Délai de règlement des différends

La procédure de règlement de différend doit conduire à une décision de l'Autorité de régulation dans un délai de quatre-vingt dix (90) jours. Toutefois, ce délai peut être porté à six (06) mois lorsqu'il est nécessaire de procéder à des investigations et expertises complémentaires.

L'Autorité de régulation peut :

- mettre en demeure les parties de se conformer à toute disposition légale ou règlementaire applicable ou de respecter toute obligation à laquelle elles sont tenues ;

- prononcer des injonctions de faire ou de ne pas faire ;

- prononcer des mesures sous astreintes.

L'Autorité de régulation peut, à la demande de la partie qui la saisit, décider que sa décision produira effet à une date antérieure à sa saisine, sans toutefois que cette date puisse être antérieure à la date à laquelle la contestation a été formellement élevée par l'une des parties pour la première fois et, en tout état de cause, sans que cette date soit antérieure de plus de deux ans à sa saisine.

Legal Benin

Les règles et procédures applicables à la procédure de règlement de différend sont précisées par décret.

Article 229 : Mesures conservatoires

En cas d'atteinte grave et immédiate aux règles régissant le secteur des communications électroniques, l'Autorité de régulation peut, après avoir entendu les parties en cause, ordonner des mesures conservatoires en vue notamment d'assurer la continuité du fonctionnement des réseaux.

Ces mesures doivent rester strictement limitées à ce qui est nécessaire pour faire face à l'urgence.

Les règles et procédures applicables aux mesures conservatoires sont précisées par décret.

Article 230 : Principes applicables à la procédure

L'Autorité de régulation met en œuvre des procédures transparentes et non discriminatoires pour trancher les différends qui lui sont soumis.

Ainsi, l'Autorité de régulation doit :

- respecter le principe du contradictoire et des droits de la défense en mettant les parties à même de présenter leurs observations écrites ou orales. L'Autorité de régulation peut refuser la communication de pièces mettant en cause le secret des affaires. Ces pièces sont alors retirées du dossier ;

- procéder à des consultations techniques, économiques ou juridiques, ou avoir recours à des expertises respectant le secret de l'instruction du différend dans les conditions prévues par le règlement intérieur de l'Autorité de régulation. Les frais engendrés par ces consultations et expertises sont mis à la charge de la partie perdante, sauf si les circonstances particulières du différend justifient qu'ils soient mis à la charge d'une autre partie ou partagés entre les parties ;

- rendre des décisions dûment motivées, notamment en précisant les conditions équitables, d'ordre technique et financier dans lesquelles les obligations en cause doivent être mises en œuvre ;

- rendre publiques ses décisions, notamment sur son site internet, et les notifier aux parties dans les conditions prévues par son règlement intérieur sous réserve des informations, données et faits dont la diffusion est protégée ou restreinte par la loi ;

- communiquer, le cas échéant, ses décisions à la Commission de la CEDEAO et de l'UEMOA.

Les parties ont le droit de se faire assister ou représenter dans ces procédures par des avocats.

Article 231 : Avis de la Haute Autorité de l'Audiovisuel et de la Communication

Lorsque les faits à l'origine du différend sont susceptibles de restreindre de façon notable l'offre de services de communication audiovisuelle, l'Autorité de régulation recueille l'avis de la Haute Autorité de l'Audiovisuel et de la Communication (HAAC) qui se prononce dans un délai maximum de trente (30) jours.

Legibenin

CHAPITRE III

DU RECOURS CONTRE LES DECISIONS DE L'AUTORITE

DE REGULATION

Article 232 : Application des décisions et recours contre les décisions de l'Autorité de régulation

L'application des décisions de l'Autorité de régulation adoptées en application du présent Titre s'impose aux parties nonobstant tout recours.

Les décisions prises par l'Autorité de régulation dans le cadre du présent Titre peuvent faire l'objet d'un appel devant la chambre administrative de la Cour Suprême dans un délai de trente (30) jours.

Article 233 : Règles applicables aux recours

Le droit de recours contre toute décision de l'Autorité rendue en matière de règlement de différend s'exerce dans un délai de trente (30) jours à compter de la notification ou de la publication de la décision.

Ce délai est de dix (10) jours pour les mesures conservatoires.

Les recours exercés ne sont pas suspensifs. Toutefois, la chambre administrative de la Cour Suprême peut ordonner un sursis à exécution lorsque la décision en cause est susceptible d'entrainer des conséquences manifestement excessives ou irréversibles ou lorsqu'il est survenu, postérieurement à la décision, des faits nouveaux d'une gravité exceptionnelle.

La chambre administrative de la Cour suprême statue sur le recours en annulation ou en reformation contre les mesures conservatoires conformément aux procédures d'urgence qui sont applicables devant elle en matière administrative.

Les recours contre les décisions rendues sur la litispendance sont formés et jugés comme en matière d'exception d'incompétence.

TITRE VI

DES PLAINTES DES UTILISATEURS DE SERVICES DE COMMUNICATIONS ELECTRONIQUES

Article 234 : Compétence de l'Autorité de régulation en matière de plainte des utilisateurs

L'Autorité de régulation est compétente pour recevoir les plaintes des utilisateurs de services de communications électroniques et des associations réunissant les utilisateurs de services de communications électroniques.

Les associations réunissant les utilisateurs de services de communications électroniques ne peuvent intervenir que sur la base de mandats confiés par des utilisateurs de services de communications électroniques.

Léga-Bénin

Pour être recevables, les plaintes doivent porter sur la fourniture de services de communications électroniques, la violation par l'opérateur concerné des dispositions légales ou règlementaires en vigueur ou des obligations qui lui sont applicables y compris celles des articles 12 à 18 du présent code ou doivent porter sur le bien-fondé d'une clause jugée abusive ou anticoncurrentielle ou doivent porter sur les résultats d'études illustrant des abus dans les prestations de l'opérateur concerné.

Les utilisateurs ou les associations réunissant les utilisateurs de services de communications électroniques dûment mandatés par eux doivent avoir épuisé les moyens et voies de réclamations mis en place par l'opérateur concerné conformément aux dispositions de l'article 28 du présent code.

L'Autorité de régulation doit assurer la confidentialité des informations reçues.

Article 235 : Pouvoirs de l'Autorité de régulation

L'Autorité de régulation est compétente pour réaliser les enquêtes afférentes aux plaintes qu'elle reçoit en application du présent Titre.

Elle peut exiger des opérateurs concernés qu'ils s'expliquent par écrit et par oral et qu'ils lui fournissent toute information nécessaire à la résolution des plaintes reçues.

Le cas échéant, l'Autorité de régulation peut :

- mettre en demeure les opérateurs concernés de lui fournir les informations utiles à la résolution des plaintes reçues ;
- mettre en demeure les opérateurs concernés de se conformer à toute obligation légale ou règlementaire applicable ;
- mettre en demeure les opérateurs concernés de réparer tout préjudice subi par des utilisateurs de services de communications électroniques, qu'elle détermine ;
- imposer aux opérateurs concernés de mettre en œuvre les mesures correctives qui s'imposent, y compris des modifications des contrats conclus avec les utilisateurs.

LégiBénin

L'Autorité de régulation doit assurer la confidentialité des informations envoyées et reçues qui relèvent du secret des affaires.

Article 236 : Ouverture d'une procédure de sanction

Sur la base des informations recueillies dans le cadre du traitement des plaintes qu'elle reçoit, l'Autorité de régulation peut décider d'ouvrir une procédure de sanction conformément aux dispositions des articles 239 et 240 du présent code.

Article 237 : Modalités de saisine et procédure de traitement des plaintes

L'Autorité de régulation met en place les moyens matériels et humains nécessaires au traitement de ces plaintes.

Une décision de l'Autorité de régulation précise les modalités de saisine et la procédure de traitement des plaintes reçues en application du présent Titre.

Article 238 : Application des décisions de l'Autorité de régulation et recours

Les décisions rendues par l'Autorité de régulation en application du présent Titre s'imposent aux parties nonobstant tout recours.

Les décisions prises par l'Autorité de régulation dans le cadre du présent Titre peuvent faire l'objet d'un recours devant la chambre administrative de la Cour Suprême dans les conditions prévues à l'article 232 du présent code, qui est applicable *mutatis mutandis*.

TITRE VII

DES MESURES ET SANCTIONS

CHAPITRE I

DES MESURES ET SANCTIONS ADMINISTRATIVES

Article 239 : Sanctions administratives à l'égard des opérateurs titulaires de licence ou d'autorisation

Lorsqu'un opérateur titulaire d'une licence ou d'une autorisation ne respecte pas les obligations prescrites par les textes législatifs et réglementaires applicables y compris celles des articles 12 à 18 du présent code, les décisions de l'Autorité de régulation et les conditions fixées dans sa licence, son autorisation, son cahier des charges ou sa convention d'exploitation, l'Autorité de régulation le met en demeure de :

- réparer les préjudices causés ;
- se conformer à ses obligations.

Si l'opérateur titulaire de la licence ou de l'autorisation ne se conforme pas à la mise en demeure qui lui est adressée, l'Autorité de régulation prononce, à son encontre et à sa charge, par une décision motivée et selon la gravité du manquement, une pénalité dont le montant varie de zéro virgule un pour cent (0,1 %) à quatre pour cent (4 %) de son chiffre d'affaires consolidé du dernier exercice comptable.

En cas de récidive, le montant de la pénalité est porté au double.

Si la violation constatée et notifiée persiste, ou en cas de manquement grave ou répété d'un opérateur titulaire de licence ou d'autorisation à une obligation essentielle, l'Autorité de régulation prononce, par une décision motivée, la suspension partielle ou totale de la licence ou de l'autorisation, la réduction de la durée ou le retrait de la licence ou de l'autorisation.

Le retrait de la licence est prononcé à la demande motivée de l'Autorité de régulation par décret pris en Conseil des ministres, sur proposition motivée de l'Autorité de régulation.

L'opérateur peut, en outre, être interdit d'exercer une activité de communications électroniques en République du Bénin.

Article 240 : Sanctions administratives à l'égard des opérateurs soumis au régime de la déclaration

Lorsqu'un opérateur soumis au régime de la déclaration ne respecte pas les obligations prescrites par les textes législatifs et réglementaires y compris celles des articles 12 à 18 du

Legi-Bénin

présent code ou les décisions de l'Autorité de régulation, celle-ci le met en demeure de s'y conformer.

Si l'opérateur soumis au régime de la déclaration cité à l'alinéa précédent ne se conforme pas à la mise en demeure qui lui est adressée, l'Autorité de régulation prononce, à son encontre et à sa charge, par une décision motivée, une pénalité allant de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA.

En cas de récidive, le montant de la pénalité est porté au double du plafond.

Si la violation constatée et notifiée persiste, l'Autorité de régulation prononce, par une décision motivée, soit la suspension de la déclaration, soit son retrait définitif.

L'opérateur de services de communications électroniques peut, en outre, être interdit d'exercer une activité de communications électroniques en République du Bénin.

Article 241 : Procédure de sanction

Les règles applicables aux procédures de sanction décrites aux articles 239 et 240 du présent code sont précisées par décret pris en Conseil des ministres ainsi que dans le règlement intérieur adopté par l'Autorité de régulation.

Article 242 : Recours contre les décisions de l'Autorité de régulation

Les décisions rendues par l'Autorité de régulation en application des articles 239 et 240 du présent code peuvent faire l'objet d'un recours devant la chambre administrative de la Cour Suprême dans un délai de trente (30) jours suivant leur notification aux intéressés.

LegiBénin

CHAPITRE II

DES MESURES ET SANCTIONS PENALES

Article 243 : Saisine du procureur de la République

Le président de l'Autorité de régulation saisit le procureur de la République des faits qui sont susceptibles de recevoir une qualification pénale.

Article 244 : Secret des correspondances

Toute personne autorisée à participer à la mise en œuvre d'un service de communications électroniques ou radioélectriques et qui viole le secret d'une correspondance ou qui, sans l'autorisation de l'expéditeur ou du destinataire, divulgue, publie ou utilise le contenu de ladite correspondance est punie d'une peine d'emprisonnement de six (06) mois à deux (02) ans et d'une amende de dix millions (10 000 000) à cinquante millions (50 000 000) de francs CFA.

Article 245 : Prospection directe

Est puni d'un emprisonnement de six (06) mois à douze (12) mois et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement, sans préjudice des dommages et intérêts, quiconque fait de la prospection directe au moyen d'un automate d'appel, d'un télécopieur ou d'un courrier électronique utilisant, sous quelque forme que ce soit, les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir ladite prospection.

Article 246 : Utilisation frauduleuse d'un réseau de communications électroniques ouvert au public raccordé frauduleusement sur une ligne privée

Toute personne qui utilise frauduleusement, à des fins personnelles ou non, un réseau de communications électroniques ouvert au public ou se raccorde frauduleusement, par tout moyen, sur une ligne privée, est punie d'un emprisonnement d'un (01) an à cinq (05) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 247 : Utilisation de services obtenus frauduleusement

Toute personne qui utilise sciemment les services obtenus au moyen du délit visé à l'article précédent est punie d'un emprisonnement de six (06) mois à vingt-quatre (24) mois et d'une amende de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 248 : Dissimulation de trafic international entrant ou sortant

Est puni d'un emprisonnement de trois (03) ans à cinq (05) ans et d'une amende de cinq cent millions (500 000 000) à huit cent millions (800 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque dissimule, ou participe, sous une forme ou une autre, à la dissimulation de trafic international entrant ou sortant en trafic national.

Article 249 : Transmission de signaux ou correspondances

Toute personne qui transmet, sans accomplissement des formalités requises des signaux ou correspondances d'un lieu à un autre, soit à l'aide d'appareils de communications électroniques soit par tout autre moyen prévu par le présent code, est punie d'un emprisonnement de trois (03) mois à douze (12) mois et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Le tribunal peut, à la requête de l'Autorité de régulation, ordonner la confiscation des installations, des appareils ou moyens de transmission et/ou leur destruction aux frais du contrevenant.

Article 250 : Signaux ou appels de détresse faux ou trompeurs

Toute personne qui, sciemment, transmet ou met en circulation, par voie radioélectrique, des signaux ou appels de détresse faux ou trompeurs, est punie d'un emprisonnement de trois (03) mois à douze (12) mois et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 251 : Transmissions radioélectriques interdites

Toute personne qui effectue des transmissions radioélectriques en utilisant sciemment un indicatif d'appel de la série internationale attribué à une station de l'Etat ou à celle de ses démembrements ou à une station privée autorisée, est punie d'un emprisonnement de quatre vingt dix (90) jours à douze (12) mois et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 252 : Interruption volontaire des communications électroniques

Quiconque, par tout moyen, cause volontairement et sans droit l'interruption des communications électroniques, est puni d'un emprisonnement d'un (01) an à trois (03) ans et d'une amende de deux millions (2 000 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement sans préjudice des dommages et intérêts.

Article 253 : Interruption volontaire des communications électroniques par un opérateur

Document

Tout opérateur qui, volontairement, cause l'interruption des communications électroniques, est puni d'une amende de dix millions (10 000 000) à cinquante millions (50 000 000) de francs CFA, sans préjudice des peines prévues à l'article 252 du présent code applicables à ses administrateurs.

Article 254 : Interruption involontaire de communications électroniques

Toute personne qui, sans intention d'interrompre les communications électroniques, commet par maladresse ou inattention un acte ayant interrompu lesdites communications, est punie d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA.

Tout opérateur de réseau ou tout exploitant de services de communications électroniques ouverts au public qui, commet par maladresse ou inattention un acte ayant interrompu lesdites communications, est punie d'une amende de cinq millions (5 000 000) à vingt cinq millions (25 000 000) de francs CFA.

Article 255 : Rupture volontaire ou détériorations de câbles sous-marins

Quiconque, dans les eaux territoriales ou sur le plateau continental contigu au territoire de la République du Bénin, rompt volontairement un câble sous-marin, lui cause ou tente de lui causer des détériorations de nature à interrompre tout ou partie des communications électroniques, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cent millions (100 000 000) à cinq cent millions (500 000 000) de francs CFA sans préjudice des dommages et intérêts.

Article 256 : Rupture involontaire ou détérioration de câbles sous-marins sans déclaration

Quiconque, dans les zones maritimes visées à l'article précédent, rompt par maladresse, imprudence, négligence ou inobservation des règlements, un câble sous-marin ou lui cause des détériorations de nature à interrompre tout ou partie des communications électroniques et omet d'en faire la déclaration dans les douze (12) heures aux autorités compétentes, est puni d'un emprisonnement d'un (01) mois à douze (12) mois et d'une amende de cinquante millions (50 000 000) à deux cent cinquante millions (250 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Article 257 : Rupture involontaire ou détériorations de câbles sous-marins avec déclaration

Quiconque, dans les zones maritimes visées à l'article 255, rompt par maladresse, imprudence, négligence ou inobservation des règlements, un câble sous-marin ou lui cause une détérioration de nature à interrompre tout ou partie des communications électroniques et en fait la déclaration dans les douze (12) heures aux autorités compétentes, est puni d'une amende de vingt millions (20 000 000) à cinquante millions (50 000 000) de francs CFA.

Article 258 : Exercice d'une activité de communications électroniques sans licence

Est puni d'un emprisonnement d'un (01) an à cinq (05) ans et d'une amende de cinquante millions (50 000 000) à cent millions (100 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque établit ou fait établir un réseau ou fournit ou fait fournir un service sans la licence prévue à l'article 46 du présent code ou le maintien en violation d'une décision de suspension ou de retrait.

Article 259 : Utilisation de numéros ou de fréquences sans autorisation

Est puni d'un emprisonnement de six (06) mois à vingt quatre (24) mois et d'une amende de dix millions (10 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque utilise un bloc de numéros sans autorisation ou une fréquence

Légibenin

qui ne lui a pas été préalablement assignée par l'Autorité de régulation, sous réserve des assignations de fréquences réservées à la sécurité publique et à la défense nationale.

Article 260 : Exercice d'une activité de communications électroniques sans autorisation

Est puni d'un emprisonnement de six (06) mois à douze (12) mois et d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque établit ou fait établir un réseau ou fournit ou fait fournir un service sans l'autorisation prévue à l'article 52 du présent code ou le maintient en violation d'une décision de suspension ou de retrait de cette autorisation.

Article 261 : Exercice d'activités sans déclaration

Est puni d'un emprisonnement d'un (01) mois à six (06) mois et d'une amende de cent mille (100 000) à cinq cent mille (500 000) francs CFA ou de l'une de ces deux peines seulement, quiconque, sans avoir effectué la déclaration prévue à l'article 55 du présent code acceptée par l'Autorité de régulation, exerce une activité soumise à la réalisation d'une déclaration.

Article 262 : Non respect des dispositions relatives aux agréments et à l'information de l'Autorité de régulation

Est puni d'une amende de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA, quiconque :

- fabrique ou fait fabriquer pour le marché intérieur, importe ou détient en vue de la vente ou de la distribution à titre onéreux ou gratuit, met en vente des équipements terminaux sans l'obtention des agréments prévus aux articles 212 et 213 du présent code ou procède à leur connexion à un réseau de communications électroniques sans préjudice de l'application du code des douanes ;

- fait de la publicité en faveur de la vente des équipements terminaux n'ayant pas obtenu les agréments prévus aux articles 212 et 213 du présent code ;

- s'abstient d'informer l'Autorité de régulation des modifications apportées aux informations énoncées dans une demande d'autorisation ou dans une déclaration ;

- communique de fausses informations à l'Autorité de régulation dans une demande d'autorisation ou dans une déclaration.

Article 263 : Non respect des dispositions relatives aux servitudes

Les infractions aux dispositions relatives aux servitudes visées au Titre VI sont punies d'une amende de cent mille (100 000) francs CFA à un million (1 000 000) de francs CFA.

En cas de récidive, les peines prévues au présent article sont portées au double.

Article 264 : Confidentialité des communications, accès ouvert à internet, transparence et communication d'informations

Toute violation des dispositions prévues aux articles 12, 13, 17 et 18 du présent code, est punie d'une amende d'un montant de deux millions (2 000 000) de francs CFA.

Article 265 : Réparation des dommages causés

LegiBénin

Toute personne qui cause un dommage à une infrastructure de communications électroniques en supporte, outre les frais de réparation, les dommages-intérêts et les amendes prévus par le code pénal en la matière, sans préjudice des dommages et intérêts vis-à-vis des tiers.

Les préjudices subis par les personnes physiques ou morales consécutifs aux infractions visées aux articles 244 à 265 du présent code ouvrent droit à réparation.

LIVRE DEUXIEME

DES OUTILS ET ECRITS ELECTRONIQUES

TITRE I

DE L'ECRIT ELECTRONIQUE

Registre

Article 266 : Validité de l'écrit électronique

Sous réserve de dispositions légales particulières, les actes juridiques sous forme électronique ont la même valeur que les actes juridiques sous forme non-électronique.

Sous réserve de dispositions légales particulières, lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique sous réserve que puisse être dûment identifiée la personne qui l'a établi et que son intégrité soit garantie.

Lorsqu'un écrit est soumis à des conditions particulières de lisibilité ou de présentation, l'écrit électronique doit répondre à des exigences équivalentes.

La validité, les effets et la force exécutoire d'un acte juridique sous forme électronique ne peuvent être contestés en raison de la forme électronique de l'acte.

Nul ne peut être contraint de poser un acte juridique par voie électronique.

Article 267 : Exceptions à la validité des écrits électroniques

Certains actes ne peuvent prendre la forme d'écrits électroniques, notamment :

1- les actes sous seing privé relatifs aux sûretés personnelles ou réelles, de nature civile ou commerciale, sauf s'ils sont passés par une personne pour les besoins de sa profession ;

2- les actes sous seing privé relatifs au droit de la famille ou au droit des successions ;

3- tous autres actes pour lesquels la loi exige un écrit sous format papier ou sous tout autre format autre que le format électronique.

Article 268 : La preuve électronique

La preuve sous forme électronique a la même force probante et est admise au même titre que la preuve sous forme non-électronique, sous réserve que puisse être identifiée la personne dont

elle émane, et qu'elle soit établie et conservée dans des conditions qui en garantissent l'intégrité et la pérennité.

Article 269 : Conservation de contenus électroniques

Lorsqu'il existe une obligation légale de conserver des documents, enregistrements ou informations, leur conservation sous forme électronique satisfait aux exigences suivantes :

1- les documents, enregistrements, contenus ou informations électroniques conservés sont stockés de manière à être accessibles et consultables ultérieurement ;

2- les documents, enregistrements, contenus ou informations électroniques conservés demeurent au format auquel ils ont été générés, envoyés ou reçus, ou se trouvent dans un format garantissant l'intégrité et l'exactitude des informations générées, envoyées ou reçues ;

3- les documents, enregistrements, contenus ou informations électroniques sont conservés sous un format permettant d'identifier, le cas échéant, leur origine et leur destination ainsi que les date et heure auxquelles ils ont été générés, envoyés et reçus pour la première fois, ainsi que celles auxquelles ils ont été conservés pour la première fois.

Article 270 : Version électronique originale

Toute communication, message, document et autres contenus électroniques satisfont aux obligations légales de présenter ou conserver les informations qu'ils contiennent sous leur forme originale, dès lors que :

1- l'intégrité et l'exactitude des informations générées sont garanties et maintenues de manière fiable ;

2- il est possible de reproduire avec exactitude l'intégralité des informations telles qu'elles ont été générées pour la première fois.

L'exigence d'intégrité visée au présent article est satisfaite dès lors que les informations sont demeurées complètes et inchangées, à l'exception d'ajouts mineurs liés à l'acheminement ou au stockage de ces informations.

Article 271 : Copie électronique

La copie ou la reproduction d'un acte sous forme électronique a la même valeur et force probante que l'acte lui-même, sous réserve que la copie ou la reproduction ait conservé l'intégrité de l'acte électronique original.

La preuve de cette intégrité peut être apportée au moyen d'un certificat de conformité délivré par un prestataire de services de confiance répondant aux exigences prévues au Livre III du présent code.

Article 272 : Copie électronique certifiée conforme

Lorsque la loi oblige ou autorise une personne à fournir un document et que ce document n'existe que sous forme électronique, cette personne fournit une impression papier certifiée conforme du document sous forme électronique.

Cette certification est fournie par la personne qui est légalement tenue de conserver le document, ou par toute autre personne légalement qualifiée.

Article 273 : Exigences d'envoi en plusieurs exemplaires

LégiBénin

L'exigence d'envoi d'un écrit électronique en plusieurs exemplaires est réputée satisfaite dès lors que l'écrit peut être reproduit avec exactitude et dans son intégralité par le destinataire, sous sa forme non-électronique dans son intégralité et avec exactitude.

Article 274 : Remise d'un écrit

La remise d'un écrit sous forme électronique est effective lorsque le destinataire en a accusé réception par tout moyen, y compris par voie électronique.

Article 275 : Envoi électronique recommandé avec accusé de réception

Une communication électronique peut être faite par envoi recommandé avec accusé de réception. Dans ce cas, elle est acheminée par un tiers selon un procédé permettant de déterminer avec fiabilité et exactitude :

1- l'identité de l'expéditeur, du destinataire et du tiers qui achemine la communication électronique ;

2- la date et l'heure d'envoi du message ;

3- la date et l'heure de réception du message par le destinataire ;

4- le cas échéant, les données techniques relatives à l'acheminement du message de l'expéditeur au destinataire.

L'accusé de réception est adressé à l'expéditeur par voie électronique ou par tout autre moyen lui permettant de le conserver et de le reproduire.

Article 276 : Effet juridique d'un service d'envoi électronique recommandé qualifié

Les données envoyées et reçues au moyen d'un service d'envoi électronique recommandé qualifié bénéficient d'une présomption quant à l'intégrité des données, à l'envoi de ces données par l'expéditeur identifié, à leur réception par le destinataire identifié et quant à l'exactitude de la date et de l'heure d'envoi et de réception indiquées par le service d'envoi recommandé électronique qualifié.

Article 277 : Exigences applicables aux services d'envoi électronique recommandé qualifié

Les services d'envoi recommandé électronique qualifié doivent :

- être fournis par un ou plusieurs prestataires de services de confiance qualifié ;

- garantir l'identification de l'expéditeur avec un degré de confiance élevé ;

3- garantir l'identification du destinataire avec un degré de confiance élevé avant la fourniture des données ;

4- garantir que l'envoi et la réception des données sont sécurisés par une signature électronique avancée ou par un cachet électronique avancé d'un prestataire de services de confiance qualifié, de manière à exclure toute possibilité de modification des données ;

5- garantir que toute modification des données nécessaire à l'envoi ou à la réception de celles-ci soit clairement identifiable et signalée à l'expéditeur et au destinataire des données ;

Legal Benin

La date et l'heure d'envoi et de réception, ainsi que toute modification des données sont indiquées par un horodatage électronique qualifié.

Dans le cas où les données sont transférées entre deux prestataires de services de confiance qualifiés ou plus, les exigences prévues au présent article s'appliquent à tous les prestataires de services de confiance qualifiés.

TITRE II

DE L'IDENTIFICATION ELECTRONIQUE

Article 278 : Niveaux de garantie des schémas d'identification électronique

Un schéma d'identification électronique détermine les spécifications des niveaux de garantie faible, substantiel et/ou élevé des moyens d'identification électronique délivrés dans le cadre dudit schéma.

Ces niveaux de garantie satisfont aux critères suivants :

1- le niveau de garantie faible est celui fourni par un moyen d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne concernée. Il est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité de la personne concernée ;

2- le niveau de garantie substantiel est celui fourni par un moyen d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne concernée. Il est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité de la personne concernée ;

3- le niveau de garantie élevé est celui fourni par un moyen d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique à niveau de garantie substantiel. Il est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférentes, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité.

Au plus tard un (01) an après la publication du présent code, compte tenu des normes internationales applicables et sous réserve des dispositions du présent article, sont fixées par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques, les spécifications techniques, normes et procédures minimales sur la base desquelles les niveaux de garanties faible, substantiel et élevé sont assurés par les moyens d'identification électronique prévus au présent article.

Ces spécifications techniques, normes et procédures minimales sont fixées par référence à la qualité et à la fiabilité des éléments suivants :

1- la procédure visant à vérifier et prouver l'identité des personnes physiques ou morales demandant la délivrance de moyens d'identification électronique ;

2- la procédure de délivrance des moyens d'identification électronique demandés ;

Legi-Pen.com

3- le mécanisme d'authentification par lequel la personne concernée utilise/confirme son identité ;

4- l'entité délivrant les moyens d'identification électronique ;

5- tout autre organisme associé à la demande de délivrance de moyens d'identification électronique ;

6- les spécifications techniques et de sécurité des moyens d'identification électronique délivrés.

Article 279 : Eligibilité des schémas d'identification électronique

Un schéma d'identification électronique est éligible si toutes les conditions suivantes sont remplies :

1- les moyens d'identification relevant du schéma d'identification électronique peuvent être utilisés pour accéder au moins à un service fourni par une entité ou une administration publique exigeant une identification électronique ;

2- le schéma d'identification électronique et les moyens d'identification électronique délivrés répondent aux exigences d'au moins un des niveaux de garantie prévus à l'article 278 du présent code ;

3- les données d'identification et le moyen d'identification sont attribués à la personne concernée, conformément aux spécifications techniques, aux normes et aux procédures pour les niveaux de garantie prévues par le décret visé à l'article 278, alinéa 3.

Article 280 : Atteinte à la sécurité ou altération du schéma d'identification

En cas d'atteinte à la sécurité ou d'altération du schéma d'identification électronique affectant la fiabilité de l'authentification de ce schéma, l'autorité compétente suspend ou révoque sans délai cette authentification ou les éléments altérés.

Lorsqu'il a été remédié à l'atteinte à la sécurité ou à l'altération visée à l'alinéa premier, l'autorité compétente rétablit l'authentification.

Article 281 : Responsabilité

La personne offrant un moyen d'identification électronique est responsable des dommages causés intentionnellement ou par sa négligence à tout utilisateur du moyen d'identification électronique.

Article 282 : Interopérabilité

Les schémas d'identification électronique sont interopérables. A cette fin, un cadre d'interopérabilité est adopté par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques. Ce cadre d'interopérabilité :

1- est technologiquement neutre et n'opère pas de discrimination entre les solutions techniques particulières destinées à l'identification électronique ;

2- suit, dans toute la mesure du possible, les normes et recommandations internationales ;

3- facilite la mise en œuvre des principes du respect de la vie privée dès la conception ;

4- garantit que les données à caractère personnel sont traitées conformément aux dispositions de la loi, notamment les dispositions du Livre V du présent code.

Le cadre d'interopérabilité est notamment composé :

Legibenin

1- d'une référence aux exigences techniques minimales liées aux niveaux de garantie prévus à l'article 278, alinéa 3 ;

2- d'une table de correspondances entre les niveaux de garantie des schémas d'identification électronique notifiés et les niveaux de garantie prévus à l'article 278, alinéa 3 ;

3- d'une référence aux exigences techniques minimales en matière d'interopérabilité ;

4- d'une référence, dans le schéma d'identification électronique, à un ensemble minimal de données permettant d'identifier de manière univoque une personne physique ou morale ;

5- de règles de procédure encadrant l'interopérabilité ;

6- de dispositions encadrant le règlement des litiges ;

7- de normes opérationnelles communes de sécurité.

Article 283 : Entité délivrant les moyens d'identification électronique

Au plus tard un (01) an après l'entrée en vigueur du présent code, est désigné par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques la ou les autorités compétentes responsables de la délivrance des moyens d'identification électronique en République du Bénin.

TITRE III

DE LA SIGNATURE ELECTRONIQUE

LégiBénin

Article 284 : Dispositions générales

La signature électronique nécessaire à la validité d'un acte juridique, identifie celui qui l'appose et manifeste son consentement aux obligations qui en découlent.

Elle est admise dans les transactions électroniques.

La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire, lorsque ce procédé met en œuvre une signature électronique qualifiée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat qualifié répondant aux exigences prévues à l'article 287 du présent code.

Article 285 : Conditions d'admission de la signature électronique

Une signature électronique créée par un dispositif qualifié, répondant aux exigences prévues à l'article 287 du présent code, que le signataire peut garder sous son contrôle exclusif et qui repose sur un certificat électronique, est admise comme signature au même titre qu'une signature manuscrite.

Une signature électronique qui résulte d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle se rattache de telle sorte que toute modification ultérieure de l'acte soit détectable et qui satisfait en outre, aux exigences fixées par voie réglementaire, relatives aux certificats qualifiés de signature électronique, est une signature électronique qualifiée.

Sauf preuve contraire, un document écrit sous forme électronique est présumé avoir été signé par son auteur et son texte est présumé ne pas avoir été modifié si une signature électronique sécurisée y est apposée ou logiquement associée.

Article 286 : Exigences relatives à la signature électronique avancée

Une signature électronique avancée satisfait aux exigences suivantes :

1- être liée au signataire de manière univoque ;

2- permettre d'identifier le signataire ;

3- avoir été créée à l'aide de données de création de signature électronique que le signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;

4- être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable.

Article 287 : Certificats qualifiés de signature électronique

Les certificats qualifiés de signature électronique satisfont aux exigences fixées par voie réglementaire.

Les certificats qualifiés de signature électronique peuvent par ailleurs comprendre des attributs spécifiques supplémentaires non obligatoires. Ces attributs n'affectent pas l'interopérabilité et la reconnaissance des signatures électroniques qualifiées.

Si un certificat qualifié de signature électronique a été révoqué après sa première activation, il perd sa validité à compter du moment de sa révocation et ne peut en aucun cas recouvrer son statut antérieur.

Article 288 : Exigences applicables aux dispositifs de création de signatures électroniques qualifiés

Les dispositifs de création de signature électronique qualifiés respectent les exigences définies par décret pris en Conseil des ministres.

Article 289 : Certification des dispositifs de création de signature électronique qualifiés

La conformité des dispositifs de création de signature électronique qualifiés avec les exigences fixées par voie réglementaire est certifiée par l'organisme ou l'administration publique désigné par décret pris en Conseil des ministres sur proposition du ministre chargé des communications électroniques.

Cette certification est fondée sur l'un des éléments suivants :

1- un processus d'évaluation de la sécurité mis en œuvre par l'autorité compétente ou

2- un processus autre que le processus visé au point 1, à condition qu'il recoure à des niveaux de sécurité comparables. Ledit processus ne peut être utilisé qu'en l'absence des normes visées au point 1 ou lorsqu'un processus d'évaluation de la sécurité visé au point 1 est en cours.

Article 290 : Exigences applicables à la validation des signatures électroniques qualifiées

Le processus de validation d'une signature électronique qualifiée confirme la validité d'une signature électronique qualifiée à condition que :

1- le certificat sur lequel repose la signature ait été, au moment de la signature, un certificat qualifié de signature électronique conforme aux exigences prévues par voie réglementaire ;

Legi Benin

2- le certificat qualifié ait été délivré par un prestataire de services de confiance qualifié et était valide au moment de la signature ;

3- les données de validation de la signature correspondent aux données communiquées à la personne concernée ;

4- l'ensemble unique de données représentant le signataire dans le certificat soit correctement fourni à la personne concernée ;

5- l'utilisation d'un pseudonyme soit clairement indiquée, si un pseudonyme a été utilisé au moment de la signature ;

6- la signature électronique ait été créée par un dispositif de création de signature électronique qualifié ;

7- l'intégrité des données signées n'ait pas été compromise ;

8- la signature électronique respecte l'ensemble des exigences prévues au présent Titre.

Le système utilisé pour valider la signature électronique qualifiée fournit à l'utilisateur le résultat exact du processus de validation et permet à celui-ci de détecter tout problème de sécurité.

Article 291 : Services de validation qualifiés des signatures électroniques qualifiées

Un service de validation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui :

1- fournit une validation conformément aux exigences légales et réglementaires applicables à la validation des signatures électroniques qualifiées ;

2- permet aux utilisateurs de recevoir le résultat du processus de validation d'une manière automatisée, fiable, efficace et portant la signature électronique avancée ou le cachet électronique avancé du prestataire qui fournit le service de validation qualifié.

Article 292 : Services de conservation qualifiés des signatures électroniques qualifiées

Un service de conservation qualifié des signatures électroniques qualifiées ne peut être fourni que par un prestataire de services de confiance qualifié qui utilise des procédures et des technologies permettant d'étendre la fiabilité des signatures électroniques qualifiées au-delà de la période de validité technologique.

TITRE IV

DES CACHETS ELECTRONIQUES

Article 293 : Effets juridiques

L'effet juridique et la recevabilité d'un cachet électronique ne peuvent être refusés au seul motif que ce cachet se présente sous forme électronique ou qu'il ne satisfait pas aux exigences du cachet électronique qualifié.

Un cachet électronique qualifié bénéficie d'une présomption d'intégrité des données et d'exactitude de l'origine des données auxquelles il est lié.

Article 294 : Exigences du cachet électronique avancé

Legal Report

Un cachet électronique avancé satisfait aux exigences suivantes :

1- être lié au créateur du cachet de manière univoque ;

2- permettre d'identifier le créateur du cachet ;

3- avoir été créé à l'aide de données de création de cachet électronique que le créateur du cachet peut, avec un niveau de confiance élevé, utiliser sous son contrôle pour créer un cachet électronique ;

4- être lié aux données auxquelles il est associé de sorte que toute modification ultérieure des données soit détectable.

Article 295 : Cachets électroniques dans les services publics

Lorsqu'un cachet électronique avancé est exigé pour utiliser un service public en ligne, sont reconnus les cachets électroniques avancés, les cachets électroniques avancés qui reposent sur un certificat qualifié de cachet électronique et les cachets électroniques qualifiés au moins dans les formats ou utilisant les méthodes prévues par voie réglementaire visées à l'alinéa 3.

Lorsqu'un cachet électronique avancé reposant sur un certificat qualifié est exigé pour utiliser un service public en ligne, sont reconnus les cachets électroniques avancés qui reposent sur un certificat qualifié et les cachets électroniques qualifiés au moins dans les formats ou utilisant les méthodes prévues par voie réglementaire visées à l'alinéa 3.

Au plus tard un (01) an après la publication du présent code, sont définis par voie réglementaire, les formats de référence des cachets électroniques avancées ou les méthodes de référence lorsque d'autres formats sont utilisés.

L'usage des signatures et cachets électroniques dans le secteur public peut être soumis à des exigences supplémentaires, fixées par voie réglementaire. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Ces exigences ne peuvent pas constituer un obstacle aux services transfrontaliers pour les citoyens, en particulier entre Etats membres de la CEDEAO.

Article 296 : Certificats qualifiés de cachet électronique

Les certificats qualifiés de cachet électronique satisfont aux exigences fixées par voie réglementaire. Ils ne font l'objet d'aucune exigence obligatoire allant au-delà des exigences ainsi fixées.

Les certificats qualifiés de cachet électronique peuvent comprendre des attributs spécifiques supplémentaires non-obligatoires. Ces attributs n'affectent pas l'interopérabilité et la reconnaissance des cachets électroniques qualifiés.

Si un certificat qualifié de cachet électronique a été révoqué après la première activation, il perd sa validité à compter du moment de sa révocation et il ne peut en aucun cas recouvrer son statut antérieur.

Article 297 : Exigences applicables aux dispositifs de création et de validation de cachets électroniques qualifiés

Les dispositions de l'article 290 relatives aux exigences applicables aux dispositifs de création de cachets électroniques qualifiés s'appliquent mutatis mutandis aux exigences applicables aux dispositifs de création de cachet électronique qualifiés.

Les dispositions de l'article 289 relatives à la certification des dispositifs de création de signature électronique qualifiés s'appliquent mutatis mutandis à la certification des dispositifs de création de cachet électronique qualifié.

Article 298 : Validation et conservation des cachets électroniques qualifiés

Les dispositions des articles 288, 291 et 292 s'appliquent mutatis mutandis aux cachets électroniques qualifiés.

TITRE V

DES HORODATAGES, ARCHIVAGES ELECTRONIQUES

ET AUTHENTIFICATION DE SITES INTERNET

CHAPITRE I

DE L'HORODATAGE ELECTRONIQUE

Article 299 : Dispositions générales

L'effet juridique et la recevabilité d'un horodatage électronique ne peuvent être refusés comme preuve au seul motif que l'horodatage se présente sous forme électronique ou qu'il ne satisfait pas aux exigences de l'horodatage électronique qualifié.

Un horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données auxquelles se rapportent ces dates et heures.

Article 300 : Exigences applicables aux horodatages qualifiés

Tout horodatage électronique qualifié satisfait aux exigences suivantes :

1- lier la date et l'heure aux données de manière à exclure la possibilité d'une modification indétectable de ces données ;

2- être fondé sur une horloge exacte liée au temps universel coordonné ; et

3- être signé au moyen d'une signature électronique avancée ou cacheté au moyen d'un cachet électronique avancé du prestataire de services de confiance qualifié, ou par une méthode équivalente.

CHAPITRE II

DE L'ARCHIVAGE ELECTRONIQUE

Article 301: Dispositions générales

Sous réserve des dispositions légales particulières, la conservation de documents électroniques archivés satisfait aux exigences suivantes :

1- l'information que contient le document est accessible et consultable ultérieurement ;

2- le document est conservé sous la forme sous laquelle il a été créé, envoyé ou reçu, ou sous une forme dont on peut démontrer qu'elle n'est susceptible ni de modification, ni d'altération de son contenu, et que le document transmis et celui conservé sont strictement identiques ;

3- les informations qui permettent de déterminer l'origine et la destination du document, ainsi que les indications de date et d'heure de l'envoi ou de la réception doivent, le cas échéant, être conservées.

L'archivage électronique garantit l'authenticité et l'intégrité des documents, données et informations conservés par ce moyen.

Article 302 : Règles générales d'archivage électronique

L'archivage électronique consiste à mettre en place des actions, outils et méthodes afin de conserver des données, documents et informations en vue d'une utilisation ultérieure.

Les données concernées doivent être structurées, indexées et conservées sur des formats appropriés à la conservation et à la migration.

L'archivage doit garantir dans leur intégrité, la restitution des données conservées ou leur accessibilité dans un contexte technologique changeant.

Les règles de l'archivage électronique s'appliquent indifféremment aux documents numérisés et aux documents conçus initialement sur support électronique.

Article 303 : Modalités de mise en œuvre

Les modalités de mise en œuvre et le régime juridique applicable à l'archivage électronique sont précisés par décret pris en Conseil des ministres**.**

CHAPITRE III

DE L'AUTHENTIFICATION DE SITES INTERNET

Article 304 : Exigences applicables aux certificats qualifiés d'authentification de sites internet

Les certificats qualifiés d'authentification de sites internet contiennent obligatoirement :

1- une mention indiquant au moins sous une forme adaptée au traitement automatisé, que le certificat a été délivré comme certificat qualifié d'authentification de sites internet ;

2- un ensemble de données identifiant sans ambiguïté le prestataire de services de confiance qualifié qui a délivré les certificats qualifiés, comprenant au moins l'État, sa raison sociale et/ou sa dénomination sociale, ainsi que son adresse exacte ;

3- pour les personnes physiques, au moins le nom, le prénom et l'adresse de la personne à qui le certificat est délivré ;

4- pour les personnes morales, au moins la raison sociale, la dénomination sociale et l'adresse du siège de la personne morale à laquelle le certificat est délivré et, le cas échéant, son numéro d'immatriculation au Registre du Commerce et du Crédit Mobilier et/ou tout autre registre officiel ;

5- le(s) nom(s) de domaine exploité(s) par la personne physique ou morale à laquelle le certificat est délivré ;

Legal-Bénin

6- toute information utile sur le début et la fin de la période de validité du certificat ;

7- le code d'identité du certificat, qui est unique pour le prestataire de services de confiance qualifié ;

8- la signature électronique avancée ou le cachet électronique avancé du prestataire de services de confiance qualifié délivrant le certificat, ainsi que l'adresse où ils peuvent être vérifiés ;

9- l'emplacement des services de statut de validité des certificats qui peuvent être utilisés pour connaître le statut de validité du certificat qualifié.

LIVRE TROISIEME

DES PRESTATAIRES DE SERVICES DE CONFIANCE

TITRE I

DES OBLIGATIONS DES PRESTATAIRES DE SERVICES DE CONFIANCE

Léo-Bénin

Article 305 : Liberté d'établissement

Sous réserve des régimes d'autorisation établis par les autorités publiques compétentes pour des motifs d'ordre public, de protection de la santé publique, de sécurité publique ou de protection des consommateurs, l'accès à l'activité de prestataire de services de confiance et l'exercice de celle-ci ne peuvent être soumis à un régime d'autorisation préalable ni à aucune autre exigence ayant un effet équivalent.

Article 306 : Obligation de déclaration des prestataires de services de confiance

Tout prestataire de services de confiance qualifié établi en République du Bénin déclare les informations suivantes aux autorités compétentes et à l'organe de contrôle désigné par voie réglementaire, soit dans le mois suivant la promulgation et la publication du présent code, soit avant le début de son activité :

1- s'il s'agit d'une personne physique, ses nom et prénom et, s'il s'agit d'une personne morale, sa raison sociale et sa dénomination sociale ;

2- l'adresse géographique complète de l'endroit où il est établi, son adresse de courrier électronique, ainsi que son numéro de téléphone ;

3- s'il est assujetti aux formalités d'inscription des entreprises ou au Registre du Commerce et du Crédit Mobilier, le numéro de son inscription, le montant de son capital social et l'adresse de son siège social ;

4- s'il est assujetti à la TVA, le numéro d'identification fiscale correspondant ;

5- un justificatif de souscription à une police d'assurance couvrant de manière efficace les dommages liés à son activité.

L'autorité compétente délivre aux prestataires de services de confiance déclarés, un récépissé de déclaration dans les cinq (05) jours ouvrables suivant leur déclaration.

Article 307 : Obligation de protection des données à caractère personnel

Sans préjudice des dispositions du Livre V, un prestataire de services de confiance qui délivre des certificats au public ne peut recueillir des données personnelles que directement auprès de la personne concernée, avec le consentement explicite de celle-ci, et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat.

Les données qui leurs sont transmises, en particulier les données à caractère personnel, ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite préalable de la personne intéressée. Les prestataires ne peuvent détenir, consulter et exploiter ces données que dans la mesure strictement nécessaire à l'accomplissement de leurs services.

Lorsque le titulaire du certificat utilise un pseudonyme et lorsque les nécessités d'enquêtes de police ou d'enquêtes judiciaires l'exigent, le prestataire de services de confiance ayant délivré le certificat est tenu de communiquer à l'autorité compétente, à la police ou à l'autorité judiciaire, toute donnée et/ou information relative à l'identité du titulaire.

Article 308 : Exigences de sécurité applicables aux prestataires de services de confiance

Les prestataires de services de confiance qualifiés et non-qualifiés prennent les mesures techniques et organisationnelles nécessaires, afin de prévenir et gérer les risques liés à la sécurité des services de confiance qu'ils fournissent. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité soit proportionné au degré de risques. Des mesures sont notamment prises en vue de prévenir et limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

Article 309 : Obligation de notification à un organe de contrôle des prestataires de services de confiance

Les prestataires de services de confiance qualifiés et non-qualifiés notifient à l'organe de contrôle et le cas échéant aux autres organismes concernés, dans les meilleurs délais et au plus tard dans un délai de vingt quatre (24) heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence significative sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Article 310 : Autres obligations de notification des prestataires de services de confiance

Lorsque l'atteinte à la sécurité ou la perte d'intégrité visée à l'article 309 est susceptible de porter préjudice à un utilisateur du service de confiance, le prestataire de services de confiance lui notifie aussi l'atteinte à la sécurité ou la perte d'intégrité dans les meilleurs délais.

Lorsque l'atteinte à la sécurité ou la perte d'intégrité concerne un Etat étranger, l'organe de contrôle qui en a reçu la notification peut en informer les autorités compétentes et/ou les organes de contrôle de cet Etat. L'organe de contrôle en informe par ailleurs le public ou exige du prestataire de services de confiance qu'il informe le public, dès lors que l'organe de contrôle constate qu'il est dans l'intérêt du public d'être alerté de l'atteinte à la sécurité ou de la perte d'intégrité.

Article 311 : Exigences applicables aux prestataires de services de confiance qualifiés

Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie par des moyens appropriés l'identité et le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié. Ces informations sont vérifiées par le prestataire de services de confiance qualifié ou par un tiers, notamment :

Projet Béta

1- par la présence physique de la personne physique concernée ou du représentant autorisé de la personne morale ;

2- au moyen d'un certificat de signature électronique qualifié ou de cachet électronique qualifié ; ou

3- à l'aide d'autres méthodes d'identification reconnues en République du Bénin qui fournissent une garantie équivalente en termes de fiabilité, à la présence physique de la personne physique concernée ou du représentant autorisé de la personne morale. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.

Un prestataire de services de confiance qualifié doit :

1- informer l'organe de contrôle de toute modification dans la fourniture de ses services de confiance qualifiés et de son intention éventuelle de cesser ses activités ;

2- démontrer qu'il dispose des moyens techniques fiables en vue de fournir les services de confiance qualifié en toute sécurité ;

3- assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;

4- veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;

5- prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de services de confiance génère des données afférentes à la création de signature ou de cachet électronique, garantir la confidentialité au cours du processus de génération de ces données ;

6- disposer des ressources financières suffisantes pour mener convenablement son activité ;

7- souscrire une police d'assurance garantissant les dommages susceptibles d'être causés dans l'exercice de cette activité ;

8- employer du personnel et sous-traitants disposant de l'expertise, de l'expérience et des qualifications nécessaires en matière de sécurité des réseaux et systèmes d'informations et de protection des données à caractère personnel, et appliquant des procédures administratives et de gestion correspondant aux normes nationales et internationales ;

9- informer les utilisateurs de services de confiance qualifiés, de manière claire, exhaustive et avant toute relation contractuelle, sur les conditions précises d'utilisation du service, y compris les limites à son utilisation, les procédures de réclamation et de règlement des litiges. Cette information peut être transmise par voie électronique, et doit faire l'objet d'un écrit en langue française et être aisément compréhensible. Des éléments pertinents de cette information doivent également, sur demande, être mis à la disposition de tiers qui se prévalent du certificat ;

10- utiliser des systèmes et équipements fiables, protégés contre les risques de modifications et assurant la sécurité technique des processus pris en charge ;

11- utiliser des systèmes fiables de stockage des données qui lui sont communiquées, sous une forme vérifiable de sorte que :

- les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée ;
- seules des personnes autorisées puissent introduire des données et modifier les données conservées ;

Le Bénin

- l'authenticité des données puisse être vérifiée ;

12- prendre les mesures appropriées contre la falsification et le vol de données ;

13- enregistrer, conserver et maintenir accessibles pour une durée appropriée, y compris après la cessation des activités du prestataire de services de confiance qualifié, toutes les informations pertinentes concernant les données envoyées et reçues par le prestataire de services de confiance qualifié, notamment à des fins probatoires et de continuité du service ;

14- disposer d'un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service ;

15- assurer le traitement licite des données à caractère personnel conformément aux dispositions du présent code ;

16- le cas échéant, établir et tenir à jour une base de données des certificats octroyés ;

17- s'assurer que les certificats ne sont disponibles au public que dans les cas où le titulaire du certificat a donné son consentement ;

18- s'assurer que toute modification technique mettant en péril les exigences de sécurité soit apparente.

Lorsqu'un prestataire de services de confiance qualifié décide de révoquer un certificat, il enregistre cette révocation dans sa base de données de certificats et publie le statut de révocation du certificat dans les vingt-quatre (24) heures suivant la réception de la demande. Cette révocation devient effective dès sa publication.

Les prestataires de services de confiance qualifiés fournissent aux utilisateurs les informations pertinentes sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée, fiable, gratuite et efficace.

Article 312 : Certificats qualifiés délivrés par des prestataires étrangers

Un certificat qualifié délivré au public par un prestataire de services de confiance qui est établi dans un Etat membre de la CEDEAO, a la même valeur et est assimilé aux certificats qualifiés délivrés par un prestataire de services de confiance établi en République du Bénin.

Les certificats qualifiés délivrés au public par un prestataire de services de confiance établi dans un Etat non membre de la CEDEAO ont la même valeur et sont assimilés aux certificats délivrés par un prestataire de services de confiance établi en République du Bénin si :

1- le prestataire de services de confiance remplit les conditions du présent code, après vérification par les autorités compétentes ;

2- le certificat ou le prestataire de services de confiance est reconnu en application d'un accord, traité ou tout autre texte national ou international pertinent conclu entre la République du Bénin et un ou plusieurs pays ou organisations internationales.

Article 313 : Révocation des certificats qualifiés

A la demande du titulaire du certificat préalablement identifié, le prestataire de services de confiance révoque immédiatement le certificat.

Le prestataire de services de confiance révoque également un certificat lorsque :

Legal Benin

1- le prestataire de services de confiance cesse ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de services de confiance garantissant un niveau de qualité et de sécurité équivalent ;

2- il existe des raisons sérieuses de penser que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus valides ou que la confidentialité des données afférentes à la signature ait été violée ou risque de l'être ;

3- le prestataire de services de confiance est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est titulaire.

Le prestataire de services de confiance prend les mesures nécessaires afin de répondre à tout moment et sans délai à une demande de révocation.

Sauf en cas de décès, le prestataire de services de confiance notifie la révocation du certificat au titulaire, dans un délai de trente (30) jours avant l'expiration du certificat. La décision de révocation doit être motivée.

La révocation d'un certificat est définitive. Elle est opposable aux tiers à compter de la date de désinscription du prestataire de services de confiance, de la liste de confiance visée à l'article 323 du présent code.

Article 314 : Responsabilité des prestataires de services de confiance

Sans préjudice des dispositions de l'alinéa 3, les prestataires de services de confiance sont responsables des dommages causés intentionnellement, par négligence ou par maladresse à toute personne physique ou morale en raison d'un manquement aux obligations prévues aux dispositions du présent code.

Il incombe à la personne physique ou morale qui invoque les dommages visés à l'alinéa premier d'apporter la preuve que le prestataire de services de confiance non-qualifié a agi intentionnellement ou par négligence. Un prestataire de services de confiance qualifié est présumé avoir agi intentionnellement ou par négligence, à moins qu'il n'apporte la preuve que les dommages visés à l'alinéa 1er ont été causés sans intention ni négligence de sa part.

Lorsque les prestataires de services de confiance informent préalablement leurs utilisateurs des limites qui existent à l'utilisation des services qu'ils fournissent et que ces limites peuvent être reconnues par des tiers, les prestataires de services de confiance ne peuvent être tenus responsables des dommages découlant de l'utilisation des services au-delà des limites ainsi définies.

Article 315 : Cessation des activités des prestataires de services de confiance qualifiés

Le prestataire de services de confiance qui délivre des certificats qualifiés informe l'autorité compétente et l'organe de contrôle dans un délai raisonnable, de son intention de cesser ses activités ou de tout fait qui pourrait conduire à la cessation de ses activités.

Dans ce cas, il s'assure de la reprise de ses activités par un autre prestataire de services de confiance garantissant un niveau de qualité et de sécurité au moins équivalent. En l'absence de repreneur, le prestataire révoque, sous réserve d'un préavis de deux (2) mois, les certificats octroyés à ses titulaires.

Le prestataire de services de confiance qui arrête ses activités pour des raisons indépendantes de sa volonté ou en cas de faillite, en informe immédiatement l'autorité compétente. Il procède, le cas échéant, à la révocation des certificats délivrés.

Legi-Bénin

Article 316 : Responsabilité des titulaires de certificats

Dès la création des données relatives à la signature ou au cachet électronique, le titulaire du certificat devient responsable de la confidentialité de ces données.

En cas de doute ou de risque de violation de la confidentialité des données relatives à la signature ou au cachet électronique, ou en cas de défaut de conformité par rapport aux informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat.

Lorsqu'un certificat est arrivé à échéance ou a été révoqué, le titulaire ne peut, après l'expiration du certificat ou après sa révocation, utiliser les données relatives à la signature pour signer ou faire certifier ces données par un autre prestataire de services de confiance.

TITRE II

DU CONTROLE DES PRESTATAIRES DE SERVICES DE CONFIANCE

Article 317 : Création et missions de l'organe de contrôle

Il est créé un organe de contrôle des prestataires des services de confiance rattaché au ministère en charge des communications électroniques.

Un arrêté du ministre chargé des communications électroniques fixe l'organisation et le fonctionnement dudit organe.

Cet organe est notamment chargé de :

1- contrôler les prestataires de services de confiance qualifiés établis en République du Bénin afin de s'assurer, par des contrôles a priori et a posteriori, que ces prestataires et les services de confiance qualifiés qu'ils fournissent satisfont aux exigences prévues au présent code ;

2- contrôler a posteriori les prestataires de services de confiance non-qualifiés établis en République du Bénin, pour lesquels il a été rapporté des manquements présumés ou avérés aux dispositions du présent code.

Dans le cadre de ses prérogatives de contrôle, l'organe de contrôle a notamment la possibilité de :

1- analyser les rapports d'évaluation de conformité des prestataires de services de confiance ;

2- informer les cas échéant, les autres organes de contrôle et le public de toutes atteintes à la sécurité ou de pertes d'intégrité ;

3- procéder, notamment via un organisme d'évaluation de conformité, à des audits et des évaluations de conformité des prestataires de services de confiance qualifiés ;

4- accorder le statut "qualifié" aux prestataires de services de confiance et aux services qu'ils fournissent et, de retirer ce statut conformément aux dispositions du présent code ;

5- informer les autorités compétentes de ses décisions d'accorder ou de retirer le statut « qualifié » ;

Legi Bénin

6- vérifier l'existence et la bonne application des dispositions relatives aux plans d'arrêt d'activité lorsque le prestataire de services de confiance qualifié cesse ses activités, y compris la façon dont les informations restent accessibles ;

7- exiger que les prestataires de services de confiance corrigent tout manquement aux obligations prévues au présent code.

Les prestataires de services de confiance qualifiés font l'objet, au moins tous les vingt-quatre (24) mois, d'un audit effectué à leurs frais par un organisme d'évaluation de la conformité. L'objet de cet audit est de confirmer que les prestataires de services de confiance qualifiés et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées par le présent code.

Dans un délai de trois (03) jours ouvrables suivant sa réception, les prestataires de services de confiance qualifiés transmettent le rapport d'évaluation de conformité à l'organe de contrôle.

Article 319 : Audit et évaluation ponctuels des prestataires de services de confiance

Sans préjudice des dispositions de l'article 318, l'organe de contrôle peut à tout moment, soumettre les prestataires de services de confiance qualifiés à un audit ou demander à un organisme d'évaluation de la conformité de procéder à une évaluation de la conformité des prestataires de services de confiance qualifiés, aux frais de ces derniers, afin de s'assurer que les prestataires et les services de confiance qualifiés qu'ils fournissent remplissent les exigences fixées au code.

Les contrôles inopinés de conformité par l'organe de contrôle ne peuvent être abusifs et doivent être justifiés au regard de la situation du prestataire de services de confiance et des éléments le concernant dont il dispose.

Article 320 : Obligation de correction des manquements des prestataires de services de confiance

Lorsque l'organe de contrôle exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues au présent code et que le prestataire n'agit pas en conséquence, et le cas échéant après expiration d'un délai raisonnable fixé par l'organe de contrôle, ce dernier a la possibilité, en tenant compte notamment de l'ampleur, de la durée et des conséquences de ce manquement, de saisir la juridiction compétente, notamment afin de :

1- faire cesser la délivrance de certificats qualifiés par le prestataire de services de confiance ;

2- obliger le prestataire de services de confiance à informer immédiatement les titulaires des certificats qualifiés qu'il a délivrés, de leur non conformité aux dispositions du présent code.

Article 321 : Retrait du statut de "qualifié" du prestataire ou du service de confiance

Lorsque l'organe de contrôle exige du prestataire de services de confiance qualifié qu'il corrige un manquement aux exigences prévues au présent code et que le prestataire n'agit pas en conséquence après expiration d'un délai raisonnable fixé par l'organe de contrôle, ce dernier a la possibilité, en tenant compte de l'ampleur, de la durée et des conséquences du manquement, de retirer le statut "qualifié" au prestataire ou au service de confiance concerné, et informe l'autorité compétente aux fins de la mise à jour des listes de confiance visées à l'article 323. L'organe de contrôle informe par ailleurs le prestataire de services de confiance qualifié du retrait de son statut "qualifié" ou du retrait du statut "qualifié" du service de confiance concerné.

Article 322 : Fourniture de services de confiance qualifiés

Léa1 Benin

Lorsque des prestataires de services de confiance non qualifiés souhaitent offrir des services de confiance qualifiés, ils soumettent à l'organe de contrôle une demande accompagnée d'un rapport d'évaluation de conformité délivré par un organisme d'évaluation de la conformité.

L'organe de contrôle vérifie notamment que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences du présent code. Si l'organe de contrôle conclut que le prestataire de services de confiance et les services de confiance qu'il fournit respectent les exigences du présent code, il accorde le statut "qualifié" au prestataire de services de confiance et aux services de confiance qu'il fournit, et informe l'autorité compétente, aux fins de la mise à jour des listes de confiance visées à l'article 323, au plus tard dans un délai de quatre-vingt-dix (90) jours suivant le jour de la demande.

Si la vérification n'est pas terminée dans le délai de quatre-vingt-dix (90) jours à compter du jour de la demande, l'organe de contrôle en informe le prestataire de services de confiance en précisant les raisons du retard et le délai nécessaire pour terminer la vérification.

Les prestataires de services de confiance qualifiés peuvent commencer à fournir le service de confiance qualifié une fois que le statut "qualifié" est indiqué sur les listes de confiance.

Article 323 : Publication et mise à jour des listes de confiance

L'autorité compétente tient à jour et publie des listes de confiance comprenant les informations relatives aux prestataires de services de confiance qualifiés, ainsi que les informations relatives aux services de confiance qualifiés qu'ils fournissent.

L'autorité compétente établit, tient à jour et publie de façon sécurisée et sous une forme adaptée au traitement automatisé, les listes de confiance visées à l'alinéa 1 relatives aux signatures électroniques et cachets électroniques.

L'autorité compétente met à la disposition du public, par l'intermédiaire d'un canal sécurisé, les informations visées à l'alinéa 1 sous une forme portant une signature électronique ou un cachet électronique adaptée au traitement automatisé.

Legal Benin

TITRE III

DES SANCTIONS ET PUBLICATION

Article 324 : Usurpation de la qualité de prestataire de services de confiance

Est puni d'une peine de trois (03) mois à six (06) mois de prison et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de francs CFA, ou d'une de ces peines seulement, quiconque aura usurpé la qualité de prestataire de services de confiance.

Les peines prévues à l'alinéa 1er sont portées au double en cas d'usurpation de la qualité de prestataire de services de confiance qualifié.

Article 325 : Publication de jugement définitif

En condamnant du chef d'infraction visé à l'article 324, la juridiction compétente peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'elle détermine, aux frais de la personne condamnée.

LIVRE QUATRIEME

DU COMMERCE ELECTRONIQUE

TITRE PREMIER

DES GENERALITES SUR LE COMMERCE ELECTRONIQUE

Article 326 : Champ d'application

Les dispositions du présent Livre s'appliquent à toute commande, contrat ou transaction conclus en ligne ou par voie électronique en vue de la fourniture de biens ou services, ainsi qu'à toute activité de commerce électronique exercée sur le territoire de la République du Bénin ou à destination des utilisateurs établis sur le territoire de la République du Bénin.

Une activité de commerce électronique ou une offre de biens ou services est considérée comme à destination des utilisateurs établis sur le territoire de la République du Bénin, si elle inclue un signe distinctif ou caractéristique de la République du Bénin, de ses ressortissants ou de ses résidents.

Par ailleurs, en fonction du contenu des messages publicitaires et offres proposées, de la langue utilisée, de la monnaie utilisée, du nom de domaine utilisé, il est considéré comme à destination des utilisateurs établis sur le territoire de la République du Bénin.

Sans préjudice des dispositions librement convenues entre les parties à un contrat électronique, les dispositions du présent Livre sont applicables dès lors que ce contrat est conclu entre un professionnel et un consommateur.

Les contrats conclus entre professionnels peuvent déroger aux dispositions du présent Livre, pour autant que ce choix n'ait pas pour objet ou pour effet de :

1- déroger aux dispositions d'ordre public béninois ;

2- priver un consommateur de la protection que lui assurent les dispositions impératives de la loi ;

3- déroger aux dispositions impératives régissant les transactions ou activités soumises à un régime particulier, dont notamment :

- en matière immobilière à l'exception des contrats de location immobilière ;
- en matière d'assurance ;
- en matière de droit de la famille et des successions ;
- en matière de sûretés et garanties fournies par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale ;
- toutes autres matières pour lesquelles la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique.

Legibenin

Sont exclues du champ d'application du présent Livre :

- les activités de jeux d'argent, sous forme de paris, de loterie ou autres ;

- les activités de représentation et d'assistance en justice ;

- les activités exercées par les notaires.

Article 327 : Restrictions extraordinaires

Des mesures restreignant, au cas par cas, le libre exercice des activités encadrées par les dispositions du présent Livre peuvent être prises par toute autorité gouvernementale, administrative ou judiciaire, lorsqu'il est porté atteinte ou qu'il existe un risque sérieux et grave d'atteinte au maintien de l'ordre ou de la sécurité publique, à la protection des personnes, à la protection des mineurs, à la santé publique ou à la préservation des intérêts de la défense nationale.

Article 328 : Obligation générale d'information

Toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs béninois, est tenue d'assurer à ceux à qui est destinée la fourniture des biens ou services proposés, un accès facile, direct et permanent, le cas échéant à partir de la page d'accueil du site, aux informations suivantes :

1- s'il s'agit d'une personne physique, ses nom et prénom et, s'il s'agit d'une personne morale, sa raison sociale et sa dénomination sociale ;

2- l'adresse géographique complète de l'endroit où elle est établie, son adresse de courrier électronique, ainsi que son numéro de téléphone ;

3- si elle est assujettie aux formalités d'inscription au Registre du Commerce et du Crédit Mobilier, le numéro de son inscription, le montant de son capital social et l'adresse de son siège social ;

4- si elle est assujettie à la taxe sur la valeur ajoutée, le numéro d'identification fiscale correspondant ;

5- si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci ainsi que la référence de l'autorisation ;

- si elle exerce une profession réglementée :

- le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite ;
- son titre professionnel et le nom de l'Etat qui l'a octroyé ;
- la référence aux règles professionnelles applicables auxquelles elle est soumise et le moyen d'y accéder.

Toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire béninois ou proposant un ou plusieurs biens ou services en ligne doit, même en l'absence d'offre de contrat et dès lors qu'elle mentionne un prix, indiquer celui-ci de manière claire et non ambigüe, notamment si les taxes et frais de livraison sont inclus.

Article 329 : Responsabilité contractuelle

Legi-Benin

Toute personne physique ou morale exerçant une activité soumise aux dispositions du présent Livre ou partie à un contrat encadré par les dispositions du présent Livre, est responsable de plein droit de la bonne exécution des obligations résultant des conventions conclues, que ces obligations soient à exécuter par elle-même ou par des tiers, sans préjudice de son droit de recours contre ceux-ci.

Toutefois, elle peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit à l'autre partie ou à un tiers, soit à un cas de force majeure.

TITRE II

DE LA PUBLICITE PAR VOIE ELECTRONIQUE

CHAPITRE I

DES DISPOSITIONS GENERALES

Legi-Reth

Article 330 : Identification des publicités par voie électronique

Toute publicité, sous quelque forme que ce soit, accessible par un service de communications électroniques ouvert au public ou un service en ligne, doit pouvoir être clairement identifiée comme telle, dès sa réception. Elle rend clairement identifiable son expéditeur, ainsi que la personne physique ou morale pour le compte de laquelle elle est réalisée.

La publicité peut notamment être identifiée comme telle en raison de son titre, de sa présentation ou de son objet. A défaut, elle comporte la mention “Publicité” de manière claire, lisible, apparente et non équivoque, le cas échéant dans l'objet ou dans le corps du message qui la véhicule.

Article 331 : Identification des offres et jeux promotionnels

Les offres promotionnelles proposant des réductions de prix, offres conjointes, primes ou cadeaux de quelque nature qu'ils soient, dès lors qu'elles sont adressées ou accessibles par voie de communications électroniques ouverte au public ou via un service en ligne, doivent être identifiables comme telles, dès réception par l'utilisateur ou dès que ce dernier y a accès, et les conditions pour en bénéficier doivent être aisément accessibles et présentées de manière claire, précise et non équivoque.

De même, les concours ou jeux promotionnels doivent être clairement identifiables comme tels, dès leur réception par l'utilisateur ou dès que ce dernier y a accès, et leurs conditions de participation doivent être aisément accessibles et présentées de manière claire, précise et non équivoque.

Le cas échéant, les offres, concours et jeux promotionnels doivent être identifiables dans l'objet ou dans le corps du message qui les véhicule.

CHAPITRE II

DES CONDITIONS DE LA PROSPECTION DIRECTE

Article 332 : Interdiction de la prospection directe

Est interdite la prospection directe au moyen de systèmes automatisés de communications électroniques, de réseaux, services et/ou terminaux de communications électroniques, télécopieurs, courriers électroniques ou SMS utilisant les données à caractère personnel d'un utilisateur qui n'a pas préalablement exprimé son consentement à recevoir des prospections directes par ces moyens.

Pour l'application du présent article, les appels et messages ayant pour objet d'inciter l'utilisateur à appeler un numéro surtaxé ou à envoyer un message textuel surtaxé relèvent de la prospection directe.

Pour les besoins du présent article, on entend par consentement toute manifestation de volonté libre, spécifique et informée par laquelle une personne accepte que des données à caractère personnel la concernant soient utilisées à fin de prospection directe. L'absence de réponse ne peut pas être considérée comme un consentement.

La charge de la preuve du consentement du destinataire de la prospection directe incombe à la personne physique ou morale à l'origine de la prospection.

Article 333 : Exception à l'interdiction de la prospection directe

La prospection directe est autorisée, sans le consentement préalable du destinataire personne physique, si l'ensemble des conditions suivantes sont remplies :

1- les coordonnées du destinataire ont été recueillies auprès de lui en toute connaissance de cause, et dans le respect des dispositions du Livre V du présent code, à l'occasion d'une vente ou d'une prestation de services ;

2- la prospection directe concerne exclusivement des produits ou services analogues proposés par le même fournisseur ;

3- le destinataire se voit offrir, de manière simple, expresse et dénuée d'ambiguïté, la possibilité de s'opposer sans frais, à l'utilisation de ses coordonnées au moment où elles sont recueillies et chaque fois qu'un message de prospection lui est adressé, au cas où il n'aurait pas préalablement refusé une telle exploitation.

La prospection directe est autorisée, sans le consentement préalable du destinataire personne morale si les coordonnées électroniques utilisées à cette fin sont impersonnelles.

Article 334 : Droit d'opposition aux prospections directes

Toute personne peut notifier directement à un fournisseur de biens ou services en ligne, sans justification et sans frais, sa volonté de ne plus recevoir de prospections directes.

Dans ce cas le fournisseur est tenu de :

1- délivrer, sans délai, un accusé de réception par tout moyen, y compris par voie électronique, confirmant à cette personne l'enregistrement de sa demande ;

2- prendre, dans un délai raisonnable, les mesures nécessaires pour respecter la volonté de cette personne ;

3- tenir à jour la liste des personnes qui ont exprimé leur volonté de ne plus recevoir de prospections directes de sa part.

Legibenin

Article 335 : Prospection directe aux personnes vulnérables

Lorsque la prospection directe est destinée aux enfants, aux personnes âgées, aux personnes malades ou vulnérables, ou à toute personne qui ne serait pas en mesure de comprendre pleinement les informations qui lui sont présentées, les exceptions prévues au présent Livre doivent être interprétées plus strictement.

Article 336 : Obligation d'information

Dans tous les cas, il est interdit d'émettre, à des fins de prospection directe, des messages au moyen de systèmes automatisés de communications électroniques, de réseaux, services et/ou terminaux de communications électroniques, télécopieurs, courriers électroniques ou SMS, sans indiquer les moyens et les coordonnées valables auxquelles le destinataire peut utilement transmettre une demande tendant à obtenir sans frais, que ces communications cessent.

Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise, notamment en :

- utilisant l'adresse électronique ou l'identité d'un tiers ;

2- falsifiant ou masquant toute information permettant d'identifier l'origine du message ou son chemin de transmission ;

3- mentionnant un objet sans rapport avec les biens ou services proposés ;

4- encourageant le destinataire des messages à visiter des sites internet de tiers.

L'Autorité de contrôle prévue au Livre V veille, pour ce qui concerne la prospection directe utilisant les coordonnées d'un utilisateur personne physique, au respect des dispositions du présent Titre en utilisant les compétences qui lui sont reconnues au Livre V. A cette fin, elle peut notamment recevoir, par tous moyens, les plaintes concernant les manquements aux dispositions du présent article.

Article 337 : Sanctions

Toute personne effectuant une prospection directe non autorisée au sens des articles 332 à 334 du présent Titre ou ne respectant pas l'obligation d'information prévue à l'article 336 est puni d'une peine allant de trente (30) jours à six (06) mois d'emprisonnement et d'une amende de cinquante mille (50 000) à cinq cent mille (500 000) francs CFA.

Lorsque ces manquements concernent la prospection directe destinée à des enfants, des personnes âgées, des personnes malades ou vulnérables, ou à toute personne qui ne serait pas en mesure de comprendre pleinement les informations qui lui sont présentées, les peines prévues à l'alinéa précédent sont doublées.

TITRE III

DE LA CONCLUSION DE CONTRATS PAR VOIE ELECTRONIQUE

CHAPITRE I

Legi-Benin

DE L'OBLIGATION D'INFORMATION PREALABLE

Article 338 : Informations sur les modalités de conclusion du contrat

Sous peine de nullité, tout fournisseur de biens ou services en ligne doit, avant la conclusion de tout contrat en ligne, assurer et maintenir un accès facile, direct et permanent sur support durable, aux conditions contractuelles ainsi qu'à toutes informations relatives à la conclusion du contrat. La mise à disposition des conditions contractuelles doit permettre leur reproduction et leur conservation par les parties.

Ces informations doivent être présentées de façon claire, lisible et non-équivoque et comprennent notamment :

1- les différentes étapes à suivre par l'utilisateur pour conclure le contrat en ligne ;

2- les langues proposées pour la conclusion du contrat ;

3- les dispositions relatives à la protection des données à caractère personnel ;

4- les moyens techniques appropriés permettant à l'utilisateur d'identifier les erreurs commises dans la saisie des données et de les corriger avant la conclusion du contrat ;

5- le mode de confirmation de l'acceptation de l'offre ;

6- les conséquences de l'absence de confirmation des informations communiquées par l'utilisateur ;

7- les informations relatives aux restrictions, limitations et/ou aux conditions liées à la conclusion du contrat, telles que l'accord obligatoire d'un parent ou d'un tuteur, le cas échéant ;

8- les conditions de conclusion du contrat ;

9- les conditions de résiliation du contrat pour les contrats à durée indéterminée ou d'une durée supérieure à un (01) an ;

10- la durée minimale du contrat pour les contrats portant sur la fourniture de produits ou services périodiquement ou à long terme ;

- les conditions de livraison et frais de livraison ;

12- la date à laquelle le fournisseur s'engage à livrer les biens ou à fournir les services ;

13- les conséquences d'une inexécution ou d'une mauvaise exécution des obligations du fournisseur ;

14- les modalités prévues par le fournisseur pour le traitement des réclamations ;

15- le numéro de téléphone, ainsi que l'adresse électronique et postale du fournisseur en vue d'éventuelles réclamations ;

16- le cas échéant, les informations relatives aux procédures extrajudiciaires de réclamation et de recours auxquelles le fournisseur est soumis, et les conditions d'accès à celles-ci ;

17- l'existence ou l'absence d'un droit de rétractation et ses conditions d'exercice ;

Legibenin

- les modalités de retour, d'échange et de remboursement des biens ;

19- le cas échéant, les informations relatives à l'assistance après-vente, le service après-vente et les conditions y afférentes ;

20- le cas échéant, les informations relatives à la nature et l'étendue des garanties commerciales ;

21- les informations relatives aux garanties légales de conformité, garanties légales des vices cachés et garanties légales d'éviction ;

22- les modalités d'archivage du contrat ainsi que les conditions d'accès au contrat archivé ;

23- les modalités de consultation des certificats de signature et de cachets électroniques ;

24- les règles professionnelles et commerciales ou codes de conduite auxquels l'auteur de l'offre entend se soumettre, ainsi que les moyens de les consulter.

Lorsqu'il est en mesure de le faire, le fournisseur de biens ou services en ligne

met en place un service permettant aux utilisateurs de dialoguer directement avec lui.

Article 339 : Informations sur les caractéristiques des biens ou services

Sous peine de nullité, tout fournisseur de biens ou services en ligne doit, avant la conclusion de tout contrat, assurer et maintenir un accès facile, direct et permanent sur support durable, à toutes informations portant sur les caractéristiques des biens ou services proposés.

Ces informations sont présentées de façon claires, lisibles, non équivoques et comprennent notamment :

1- les caractéristiques essentielles du bien ou du service ;

2- les caractéristiques techniques du bien ou du service ;

3- les informations relatives au mode d'emploi et conditions d'utilisation du bien ou du service ;

4- les mises en garde relatives à la sécurité et à la santé liées au bien ou au service ;

5- s'il s'agit d'un contenu numérique, ses fonctionnalités, et s'il y a lieu, les mesures de protections applicables et toute interopérabilité du contenu numérique avec certains matériels ou logiciels dont le fournisseur a ou devrait raisonnablement avoir connaissance.

Pour les contenus numériques téléchargés, l'offre doit indiquer :

1- les caractéristiques du système d'exploitation ou de l'équipement nécessaire pour utiliser de manière efficace le contenu téléchargé ;

2- le temps approximatif et le coût de téléchargement éventuel du contenu, et le cas échéant, les modalités et conditions du contrat de licence ;

3- les caractéristiques techniques pour reprendre le téléchargement d'un contenu interrompu ;

- le cas échéant, le nom du directeur de publication.

Legi-Benin

Tout bien ou service dangereux pour la santé humaine ou animale ou pour l'environnement est accompagné d'un manuel d'instructions en français, comprenant des avertissements clairs et facilement visibles, afin de permettre une utilisation dans des conditions de sécurité maximales.

Article 340 : Informations sur le prix des biens et services

Sous peine de nullité, tout fournisseur de biens ou services en ligne doit, avant la conclusion de tout contrat, assurer et maintenir un accès facile, direct et permanent sur support durable, à toutes informations portant sur le prix des biens et services proposés.

Ces informations sont présentées de façon claires, lisibles et non équivoques, et comprennent notamment :

1- le prix du bien ou du service toutes taxes comprises et s'il inclut ou non les frais de livraison ;

2- le cas échéant, les frais de livraison ainsi que les assurances proposées ;

3- la durée de validité de l'offre ;

4- les modalités, conditions et méthodes de paiement ;

5- le cas échéant, les facilités de paiement proposées ;

6- la monnaie de facturation du bien ou du service ;

7- le cas échéant, les coûts d'utilisation des services en ligne ;

8- le cas échéant, les coûts d'utilisation des moyens de communications électroniques lorsqu'ils sont calculés sur une autre base que les tarifs en vigueur, notamment s'agissant des numéros surtaxés ;

9- le cas échéant, l'existence d'autres coûts normalement dus par l'utilisateur, non-perçus par le fournisseur et/ou non imposés par celui-ci.

Toutes les informations faisant référence à des coûts prévus au présent article indiquent la monnaie utilisée.

Sans préjudice des conditions de validité mentionnées dans l'offre, l'auteur reste engagé par elle tant qu'elle est accessible par l'utilisateur.

Article 341: Charge de la preuve

La charge de la preuve de l'existence d'une information préalable, d'une confirmation des informations communiquées, du respect des délais et du consentement de l'utilisateur incombe au fournisseur de biens ou services en ligne.

Article 342 : Conditions d'échange d'informations

Les informations prévues au présent Chapitre, doivent être fournies par tout moyen adapté au service utilisé et accessible à tout stade de la conclusion du contrat, dans le respect des principes qui régissent la protection des personnes frappées d'incapacité juridique, notamment les mineurs et les majeurs incapables.

Les informations demandées en vue de la conclusion d'un contrat en ligne ou celles qui sont adressées ou échangées au cours de son exécution peuvent être transmises par voie électronique si le destinataire a accepté l'usage de ce procédé.

CHAPITRE II

Legi-Bénin

DE L'APRES CONCLUSION DU CONTRAT

SECTION 1

DES CONDITIONS DE VALIDITE

Article 343 : Conditions de validité du contrat conclu par voie électronique

Pour qu'un contrat soit valablement conclu par voie électronique, l'utilisateur doit avoir eu la possibilité, par des moyens techniques appropriés, efficaces et aisément accessibles, de vérifier le détail de sa commande et d'y apporter les corrections nécessaires, avant de confirmer son acceptation. Le détail de la commande doit permettre un consentement éclairé et avisé.

L'utilisateur doit avoir eu la possibilité d'interrompre la passation de la commande à tout moment, avant de confirmer son acceptation.

Article 344 : Accusé de réception

Après la passation d'une commande, l'auteur de l'offre doit accuser réception de l'acceptation de l'utilisateur qui passe la commande, sans retard injustifié et par tout moyen, y compris par voie électronique.

L'accusé de réception doit être accompagné de la facture ou du justificatif de paiement présentant un récapitulatif détaillé de la commande ainsi que la date et l'heure de celle-ci.

La commande, l'acceptation de l'offre, la confirmation, l'accusé de réception et la facture ou le justificatif de paiement, sont considérés comme reçus, lorsque les parties auxquelles ils sont adressés peuvent y avoir accès.

Article 345 : Indisponibilité du bien ou du service

Lorsqu'un bien ou service offert est indisponible, le fournisseur de biens ou services doit en informer l'acquéreur sans délai et au moins vingt-quatre (24) heures avant la date de livraison prévue au contrat. Le cas échéant, le fournisseur de biens ou services rembourse à l'acquéreur, l'intégralité des sommes perçues.

Article 346 : Conservation

Tout contrat conclu par voie électronique doit être conservé pour une durée de dix (10) ans à compter de la livraison du bien ou de la fourniture du service.

SECTION II

DU DROIT DE RETRACTATION

Article 347 : Principe général

Les dispositions de la présente section relative au droit de rétractation ne s'appliquent qu'aux contrats conclus entre professionnel et consommateur. Ces dispositions s'appliquent sans préjudices d'éventuelles dispositions conventionnelles plus favorables pour le consommateur.

Legi-Benin

Article 348 : Délai de rétractation

Le consommateur dispose d'un délai de quinze (15) jours ouvrables pour exercer son droit de rétractation. Ce droit s'exerce par le consommateur, sans justifications et sans frais, autres que les éventuels coûts directs de renvoi du bien au professionnel, le cas échéant.

Si les informations prévues aux articles 338 à 340 du présent code sont communiquées au consommateur avant la conclusion du contrat, le délai d'exercice du droit de rétractation commence à courir :

- à compter du lendemain de la date à laquelle le consommateur prend possession du bien, s'agissant des contrats portant sur la fourniture de biens ;

- à compter du lendemain du jour de la passation de la commande, s'agissant des contrats portant sur la fourniture de services.

Si le professionnel manque à son obligation d'information préalable prévue aux articles 338 à 340 du présent code, le délai de rétractation est porté à quatre-vingt-dix (90) jours :

- à compter du lendemain de la date à laquelle le consommateur prend possession du bien, s'agissant des contrats portant sur la fourniture de biens ;

- à compter du lendemain du jour de la passation de la commande, s'agissant des contrats portant sur la fourniture de services.

Le consommateur notifie au professionnel sa décision d'exercer son droit de rétractation, par courrier postal ou électronique, avec accusé de réception, dans le délai de quatorze (14) jours ouvrables prévus à l'alinéa 1 ci-dessus.

Article 349 : Exercice du droit de rétractation

L'exercice du droit de rétractation par le consommateur suppose qu'il ait eu la possibilité de raisonnablement essayer le bien commandé, en vue de s'assurer de sa conformité. Cette disposition ne s'applique pas aux services dont l'exécution est effectuée en une fois.

Article 350 : Conditions d'exercice du droit de rétractation

En cas d'exercice du droit de rétractation, le consommateur doit, sans délai, cesser l'utilisation du bien ou du service fourni et renvoyer, à ses frais, le bien au professionnel, pour les contrats portant sur la fourniture de biens.

En cas d'exercice du droit de rétractation, le consommateur est tenu de renvoyer le bien au professionnel dans le délai de quatorze (14) jours ouvrables, prévu à l'article 348 ci-dessus.

Le professionnel peut s'opposer à la réception du bien retourné et au remboursement du consommateur en raison de la dépréciation du bien, seulement si cette dépréciation résulte de manipulations par le consommateur autres que celles strictement nécessaires à vérifier sa conformité ou dépassant manifestement l'usage fait à titre de test ou d'essai.

Article 351 : Droits et obligations du professionnel

En cas d'exercice du droit de rétractation, le professionnel est tenu de rembourser, sans délai, toutes sommes reçues du consommateur en paiement de sa commande ou liées à celle-ci.

Ce remboursement intervient dans un délai maximum de trente (30) jours ouvrables, à compter de la date de réception par le professionnel du bien retourné, pour les contrats portant sur la fourniture de biens, et à compter de la date de notification de la rétractation, pour les contrats portant sur la fourniture de services.

Legi-Bénin

Si le remboursement ne s'opère pas dans le délai prévu à l'alinéa 2, les sommes dues au consommateur sont de plein droit majorées au taux d'intérêt légal, à compter du lendemain de l'expiration du délai.

Article 352 : Remboursement des frais de livraison

Les frais de livraisons sont remboursés au consommateur, si le droit de rétractation est exercé en raison :

- d'un dépassement du délai de livraison par le professionnel ;

- d'un manquement du professionnel à l'une quelconque de ses obligations contractuelles ou de celles prévues au titre du présent Livre.

Si le droit de rétractation est exercé pour des raisons autres que celles prévues à l'alinéa premier ci-dessus, le professionnel n'est pas tenu de rembourser les frais de livraison au consommateur.

Article 353 : Remboursement de la commande

Le remboursement de la commande, du professionnel au consommateur, s'effectue sans frais pour le consommateur, dans les mêmes conditions et par les mêmes moyens de paiement que ceux utilisés pour le paiement de sa commande, sauf accord express du consommateur et pour autant que ce remboursement ne lui occasionne pas de frais supplémentaires.

Article 354 : Perte du droit de rétractation dans le cadre de la fourniture de services

Le consommateur perd son droit de rétractation, dans le cadre de contrats portant sur la fourniture de services lorsque le service a été fourni dans sa totalité.

Si le consommateur souhaite que la fourniture du service commence avant la fin du délai de rétractation, le professionnel recueille son accord préalable exprès sur support durable.

En cas d'exercice du droit de rétractation après le commencement de la fourniture du service, le consommateur est tenu au paiement de la partie du prix déterminée proportionnellement au service effectivement fourni, entre le jour du début de la fourniture du service et le jour de sa notification d'exercice du droit de rétractation.

Article 355 : Perte du droit de rétractation dans le cadre de la fourniture de biens

Le consommateur perd son droit de rétractation dans le cadre de contrats portant sur la fourniture de biens lorsqu'il s'agit de :

1- biens confectionnés sur mesures ou suivant les spécifications du consommateur ou personnalisés par ce dernier ;

2- denrées alimentaires, boissons, et autres biens consommables susceptibles de se périmer rapidement ;

3- biens qui, de par leur nature ne peuvent être réexpédiés au risque de se détériorer ;

4- biens scellés pour des raisons d'hygiène ou de protection de la santé, et descellés par le consommateur après la livraison ;

5- contenus numériques audio ou vidéo descellés ou téléchargés ;

6- journaux, périodiques ou magazines, sans préjudice du droit du consommateur de résilier les contrats d'abonnement à ces publications ;

- biens acquis dans le cadre d'enchères publiques.

Le Gi Bénin

Article 356 : Résolution ou résiliation de contrat

Sous réserve d'accord express entre les parties, le professionnel exécute la commande dans un délai maximum de trente (30) jours ouvrables, à compter du lendemain de la conclusion du contrat.

En cas de manquement contractuel du professionnel, y compris le dépassement des délais de livraison, le consommateur obtient de plein droit la résolution ou la résiliation du contrat, par simple notification adressée au professionnel par courrier avec accusé de réception.

En cas de résolution ou résiliation du contrat par le consommateur, le professionnel est tenu de lui rembourser les sommes dues au titre du contrat, le cas échéant, dans un délai de trente (30) jours ouvrables à compter du jour de la notification de la résolution ou résiliation par le consommateur.

CHAPITRE III

DES GARANTIES LEGALES

SECTION I

DE LA GARANTIE DE CONFORMITE

Article 357 : Principe général

Toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire de la République du Bénin, fournit des biens ou services conformément aux contrats conclus avec les utilisateurs, et répond des défauts de conformité existant à la livraison.

Elle répond également des défauts de conformité résultant de l'emballage, des instructions de montage ou de l'installation lorsque ceux-ci ont été mis à sa charge par le contrat ou ont été réalisés sous sa responsabilité.

Article 358 : Conditions de conformité

Un bien est conforme à la commande :

1- s'il est propre à l'usage habituellement attendu d'un bien semblable et, le cas échéant :

- s'il correspond à la description donnée par le vendeur dans son offre et possède les qualités que celui-ci a présentées à l'acquéreur ;

- s'il présente les qualités qu'un acquéreur peut légitimement attendre eu égard aux déclarations publiques faites par le vendeur, par le producteur ou par son représentant, notamment dans la publicité ;

2- ou s'il présente les caractéristiques définies d'un commun accord par les parties ou est propre à tout usage spécial recherché par l'acquéreur, porté à la connaissance du vendeur et que ce dernier a accepté.

LégiBénin

Article 359 : Dénonciation de non-conformité

L'acquéreur dispose d'un délai de quinze (15) jours ouvrables à partir de son entrée en possession du bien pour dénoncer sa non-conformité au vendeur. Cette dénonciation est faite par courrier avec accusé de réception.

Les défauts de conformité qui apparaissent dans un délai de vingt-quatre (24) mois à partir de la livraison du bien sont présumés exister au moment de la livraison, sauf preuve contraire. Pour les biens vendus d'occasion, ce délai est fixé à six (06) mois.

Le vendeur peut combattre cette présomption si celle-ci n'est pas compatible avec la nature du bien ou le défaut de conformité invoqué.

Article 360 : Défaut connu

L'acquéreur est en droit d'exiger la conformité du bien à la commande. Il ne peut cependant contester la conformité en invoquant un défaut qu'il connaissait ou ne pouvait ignorer à la passation de la commande. Il en va de même lorsque le défaut a son origine dans les matériaux qu'il a lui-même fournis.

Article 361 : Défaut de conformité

En cas de défaut de conformité, l'acquéreur a le choix, sans frais, entre :

- conserver le bien et se faire rembourser une partie du prix par le vendeur ; - retourner le bien au vendeur et se faire rembourser la totalité du prix ; - retourner le bien au vendeur et se faire livrer un nouveau bien conforme à sa commande.

Les dispositions à l'alinéa 1er ne font pas obstacle à l'allocation de dommages et intérêts.

Article 362 : Prescription

L'action résultant du défaut de conformité se prescrit par deux (2) ans à compter de la livraison du bien.

Legi-Bénin

SECTION II

DE LA GARANTIE DES VICES CACHES

Article 363 : Garantie proprement dite

Toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire de la République du Bénin, garantit les biens vendus contre les vices cachés qui le rendent impropre à l'usage auquel on le destine, ou qui diminuent tellement cet usage que l'acquéreur ne l'aurait pas acquis, ou n'en aurait donné qu'un moindre prix, s'il les avait connus.

Article 364 : Vices apparents

Le vendeur n'est pas tenu des vices apparents et dont l'acquéreur a pu se convaincre lui-même.

Article 365 : Vices cachés inconnus du vendeur

Le vendeur de biens en ligne est tenu d'en garantir les vices cachés, même s'il n'en avait pas connaissance au moment de la commande, à moins que dans ce cas, il n'ait stipulé qu'il ne sera obligé à aucune garantie.

Article 366 : Découverte de vices cachés

En cas de découverte de vices cachés après l'entrée en possession du bien, l'acquéreur a le choix, sans frais, entre :

- conserver le bien et se faire rembourser une partie du prix par le vendeur ;

- retourner le bien au vendeur et se faire rembourser la totalité du prix ;

- retourner le bien au vendeur et se faire livrer un nouveau bien, exempt de vices.

Il n'y aura pas lieu à résolution du contrat ou à diminution du prix si le vendeur s'oblige à réparer les vices cachés.

Article 367 : Connaissance des vices par le vendeur

Si le vendeur connaissait les vices du bien, il est tenu, outre la restitution du prix qu'il en a reçu et des frais occasionnés par la vente, de tous les dommages et intérêts envers l'acquéreur.

Si le vendeur ignorait les vices du bien, il n'est tenu qu'à la restitution du prix, et au remboursement à l'acquéreur des frais occasionnés par la vente.

Article 368 : Destruction du bien

Si le bien comportant le ou les vices a été détruit ou disparait par suite de sa mauvaise qualité, la perte est imputable au vendeur, qui sera tenu envers l'acquéreur à la restitution du prix et le cas échéant, au paiement de dommages intérêts.

Si la destruction ou disparition est fortuite, l'acquéreur assume seul la perte.

Article 369 : Prescription

L'action résultant des vices cachés se prescrit par un délai de deux (2) ans à compter de la découverte du vice.

Legi Benin

SECTION III

DE LA GARANTIE D'EVICTION

Article 370 : Garantie proprement dite

Le vendeur garantit l'acquéreur de l'éviction qu'il souffre dans la totalité ou partie du bien vendu, ou des charges prétendues sur ce bien, et non déclarées lors de la vente.

Article 371: Contrats conclus entre professionnels

Dans le cadre de contrats conclus entre professionnels, les parties peuvent, par des dispositions particulières, aménager les effets et/ou les obligations liées à la garantie d'éviction. Elles peuvent même convenir que le vendeur ne sera soumis à aucune garantie.

Une telle exonération ne peut être applicable en cas de fait personnel du vendeur.

Dans le même cas de stipulations d'exemption de garantie, le vendeur, en cas d'éviction, est tenu à la restitution du prix, à moins que l'acquéreur n'ait connu lors de la vente le danger de l'éviction ou qu'il n'ait acquis le bien à ses risques et périls.

Article 372 : Effets de la garantie d'éviction

Lorsque la garantie d'éviction a été promise, ou qu'il n'a rien été stipulé à ce sujet, si l'acquéreur est évincé, il a droit de demander au vendeur :

- la restitution du prix ;

- celle des fruits, lorsqu'il est obligé de les rendre au propriétaire qui l'évince ;

- les frais faits sur la demande en garantie de l'acquéreur, et ceux faits par le demandeur originaire ;

- les dommages et intérêts, ainsi que les frais et loyaux coûts du contrat.

Lorsqu'au moment de l'éviction, le bien vendu se trouve diminuée de valeur, ou considérablement détériorée, soit par la négligence de l'acquéreur, soit par des faits relevant de la force majeure, le vendeur n'en est pas moins tenu de restituer la totalité du prix.

Si en revanche, l'acquéreur a tiré profit des dégradations faites par lui, le vendeur a droit de retenir sur le prix une somme égale à ce profit.

Article 373 : Augmentation du prix

Si le bien vendu se trouve avoir augmenté de prix au moment de l'éviction, indépendamment même du fait de l'acquéreur, le vendeur est tenu de lui payer ce qu'il vaut au-dessus du prix de la vente.

Article 374 : Remboursement

Le vendeur est tenu de rembourser ou de faire rembourser à l'acquéreur, par celui qui l'évince, toutes les réparations et améliorations utiles qu'il aura faites au bien.

Article 375 : Eviction partielle

Si l'acquéreur n'est évincé que d'une partie du bien qui relativement au tout, soit d'une importance telle que l'acquéreur n'eût pas acquis le bien dans son ensemble sans la partie dont il a été évincé, il peut demander la résolution de la vente.

Article 376 : Prescription

La garantie d'éviction cesse lorsque l'acquéreur s'est laissé condamner par un jugement en dernier ressort, ou dont l'appel n'est plus recevable, sans avoir appelé le vendeur, si celui-ci prouve qu'il existait des moyens suffisants de faire rejeter la demande.

TITRE IV

DE LA RESPONSABILITE DES FOURNISSEURS DE BIENS

ET SERVICES EN LIGNE

Article 377 : Obligation générale de vigilance

Toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire de la République du Bénin est tenue à une obligation générale de vigilance sur les contenus et offres proposés dans le cadre de ses prestations de services, ainsi que sur les activités de ses utilisateurs.

LégiBénin

A ce titre, toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire de la République du Bénin est tenue d'informer sans délai les services de polices ou de gendarmerie et/ou les autorités administratives et judiciaires compétentes, de toute activité illégale, illicite ou suspecte, dont elle pourrait avoir connaissance.

Cette obligation générale de vigilance ne constitue pas une obligation générale de surveillance des informations transmises ou stockées par les utilisateurs, ni une obligation de rechercher activement les faits ou circonstances relevant d'activités illégales, illicites ou suspectes.

Article 378 : Protection des données à caractère personnel

Toute personne exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire national, est tenue au respect des dispositions du présent code relatives à la protection des données à caractère personnel prévues au Livre V.

Sans préjudice des dispositions du Livre V, les personnes exerçant une activité de commerce électronique en République du Bénin ou à destination des utilisateurs établis sur le territoire national, sont tenues d'informer leurs utilisateurs de tout manquement à la sécurité susceptible d'avoir une incidence sur la confidentialité de leurs données personnelles.

LIVRE CINQUIEME

DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

TITRE I

DES PRINCIPES GENERAUX

Article 379 : Objet et principes

Les dispositions du présent Livre ont pour objectif de mettre en place un cadre légal de protection de la vie privée et professionnelle consécutif à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel.

Ce dispositif doit garantir que tout traitement, quelle qu'en soit la forme, respecte les libertés et droits fondamentaux des personnes physiques quelle que soient sa nationalité ou sa résidence tout en prenant en compte les prérogatives de l'Etat, les droits des collectivités locales et les buts pour lesquels les entreprises ont été créées.

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Article 380 : Champ d'application matériel

Les dispositions du présent Livre s'appliquent notamment à :

1- toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation de données à caractère personnel par une personne physique, par l'État, les collectivités locales, les personnes morales de droit public ou de droit privé ;

2- tout traitement automatisé en tout ou en partie, ainsi que tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l'exception des traitements visés à l'alinéa 2 ;

3- tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté et les intérêts essentiels de l'État, sous réserve

LégiBénin

des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

Toute collecte, traitement, transmission, stockage, et usage de données à caractère personnel restent toutefois soumis aux dispositions nationales, communautaires, régionales et internationales applicables en matières commerciale, civile et pénale.

Article 381 : Champ d'application territorial

Les dispositions du présent Livre s'appliquent au traitement des données à caractère personnel effectué dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant sur le territoire de la République du Bénin, que le traitement ait lieu ou non en République du Bénin.

Les dispositions du présent Livre s'appliquent au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de la République du Bénin par un responsable du traitement ou un sous-traitant qui n'est pas établi en République du Bénin, lorsque les activités de traitement sont liées :

1- à l'offre de biens ou de services à ces personnes concernées en République du Bénin, qu'un paiement soit exigé ou non desdites personnes ; ou

2- au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de la République du Bénin ;

3- le traitement est mis en œuvre sur le territoire d'un Etat membre de la CEDEAO.

Les dispositions du présent Livre s'appliquent au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi en République du Bénin mais dans un lieu où le droit de la République du Bénin s'applique en vertu du droit international public.

Article 382 : Exclusions

Les dispositions du présent Livre ne s'appliquent pas aux traitements de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques lorsque ces données ne sont pas destinées à une communication à des tiers ou à la diffusion.

Les dispositions du présent Livre ne peuvent restreindre :

1- des modes de production d'informations disponibles en vertu d'une loi pour une partie dans quelque procédure judiciaire que ce soit ;

2- le pouvoir des cours et tribunaux judiciaires de contraindre un témoin à témoigner ou de contraindre à la production de preuves.

TITRE II

DU TRAITEMENTS DES DONNEES A CARACTERE PERSONNEL

CHAPITRE I

DES DISPOSITIONS GENERALES

Article 383 : Conditions générales de licéité des traitements de données à caractère personnel

Les données à caractère personnel doivent être :

1- traitées légitimement ;

2- collectées, enregistrées, traitées, stockées et transmises de manière licite, loyale, transparente et non frauduleuse ;

Legi-Bénin

3- collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ;

4- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

5- exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

6- conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées.

Les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 396, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par les dispositions du présent Livre afin de garantir les droits et libertés de la personne concernée ;

7- traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

Il incombe au responsable du traitement d'assurer le respect de l'alinéa premier.

Article 384 : Principe de transparence

Le principe de transparence implique une information obligatoire et claire ainsi qu'intelligible de la part du responsable du traitement portant sur les données à caractère personnel.

Article 385 : Principe de confidentialité et de sécurité

Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Article 386 : Sous-traitant

Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens du présent Livre.

Lorsque le traitement est confié à un sous-traitant, le responsable du traitement ou, le cas échéant, son représentant en République du Bénin, doit :

1- choisir un sous-traitant apportant des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements, notamment pour assurer la mise en œuvre des mesures de sécurité et de confidentialité, de manière à ce que le traitement réponde aux exigences du présent Livre et garantisse la protection des droits des personnes concernées ;

2- veiller au respect des mesures du point i. ci-dessus, notamment par la stipulation de mentions spécifiques dans les contrats passés avec des sous-traitants ;

Legi-Bénin

3- fixer dans le contrat, la responsabilité du sous-traitant à l'égard du responsable du traitement et les obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données ;

4- convenir avec le sous-traitant que celui-ci n'agit que sur la seule instruction du responsable du traitement et est tenu par les mêmes obligations que celles auxquelles le responsable du traitement est tenu ;

5- consigner par écrit ou sur un support électronique les éléments du contrat visés dans le présent article.

Toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instruction du responsable du traitement, sauf en cas d'une obligation imposée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

Article 387 : Principe de responsabilité du responsable de traitement

Le responsable du traitement ou son représentant doit notamment :

1- faire toute diligence pour tenir les données à jour, pour rectifier ou supprimer les données inexactes, incomplètes, ou non pertinentes, ainsi que celles obtenues ou traitées en méconnaissance des articles 383, 389, 395, 396 et 397 du présent code

2- veiller à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service ;

3- informer les personnes agissant sous son autorité des dispositions du présent Livre et de ses textes d'application, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel ;

4- s'assurer de la conformité des programmes servant au traitement automatisé des données à caractère personnel avec les termes de la déclaration visée à l'article 405 ainsi que de la régularité de leur application ;

5- mettre en œuvre toutes les mesures techniques et l'organisation appropriées pour assurer la protection des données qu'il traite contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ;

6- empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données ;

7- empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée ;

8- empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées ;

9- empêcher que des systèmes de traitement de données soient utilisés à des fins de blanchiment de capitaux et de financement du terrorisme ;

10- empêcher que, lors de la communication de données et du transport de supports de données, les données puissent être lues, copiées, modifiées, altérées ou effacées de façon non autorisée ;

Legibenin

11- garantir que, lors de l'utilisation d'un système de traitement automatisé de données, les personnes autorisées ne puissent accéder qu'aux données relevant de leur autorisation ;

12- garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données peuvent être transmises par des installations de transmission ;

13- garantir que puisse être vérifiée et constatée a posteriori l'identité des personnes ayant eu accès au système d'information contenant des données à caractère personnel, la nature des données qui ont été introduites, modifiées, altérées, copiées, effacées ou lues dans le système, le moment auquel ces données ont été manipulées ;

14- sauvegarder les données par la constitution de copies de sécurité protégées.

Le responsable du traitement est tenu d'établir un rapport annuel pour le compte de l'Autorité concernant le respect des alinéas 1 et 2.

Article 388 : Responsables conjoints du traitement

Lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Les responsables conjoints du traitement définissent de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent Livre, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations visées aux articles 415 et 416, par voie d'accord entre eux. Un point de contact pour les personnes concernées peut être désigné dans l'accord.

L'accord visé à l'alinéa 1 reflète dûment les rôles respectifs des responsables conjoints du traitement et leurs relations vis-à-vis des personnes concernées. Les grandes lignes de l'accord sont mises à la disposition de la personne concernée.

Indépendamment des termes de l'accord visé à l'alinéa 1, la personne concernée peut exercer les droits que lui confère les dispositions du présent Livre à l'égard de et contre chacun des responsables du traitement.

Article 389 : Principe du consentement et de légitimité

Le traitement des données à caractère personnel est considéré comme légitime si la personne concernée donne son consentement.

Toutefois, il peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire :

1- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

2- à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;

3- à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

4- à la sauvegarde de l'intérêt ou des droits fondamentaux ou à l'intimité de la vie privée physique concernée.

Lorsque le traitement à une fin autre que celle pour laquelle les données ont été collectées n'est pas fondé sur le consentement de la personne concernée, le responsable du traitement, afin de déterminer si le traitement à une autre fin est compatible avec la finalité pour laquelle les données à caractère personnel ont été initialement collectées, tient compte, entre autres :

1- de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé ;

2- du contexte dans lequel les données à caractère personnel ont été collectées, en particulier en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;

3- de la nature des données à caractère personnel, en particulier si le traitement porte sur des catégories particulières de données à caractère personnel, ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées, en vertu de l'article 395 et si ce n'est pas le cas ;

4- des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;

5- de l'existence de garanties appropriées, qui peuvent comprendre le chiffrement ou la pseudonymisation.

Article 390 : Conditions applicables au consentement

Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.

Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent Livre n'est contraignante.

La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il doit être aussi simple de retirer que de donner son consentement.

Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

Article 391 : Transfert de données à caractère personnel vers un Etat tiers ou une organisation internationale - Règles générales

Le transfert de données à caractère personnel faisant l'objet d'un transfert vers un État tiers ou une organisation internationale ne peut avoir lieu que lorsque l'Autorité constate que l'État ou l'Organisation International en question assure un niveau de protection équivalent à celui mis en place par les dispositions du présent Livre.

Le caractère équivalent et suffisant du niveau de protection s'apprécie au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts de données.

Afin de déterminer ce caractère équivalent et suffisant, il est notamment tenu compte de :

1- l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, notamment dans le domaine de la sécurité publique, de la défense, de la sécurité nationale et du droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre

pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;

2- l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres de la Communauté économique des Etats de l'Afrique de l'Ouest ; et

3- les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

Avant tout transfert effectif de données à caractère personnel vers un État tiers ou une organisation internationale, le responsable du traitement doit préalablement obtenir l'autorisation de l'Autorité.

Les transferts de données à caractère personnel vers des Etats tiers ou une organisation internationale font l'objet d'un contrôle régulier de l'Autorité au regard de leur finalité.

Article 392 : Exceptions

Un transfert ou une catégorie de transferts de données à caractère personnel vers un État tiers ou une organisation internationale et n'assurant pas un niveau de protection adéquat, peut être effectué dans un des cas suivants :

1- la personne concernée a expressément donné son consentement au transfert envisagé ;

2- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou des mesures préalables à la conclusion de ce contrat, prises à la demande de la personne concernée ;

3- le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ;

4- le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice ;

5- le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ;

6- le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

Sans préjudice des dispositions de cet article, le Conseil des ministres peut par décret et après avis conforme de l'Autorité, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un État tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat et suffisant, lorsque le responsable du traitement offre des garanties

LegiBenin

suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

Article 393 : Interconnexion des fichiers comportant des données à caractère personnel

L'interconnexion des fichiers visée à l'article 405 du présent code doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements. Elle ne peut pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées ni être assortie de mesures de sécurité appropriées et doit en outre tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

CHAPITRE II

DES DONNEES PERSONNELLES SOUMISES A REGIMES PARTICULIERS

Article 394 : Données sensibles

Le traitement de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

L'interdiction de traiter des données à caractère personnel visées à l'alinéa 1 du présent article ne s'applique pas dans les cas suivants :

1- le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée ;

2- la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit en vigueur en République du Bénin prévoit que l'interdiction visée à l'alinéa 1 ne peut pas être levée par la personne concernée. Le consentement peut être retiré à tout moment sans frais par la personne concernée ;

3- le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

4- le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public ;

5- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou est effectué par une Autorité publique ou est assigné par une Autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;

6- le traitement est effectué en exécution de lois relatives à la statistique publique ;

7- le traitement est nécessaire aux fins de médecine préventive ou la médecine du travail, de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la

Legi-Benin

personne concernée et le traitement est effectué sous la surveillance d'un professionnel des soins de santé ;

8- le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tel que la protection contre les menaces transfrontalières graves pesant sur la santé, aux fins de garantir des normées élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux sur la base du droit en vigueur, qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

9- le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu des dispositions du présent Livre, en vue de l'application de la sécurité sociale ;

10- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée pendant la période précontractuelle ;

11- le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;

12- le traitement est nécessaire afin d'exécuter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail ;

13- le traitement est effectué par des associations dotées de la personnalité juridique ou par des établissements d'utilité publique qui ont pour objet social principal la défense et la promotion des droits de l'homme et des libertés fondamentales, en vue de la réalisation de cet objet, à condition que ce traitement soit autorisé par l'Autorité et que les données ne soient pas communiquées à des tiers sans le consentement écrit des personnes concernées, que ce soit sur un support papier, support électronique ou tout autre support équivalent ;

14- le traitement est effectué dans le cadre des activités légitimes et moyennant les garanties appropriées d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter exclusivement aux membres ou anciens membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à ses objectifs et à sa finalité, et que les données ne soient pas communiquées à un tiers extérieur sans le consentement des personnes concernées ;

15- le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 396.

Les données à caractère personnel visées à l'alinéa 1 peuvent faire l'objet d'un traitement aux fins prévues à l'alinéa 2, point viii, si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit en République du Bénin ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit du Bénin ou aux règles arrêtées par les organismes nationaux compétents.

Article 395 : Données à caractère personnel relatives aux condamnations pénales et aux mesures de sûreté connexes

Les traitements de données à caractère personnel relatives aux infractions, aux condamnations pénales et aux mesures de sûreté connexes peuvent uniquement être mises en œuvre par :

Loi Bénin

1- les juridictions, les autorités publiques et les personnes morales gérant un service public dans le cadre de leurs attributions légales, notamment leurs missions de police judiciaire ou administrative ;

2- les auxiliaires de justice, pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi notamment par des avocats ou d'autres conseils juridiques, pour autant que la défense de leurs clients l'exige ;

3- par d'autres personnes lorsque le traitement est nécessaire à la réalisation de finalités fixées par ou en vertu d'une loi, d'un décret ou d'une ordonnance ;

4- par des personnes physiques ou par des personnes morales de droit public ou de droit privé pour autant que la gestion de leurs propres contentieux l'exige.

Le traitement des données relatives aux condamnations pénales ou aux mesures de sûreté connexes est interdit sauf lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis, ou à l'exécution d'une mission effectuée pour des motifs importants d'intérêt général, dans la mesure où ce traitement est autorisé par le droit des Etats membres de la CEDEAO ou par la législation d'un État membre prévoyant des garanties adéquates.

Un registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'Autorité publique.

Les personnes visées à l'alinéa 1er sont soumises au secret professionnel.

Article 396 : Données à caractère personnel à des fins historiques, statistiques ou scientifiques

Le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques est interdit.

L'interdiction de traiter les données à caractère personnel visées à l'alinéa 1er ne s'applique pas dans les cas suivants :

1- l'objectif de la recherche ne peut être raisonnablement atteint sans que ces informations soient fournies sous une forme permettant d'identifier l'individu ;

2- les informations sont divulguées à la condition qu'elles ne soient pas utilisées afin de contacter une personne pour participer à une étude ;

3- le lien enregistré ne porte pas préjudice à la personne concernée et les avantages découlant du lien enregistré relèvent clairement de l'intérêt public ;

4- le responsable du traitement concerné a approuvé l'ensemble des conditions relatives :

- à la sécurité et confidentialité ;

- au retrait ou destruction des identifiants individuels le plus tôt possible ;

- à l'interdiction de toute utilisation ou divulgation ultérieure de ces informations sous une forme permettant d'identifier les individus sans l'autorisation expresse du responsable du traitement ; et

5- la personne à laquelle ces informations sont communiquées a signé un contrat l'engageant à respecter les conditions approuvées, les dispositions du présent Livre, les politiques et les procédures du responsable du traitement relatives à la confidentialité des informations à caractère personnel.

Legi-Bénin

Le traitement ultérieur de données à caractère personnel à des fins historiques, statistiques ou scientifiques effectué à l'aide de données anonymes est admis.

Article 397 : Données à caractère personnel aux fins de journalisme, de recherche, d'expression artistique ou littéraire

Le traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche ou d'expression artistique ou littéraire est admis lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique ou d'exercice, à titre professionnel, de l'activité de journaliste ou chercheur, dans le respect des règles déontologiques de ces professions.

Article 398 : Application des dispositions de lois relatives à la presse écrite et/ou au secteur audiovisuel et au code pénal

Les dispositions du présent Livre ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou au secteur de l'audiovisuel et du code pénal qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes physiques.

Article 399 : Traitement ne nécessitant pas l'identification

Si les finalités pour lesquelles des données à caractère personnel sont traitées n'imposent pas ou n'imposent plus au responsable du traitement d'identifier une personne concernée, celui-ci n'est pas tenu de conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée à la seule fin de respecter les dispositions du présent Livre.

Lorsque, dans les cas visés à l'alinéa 1er du présent article, le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, il en informe la personne concernée, si possible. En pareil cas, les articles 437, 438, 441 et 443 ne sont pas applicables, sauf lorsque la personne concernée fournit, aux fins d'exercer les droits que lui confèrent ces articles, des informations complémentaires qui permettent de l'identifier.

Article 400 : Interdiction de prospection directe

Il est interdit de procéder à la prospection directe au sens de l'article 332 du présent code.

Article 401 : Fondement d'une décision de justice – Aspects de la personnalité d'une personne physique

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne physique ne peut avoir pour fondement un traitement automatisé, y compris le profilage, des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité.

L'interdiction visée aux alinéas précédents ne s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu des dispositions du présent Livre, d'un décret ou d'une ordonnance. Ce contrat ou cette disposition doivent contenir des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Il devra au moins être permis à celui-ci de faire valoir utilement son point de vue.

Article 402 : Mesures supplémentaires

Lors du traitement de données à caractère personnel visées aux articles 394 et 395 du présent code, le responsable du traitement doit prendre les mesures supplémentaires suivantes :

1- les catégories de personnes, ayant accès aux données à caractère personnel, doivent être désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées ;

2- la liste des catégories des personnes ainsi désignées doit être tenue à la disposition de l'Autorité par le responsable du traitement ou, le cas échéant, par le sous-traitant ;

3- il doit veiller à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées ;

4- lorsque l'information, due en vertu des articles 415 et 416 du présent code, est communiquée à la personne concernée ou lors de la déclaration visée à l'article 405, alinéa premier du présent code, le responsable du traitement doit mentionner la base légale ou réglementaire autorisant le traitement de données à caractère personnel visées aux articles 394 et 395 du présent code.

Article 403 : Informations supplémentaires

Lorsque le traitement de données à caractère personnel, visées aux articles 394 et 395 du présent code, est exclusivement autorisé par le consentement écrit que ce soit sur support papier, support électronique ou tout autre support équivalent, de la personne concernée, le responsable du traitement doit préalablement communiquer, à la personne concernée, en sus des informations dues en vertu des articles 415 et 416 du présent code, les motifs pour lesquelles ces données sont traitées, ainsi que la liste des catégories de personnes ayant accès aux données à caractère personnel.

Article 404 : Lien d'autorité

Lorsque le traitement de données à caractère personnel, visées aux articles 394 et 395 du présent code, est exclusivement autorisé par le consentement écrit que ce soit sur un support papier, support électronique ou tout autre support équivalent de la personne concernée, ce traitement reste, néanmoins, interdit lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement qui l'empêche de refuser librement de donner son consentement.

Cette interdiction est levée lorsque le traitement vise l'octroi d'un avantage à la personne concernée.

CHAPITRE III

DES FORMALITES ET CONDITIONS PREALABLES AU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL

Article 405 : Obligation de déclaration

Les traitements automatisés ou non automatisés exécutés par des organismes publics ou privés et comportant des données à caractère personnel doivent, préalablement à leur mise en œuvre, faire l'objet d'une déclaration préalable auprès de l'Autorité ou être inscrits dans un registre tenu par la personne désignée à cet effet par le responsable du traitement.

En dehors des cas prévus par les dispositions du présent Livre, tous les traitements de données à caractère personnel font l'objet d'une obligation de déclaration auprès de l'Autorité.

Legifrance

Article 406 : Simplification de l'obligation de déclaration

Pour les catégories les plus courantes de traitement des données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés et droits fondamentaux, l'Autorité établit et publie des normes destinées à simplifier l'obligation de déclaration.

Ces normes peuvent prendre en compte les codes de conduite homologués par l'Autorité.

Article 407 : Types de traitements à mettre en œuvre après autorisation

L'Autorité détermine les catégories de traitements qui présentent des risques particuliers au regard des libertés et droits fondamentaux des personnes concernées et qui requièrent une autorisation de l'Autorité.

De telles autorisations sont accordées après réception de la demande d'autorisation du responsable du traitement ou son représentant, qui, en cas de doute, doit consulter l'Autorité.

Sont mis en œuvre après autorisation préalable de l'Autorité:

1- les traitements de données visées aux articles 394 et 397 du présent code ;

2- les traitements portant sur un numéro national d'identification ou tout autre identifiant de la même nature ;

3- les traitements des données à caractère personnel comportant des données biométriques ;

4- les traitements des données à caractère personnel ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques ;

5- les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers ;

6- le transfert de données à caractère personnel envisagé à destination d'un État tiers ;

7- les traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire ;

8- les traitements automatisés de données comportant des appréciations sur les difficultés sociales des personnes.

La demande d'autorisation est présentée par le responsable du traitement ou son représentant.

L'autorisation n'exonère pas de la responsabilité à l'égard des tiers.

Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires et peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à l'Autorité un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

Article 408 : Exemptions

L'Autorité peut exempter certaines catégories de traitements de l'obligation de déclaration lorsque :

1- compte tenu des données traitées, il n'y a manifestement pas de risque d'atteinte aux droits et libertés individuelles des personnes concernées et que sont précisées les finalités du traitement,

LegiBenin

les catégories de données traitées, les catégories de personnes concernées, les catégories de destinataires et la durée de conservation des données ;

2- le responsable du traitement désigne un délégué à la protection des données à caractère personnel pour garantir que les traitements ne soient pas susceptibles de porter atteinte aux droits et libertés des personnes concernées. Le correspondant est chargé notamment :

- d'assurer, d'une manière indépendante, l'application interne des dispositions du présent Livre ;

- de tenir un registre des traitements effectués par le responsable du traitement, contenant les informations visées aux articles 415 et 416 du présent code.

Le bénéfice de la simplification ou de l'exonération de l'obligation de déclaration ne dispense le responsable du traitement de données à caractère personnel d'aucune des autres obligations découlant du présent code.

Le traitement exécuté par les autorités publiques ne peut pas bénéficier de l'exonération de déclaration établie par l'alinéa 1er.

Article 409 : Formalités de demandes d'avis, de déclaration et d'autorisation

Les demandes d'avis, de déclaration et d'autorisation doivent au moins contenir :

1- l'identité, l'adresse complète ou la dénomination sociale du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire de la République du Bénin, les coordonnées de son représentant dûment mandaté ;

2- la ou les finalités du traitement ainsi que la description générale de ses fonctions ;

3- les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements ;

4- les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5- la période au-delà de laquelle les données ne peuvent plus, le cas échéant, être gardées, utilisées ou diffusées ;

6- le ou les services chargés de mettre en œuvre le traitement ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7- les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8- la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès ;

9- les dispositions prises pour assurer la sécurité des traitements et des données dont les garanties qui doivent entourer la communication aux tiers ;

10- l'indication du recours à un sous-traitant ;

11- les transferts de données à caractère personnel envisagés à destination d'un État tiers, sous réserve de réciprocité ;

12- l'engagement que les traitements sont conformes aux dispositions du présent Livre.

Legi-Bénin

L'Autorité peut définir d'autres informations devant être contenues dans les demandes d'avis, de déclaration et d'autorisation.

Article 410 : Dispenses de formalités

Sont dispensés des formalités préalables:

1- les traitements mentionnés à l'article 382, alinéa 1er du présent code ;

2- les traitements ayant pour seul objet la tenue d'un registre destiné à un usage exclusivement privé ;

3- les traitements des données à caractère personnel mis en œuvre par les organismes publics ou privés pour la tenue de leur comptabilité générale ;

4- les traitements des données à caractère personnel mis en œuvre par les organismes publics ou privés relatifs à la gestion des rémunérations de leurs personnels ;

5- les traitements des données à caractère personnel mis en œuvre par les organismes publics ou privés pour la gestion de leurs fournisseurs ;

6- les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dès lors que ces données correspondent à l'objet de cette association ou de cet organisme, qu'elles ne concernent que leurs membres et qu'elles ne doivent pas être communiquées à des tiers.

LegiBenin

Article 411 : Traitements de données à caractère personnel pour le compte du service public

Les traitements des données à caractère personnel opérés pour le compte de l'État, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public sont autorisés par décret pris en Conseil des ministres après avis motivé de l'Autorité.

Ces traitements portent sur :

1- la sûreté de l'État, la défense ou la sécurité publique ;

2- la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;

3- le recensement de la population ;

4- les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle ;

5- le traitement de salaires, pensions, impôts, taxes et autres liquidations.

L'avis de l'Autorité est publié avec le décret autorisant ou refusant le traitement.

Article 412 : Délai

L'Autorité doit se prononcer dans un délai de soixante (60) jours à compter de la réception de la demande d'avis, de déclaration ou d'autorisation.

Toutefois, ce délai peut être prorogé une fois, de trente (30) jours sur décision motivée de l'Autorité.

Si l'avis, la déclaration ou l'autorisation demandé à l'Autorité n'est pas rendu dans le délai prévu, la réponse est réputée favorable.

Article 413 : Voie de demande d'avis, de déclaration ou d'autorisation

La demande d'avis, de déclaration ou d'autorisation peut être adressée à l'Autorité par voie électronique ou par voie postale ou par tout autre moyen contre remise d'un accusé de réception par l'Autorité.

Article 414 : Obligations et pouvoirs de l'organe chargé du contrôle du respect du code de conduite

Le contrôle du respect du code de conduite peut être effectué par un organe qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé à cette fin par l'Autorité.

L'organe visé à l'alinéa premier peut être agréé pour contrôler le respect du code de conduite lorsque cet organe a :

1- démontré, à la satisfaction de l'Autorité, son indépendance et son expertise au regard de l'objet du code ;

2- établi des procédures qui lui permettent d'apprécier si les responsables du traitement et les sous-traitants concernés satisfont aux conditions pour appliquer le code, de contrôler le respect de ses dispositions et d'examiner périodiquement son fonctionnement ;

3- établi des procédures et des structures pour traiter les réclamations relatives aux violations du code ou à la manière dont le code a été ou est appliqué par un responsable du traitement ou un sous-traitant et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public ; et

4- démontré, à la satisfaction de l'Autorité, que ses tâches et ses missions n'entraînent pas de conflit d'intérêts.

L'organe visé à l'alinéa premier du présent article prend, sous réserve des garanties appropriées, des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant, et peut notamment suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informe l'Autorité de ces mesures et des raisons pour lesquelles elles ont été prises.

L'Autorité compétente révoque l'agrément de l'organe visé à l'alinéa 1er si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organe constituent une violation des dispositions du présent Livre.

Le contrôle des traitements effectués par les autorités publiques et les organes publics ainsi que les sanctions administratives de leur non conformité au présent livre, sont de la compétence exclusive de l'Autorité.

Cette prérogative ne peut être déléguée à un organe tiers.

CHAPITRE IV

DES OBLIGATIONS INCOMBANT AUX RESPONSABLES DE TRAITEMENT

Legi Beni

Article 415 : Obligation d'information – Collecte des données auprès de la personne dont les données font l'objet d'un traitement

Le responsable du traitement ou son représentant doit fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, au moins les informations suivantes :

1- son identité et l'adresse de sa résidence habituelle ou de l'établissement principal et, le cas échéant, les coordonnées de son représentant ;

2- le cas échéant, les coordonnées du délégué à la protection des données ;

3- la ou les finalités déterminées du traitement auquel les données sont destinées lorsque le traitement est fondé sur des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

4- les catégories de données concernées ;

5- le ou les destinataires auxquels les données sont susceptibles d'être communiquées ;

6- le fait de pouvoir demander à ne plus figurer sur le fichier ;

7- l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de prospection notamment commerciale, caritative ou politique ;

8- le caractère obligatoire ou non de la réponse, le caractère réglementaire ou contractuel ainsi que les conséquences éventuelles d'un défaut de réponse ;

9- l'existence d'un droit d'accès aux données la concernant et de rectification ou l'effacement de ces données ;

10 lorsque le traitement est fondé sur l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

11- le droit d'introduire une réclamation auprès de l'Autorité ;

12- la durée de conservation des données ;

13- l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 401 et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ;

14- l'éventualité de tout transfert de données à destination d'Etats tiers.

Article 416 : Obligation d'information lorsque les données ne sont pas collectées auprès de la personne dont les données font l'objet d'un traitement

Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement ou son représentant, dès l'enregistrement des données ou, si une communication de données à un tiers est envisagée, au plus tard au moment de la première communication des données, fournit à la personne concernée, sauf si elle en est déjà informée, au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée :

1- le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;

2- le cas échéant, les coordonnées du délégué à la protection des données ;

Légi-Bénin

3- la ou les finalités du traitement ;

4- l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant à des fins de prospection directe notamment commerciale, caritative ou politique. Dans ce cas, la personne concernée est informée avant que des données à caractère personnel ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection ;

5- d'autres informations supplémentaires, y compris :

- les catégories de données concernées ;

- les destinataires ou les catégories de destinataires ;

- la durée de conservation des données ;

- l'éventualité de tout transfert de données à destination d'Etats tiers,

- lorsque le traitement est fondé sur les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ;

- l'existence d'un droit d'accès aux données la concernant et de rectification ou l'effacement de ces données ;

- lorsque le traitement est fondé sur l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;

- le droit d'introduire une réclamation auprès de l'Autorité ;

- la source d'où proviennent les données à caractère personnel et, le cas, échéant, une mention indiquant qu'elles sont issues de sources accessibles au public ;

- l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 401 et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Le responsable du traitement fournit les informations visées à l'alinéa premier :

1- dans un délai raisonnable après avoir obtenu les données à caractère personnel, mais ne dépassant pas trente (30) jours, eu égard aux circonstances particulières dans lesquelles les données à caractère personnel sont traitées ;

2- si les données à caractère personnel doivent être utilisées aux fins de la communication avec la personne concernée, au plus tard au moment de la première communication à ladite personne ; ou

3- s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

Lorsqu'il a l'intention d'effectuer un traitement ultérieur des données à caractère personnel pour une finalité autre que celle pour laquelle les données à caractère personnel ont été obtenues, le responsable du traitement fournit au préalable à la personne concernée des informations au sujet de cette autre finalité et toute autre information pertinente visée à l'alinéa 1er.

Article 417 : Dispenses

Le responsable du traitement est dispensé de fournir les informations visées aux articles 445 et 446, lorsque :

1- en particulier pour un traitement à des fins statistiques, historiques ou scientifiques ou pour le dépistage motivé par la protection et la promotion de la santé publique, l'information de la personne concernée se révèle impossible ou implique des efforts disproportionnés ;

2- la personne concernée dispose déjà de ces informations ;

3- l'enregistrement ou la communication des données à caractère personnel est effectué en vue de l'application d'une disposition d'une loi ou d'un décret.

Article 418 : Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée

Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 415 et 416 ainsi que pour procéder à toute communication au titre des articles 437 et 443 et de l'article 410, en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant. Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. Lorsque la personne concernée en fait la demande, les informations peuvent être fournies oralement, à condition que l'identité de la personne concernée soit démontrée par d'autres moyens.

Article 419 : Facilitation de l'exercice des droits par le responsable du traitement

Le responsable du traitement facilite l'exercice des droits conférés à la personne concernée au titre des articles 437 et 443. Dans les cas visés à l'article 399, alinéa 2, le responsable du traitement ne refuse pas de donner suite à la demande de la personne concernée d'exercer les droits que lui confèrent les articles 437 et 443, à moins que le responsable du traitement ne démontre qu'il n'est pas en mesure d'identifier la personne concernée.

Article 420 : Fourniture des informations par le responsable du traitement

Le responsable du traitement fournit à la personne concernée des informations sur les mesures prises à la suite d'une demande formulée en application des articles 437 et 443, dans les meilleurs délais et en tout état de cause dans un délai de trente (30) jours à compter de la réception de la demande. Au besoin, ce délai peut être prolongé de soixante (60) jours, compte tenu de la complexité et du nombre de demandes. Le responsable du traitement informe la personne concernée de cette prolongation et des motifs du report dans un délai de trente (30) jours à compter de la réception de la demande. Lorsque la personne concernée présente sa demande sous une forme électronique, les informations sont fournies par voie électronique lorsque cela est possible, à moins que la personne concernée ne demande qu'il en soit autrement.

Si le responsable du traitement ne donne pas suite à la demande formulée par la personne concernée, il informe celle-ci sans tarder et au plus tard dans un délai de trente (30) jours à compter de la réception de la demande des motifs de son inaction et de la possibilité d'introduire une réclamation auprès de l'Autorité et de former un recours juridictionnel.

Article 421 : Conditions de gratuité des informations

Aucun paiement n'est exigé pour fournir les informations au titre des articles 415 et 416 et pour procéder à toute communication et prendre toute mesure au titre des articles 437 et 443 et de l'article 427. Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut :

Loi Bénin

1- exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées ; ou

2- refuser de donner suite à ces demandes. Il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

Article 422 : Confirmation de l'identité

Sans préjudice des dispositions de l'article 399, lorsque le responsable du traitement a des doutes raisonnables quant à l'identité de la personne physique présentant la demande visée aux articles 437 et 443, il peut demander que lui soient fournies des informations supplémentaires nécessaires pour confirmer l'identité de la personne concernée.

Article 423 : Icônes normalisées

Les informations à communiquer aux personnes concernées en application des articles 415 et 416 peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible, du traitement prévu. Lorsque les icônes sont présentées par voie électronique, elles sont lisibles par machine.

Article 424 : Protection des données dès la conception et la protection des données par défaut

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, tels que la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent Livre et de protéger les droits de la personne concernée.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Ces mesures s'appliquent à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

Article 425 : Les obligations de confidentialité

Le traitement des données à caractère personnel est confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement et seulement sur ses instructions, sauf en vertu d'obligations légales contraires.

Article 426 : Les obligations de sécurité

Afin de garantir la sécurité des données à caractère personnel, le responsable du traitement et/ou son sous-traitant doivent mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, l'interception notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié tenant compte, d'une part, de l'état de la technique en la matière et des frais qu'entraîne l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

Il incombe également au responsable du traitement, son représentant ainsi qu'au sous- traitant de veiller au respect de ces mesures de sécurité.

Ces mesures peuvent notamment comprendre :

1- la pseudonymisation et le chiffrement des données à caractère personnel ;

2- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

3- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;

4- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le choix du sous-traitant et les modalités du contrat liant celui-ci avec le responsable du traitement sont soumis aux dispositions du présent Livre.

Aux fins de la conservation des preuves, les éléments du contrat ou de l'acte juridique relatifs à la protection des données et les exigences portant sur les mesures visées à l'alinéa précédent du présent article sont consignés par écrit ou sous une autre forme équivalente mais garantissant la pérennité et l'inaltérabilité du document.

Legi-Bénin

Article 427 : Responsabilités

Le responsable du traitement doit notifier, sans délai, à l'Autorité et à la personne concernée toute rupture de la sécurité ayant affecté les données à caractère personnel de la personne concernée.

Le sous-traitant doit avertir, sans délai, le responsable du traitement de toute rupture de la sécurité ayant affecté les données à caractère personnel qu'il traite pour le compte et au nom du responsable du traitement.

La notification visée à l'alinéa 1er doit, à tout le moins :

1- décrire la nature de la rupture de sécurité ayant affecté des données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la rupture et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;

2- communiquer le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;

3- décrire les conséquences probables de la rupture de sécurité ;

4- décrire les mesures prises ou que le responsable du traitement propose de prendre pour remédier à la rupture de sécurité, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

La communication à la personne concernée visée à l'alinéa 1er n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

1- le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite rupture, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;

2- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé à l'alinéa 1er n'est plus susceptible de se matérialiser ;

3- elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

Article 428 : Analyse d'impact

Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires.

Lorsqu'il effectue une analyse d'impact relative à la protection des données, le responsable du traitement demande conseil au délégué à la protection des données, si un tel délégué a été désigné.

L'analyse d'impact relative à la protection des données visée à l'alinéa 1er est, en particulier, requise dans les cas suivants :

1- l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

2- le traitement à grande échelle de catégories particulières de données visées à l'article 394, alinéa premier, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395 ; ou

3- la surveillance systématique à grande échelle d'une zone accessible au public.

L'Autorité établit et publie une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise conformément à l'alinéa 1er.

L'Autorité peut aussi établir et publier une liste des types d'opérations de traitement pour lesquelles aucune analyse d'impact relative à la protection des données n'est requise.

L'analyse contient au moins :

1- une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;

2- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;

Légi-Bénin

3- une évaluation des risques pour les droits et libertés des personnes concernées conformément à l'alinéa 1 ; et

4- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect des dispositions du présent Livre, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.

Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.

Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Article 429 : Consultation préalable

Le responsable du traitement consulte l'Autorité préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article précédent indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.

Lorsque l'Autorité est d'avis que le traitement envisagé visé à l'alinéa 1er, constituerait une violation des dispositions du présent Livre, en particulier lorsque le responsable du traitement n'a pas suffisamment identifié ou atténué le risque, l'Autorité fournit par écrit, dans un délai maximum de huit (08) semaines à compter de la réception de la demande de consultation, un avis écrit au responsable du traitement et, le cas échéant, au sous-traitant, et peut faire usage de ses pouvoirs. Ce délai peut être prolongé de six (06) semaines, en fonction de la complexité du traitement envisagé. L'Autorité informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai de trente (30) jours à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'Autorité ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.

Lorsque le responsable du traitement consulte l'Autorité en application de l'alinéa 1er, il lui communique :

1- le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises ;

2- les finalités et les moyens du traitement envisagé ;

3- les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu des dispositions du présent Livre ;

4- le cas échéant, les coordonnées du délégué à la protection des données ;

5- l'analyse d'impact relative à la protection des données prévue à l'article précédent ; et

6- toute autre information que l'Autorité demande.

Article 430 : Désignation du délégué à la protection des données

Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

Togo Digital

1- le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

2- les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou

3- les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 394 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 395.

Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.

Dans les cas autres que ceux visés à l'alinéa 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 432.

Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'Autorité.

Article 431 : Fonction du délégué à la protection des données

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

Le responsable du traitement et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 432 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.

Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère les dispositions du présent Livre.

Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.

Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

Article 432 : Missions du délégué à la protection des données

Les missions du délégué à la protection des données sont au moins les suivantes :

1- informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu des dispositions du présent Livre en matière de protection des données ;

2- contrôler le respect des dispositions du présent Livre en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ;

3- dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 428 ;

4- coopérer avec l'Autorité ;

5- faire office de point focal pour l'Autorité sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 412, et mener des consultations, le cas échéant, sur tout autre sujet.

Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Article 433 : Les obligations de conservation

Les données à caractère personnel ne doivent pas être conservées au-delà de la période requise pour les fins en vue desquelles elles ont été recueillies et traitées.

Au-delà de cette période requise, les données ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales. Les traitements dont la finalité se limite à assurer la conservation à long terme de documents d'archives sont dispensés des formalités préalables à la mise en œuvre des traitements prévus par les dispositions du présent Livre.

Il peut être procédé à un traitement ayant des finalités autres que celles mentionnées à l'alinéa 2 :

1- soit avec l'accord exprès de la personne concernée ;

2- soit avec l'autorisation de l'Autorité.

Article 434 : Les obligations de pérennité

Legi-Benin

Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées quel que soit le support technique utilisé.

Il doit particulièrement s'assurer que l'évolution de la technologie ne sera pas un obstacle à cette exploitation.

Article 435 : Registre des activités de traitement

Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes :

1- le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;

2- les finalités du traitement ;

3- une description des catégories de personnes concernées et des catégories de données à caractère personnel ;

4- les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;

5- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale ;

6- les délais prévus pour l'effacement des différentes catégories de données ;

7- une description générale des mesures de sécurité techniques et organisationnelles.

Chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tiennent un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement, comprenant :

1- le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit ainsi que, le cas échéant, les noms et les coordonnées du représentant du responsable du traitement ou du sous-traitant et celles du délégué à la protection des données ;

2- les catégories de traitements effectués pour le compte de chaque responsable du traitement ;

3- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts, les documents attestant de l'existence de garanties appropriées ;

4- une description générale des mesures de sécurité techniques et organisationnelles.

Les registres visés aux alinéas 1 et 2 se présentent sous une forme écrite y compris la forme électronique.

Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent le registre à la disposition de l'Autorité sur demande.

LegiBenin

Les obligations visées aux alinéas 1 et 2 ne s'appliquent pas aux petites et moyennes entreprises sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 394, alinéa premier, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions.

Article 436 : Obligations des prestataires de confiance

Sans préjudice du Livre II, les prestataires de services visés par le Livre précité sont soumis aux exigences en matière de protection des données à caractère personnel prévues par les dispositions du présent Livre.

CHAPITRE V

DES DROITS DES PERSONNES A L'EGARD DE LEURS DONNEES PERSONNELLES

Article 437 : Droit d'accès

Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement :

1- les informations permettant de connaître et de contester le traitement de ses données à caractère personnel ;

2- la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;

3- la communication sous forme intelligible des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;

4- le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État tiers ;

5- lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée ;

6- l'existence du droit de demander au responsable du traitement la rectification ou l'effacement de données à caractère personnel, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement ;

7- le droit d'introduire une réclamation auprès d'une Autorité de contrôle ;

8- lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;

9- l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 401, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

A cette fin, la personne concernée adresse une demande datée et signée au responsable du traitement par voie postale ou électronique, ou son représentant.

Legibenin

Une copie des renseignements lui est communiquée sans délai et au plus tard dans les soixante (60) jours de la réception de la demande.

Le paiement des frais pour toute copie supplémentaire demandée par la personne concernée devra être fixé par note de service de la structure responsable du traitement sur la base des coûts administratifs conséquents.

Toutefois, l'Autorité saisie contradictoirement par le responsable du fichier peut lui accorder :

1- des délais de réponse ;

2- l'autorisation de ne pas tenir compte de certaines demandes manifestement abusives par leur nombre, leur caractère répétitif ou systématique.

Lorsqu'il y a lieu de craindre la dissimulation ou la disparition des informations mentionnées au premier alinéa du présent article, et même avant l'exercice d'un recours juridictionnel, il peut être demandé au juge compétent que soient ordonnées toutes mesures de nature à éviter cette dissimulation ou cette disparition.

Lorsque les données relatives à la santé de la personne concernée sont traitées aux fins de recherches médico-scientifiques, qu'il est manifeste qu'il n'existe aucun risque qu'il soit porté atteinte à la vie privée de cette personne et que les données ne sont pas utilisées pour prendre des mesures à l'égard d'une personne concernée individuelle, la communication peut, pour autant qu'elle soit susceptible de nuire gravement auxdites recherches, être différée au plus tard jusqu'à l'achèvement des recherches. Dans ce cas, la personne concernée doit avoir préalablement donné son autorisation écrite au responsable du traitement que les données à caractère personnel la concernant peuvent être traitées à des fins médico-scientifiques et la communication de ces données peut dès lors être différée.

Article 438 : Droit à la portabilité des données

Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque :

1- le traitement est fondé sur le consentement ou sur un contrat ; et

2- le traitement est effectué à l'aide de procédés automatisés.

Lorsque la personne concernée exerce son droit à la portabilité des données en application de l'alinéa premier, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.

Le droit visé à l'alinéa premier ne porte pas atteinte aux droits et libertés de tiers.

Article 439 : Droit d'interrogation

Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication.

Article 440 : Droit d'opposition

Legibenin

Toute personne physique a le droit de s'opposer, à tout moment, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Elle a le droit, d'une part, d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection notamment commerciale, caritative ou politique et, d'autre part, de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Ce droit doit être explicitement proposé à la personne concernée d'une façon intelligible et doit pouvoir être clairement distingué d'autres informations.

Lorsqu'il est fait droit à une opposition conformément à cet article, le responsable du traitement n'utilise ni ne traite plus les données à caractère personnel concernées.

Lorsque les données à caractère personnel sont collectées à des fins de prospection notamment commerciale, caritative ou politique, la personne concernée peut s'opposer, gratuitement et sans aucune justification, au traitement projeté de données à caractère personnel la concernant.

Pour exercer son droit d'opposition, l'intéressé adresse une demande datée et signée, par voie postale ou électronique, au responsable du traitement ou son représentant. Le responsable du traitement doit communiquer dans les trente (30) jours qui suivent la réception de la demande prévue à l'alinéa précédent, quelle suite il a donnée à la demande de la personne concernée.

Lorsque des données à caractère personnel sont collectées par écrit, que ce soit sur un support papier, support électronique ou tout autre support équivalent, auprès de la personne concernée, le responsable du traitement demande, à celle-ci, sur le document grâce auquel il collecte ses données, si elle souhaite exercer le droit d'opposition.

Lorsque les données à caractère personnel sont collectées auprès de la personne concernée, autrement que par écrit, le responsable du traitement demande à celle-ci si elle souhaite exercer le droit d'opposition, soit sur un document qu'il lui communique à cette fin au plus tard soixante (60) jours après la collecte des données à caractère personnel, soit par tout moyen technique qui permet de conserver la preuve que la personne concernée a eu la possibilité d'exercer son droit.

En cas de contestation, la charge de la preuve incombe au responsable de traitement auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.

Article 441: Droit de rectification et de suppression

Toute personne physique peut exiger du responsable du traitement que soient, selon les cas, et dans les meilleurs délais, rectifiées, complétées, mises à jour, verrouillées ou supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, non pertinentes ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Pour exercer son droit de rectification ou de suppression, l'intéressé adresse une demande, par voie postale ou par voie électronique, datée et signée au responsable du traitement, ou son représentant.

Dans les quarante cinq (45) jours qui suivent la réception de la demande prévue à l'alinéa précédent, le responsable du traitement communique les rectifications ou effacements des données effectués à la personne concernée elle-même ainsi qu'aux personnes à qui les données inexactes, incomplètes, équivoques, périmées, non pertinentes ou dont la collecte, l'utilisation, la communication ou la conservation est interdite, ont été communiquées. Quand le responsable du traitement n'a pas connaissance des destinataires de la communication et que la notification

à ces destinataires ne parait pas possible ou implique des efforts disproportionnés, il le leur notifie dans le délai imparti.

En cas de non-respect du délai prévu à l'alinéa précédent, une plainte peut être adressée à l'Autorité par l'auteur de la demande.

Si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par l'Autorité.

Les ayants droit d'un "de cujus" justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les ayants droit en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.

Article 442 : Fichier nominatif

Sur avis favorable de l'Autorité, un fichier nominatif peut être complété ou corrigé même d'office lorsque l'organisme qui le tient acquiert connaissance de l'inexactitude ou du caractère incomplet d'une information nominative contenue dans ce fichier.

Si une information a été transmise à un tiers, sa rectification ou son annulation doit être notifiée à ce tiers, sauf dispense accordée par l'Autorité.

Article 443 : Données rendues publiques - Droit à l'oubli

Lorsque le responsable du traitement a rendu publiques les données à caractère personnel de la personne concernée, il prend toutes les mesures raisonnables, y compris les mesures techniques, en ce qui concerne les données publiées sous sa responsabilité, en vue d'informer les tiers qui traitent lesdites données qu'une personne concernée leur demande d'effacer tout lien vers ces données à caractère personnel, ou toute copie ou reproduction de celles-ci.

Lorsque le responsable du traitement a autorisé un tiers à publier des données à caractère personnel de la personne concernée, il est réputé responsable de cette publication et prend toutes les mesures appropriées pour mettre en œuvre le droit à l'oubli numérique et à l'effacement des données à caractère personnel.

Le responsable du traitement met en place des mécanismes appropriés assurant la mise en œuvre du respect du droit à l'oubli numérique et à l'effacement des données à caractère personnel ou examine périodiquement la nécessité de conserver ces données, conformément aux dispositions du présent Livre.

Lorsque l'effacement est effectué, le responsable du traitement ne procède à aucun autre traitement de ces données à caractère personnel.

Les alinéas 1, 2, 3 et 4 ne s'appliquent pas dans la mesure où ce traitement est nécessaire :

1- à l'exercice du droit à la liberté d'expression et d'information ;

2- pour respecter une obligation légale qui requiert le traitement ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

3- pour des motifs d'intérêt public dans le domaine de la santé publique ;

4- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 366, dans la mesure où le droit visé à l'alinéa 1erest susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement ; ou

5- à la constatation, à l'exercice ou à la défense de droits en justice.

Article 444 : Conditions de suppression

L'Autorité adopte, sans préjudice des dispositions du présent code, des mesures ou des lignes directrices aux fins de préciser :

1- les conditions de la suppression des liens vers ces données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communications électroniques accessibles au public ;

2- les conditions et critères applicables à la limitation du traitement des données à caractère personnel.

Article 445 : Droit d'accès relatif à des traitements concernant la sûreté de l'Etat, la défense et la sécurité publique

En ce qui concerne les traitements relatifs à la sûreté de l'Etat, la défense et la sécurité publique, la demande est adressée à l'Autorité qui désigne l'un de ses membres appartenant ou ayant appartenu à la Cour suprême ou à la chambre des comptes de la Cour suprême pour mener toutes investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un autre membre de l'Autorité.

Il est notifié au requérant qu'il a été procédé aux vérifications.

Lorsque l'Autorité constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'Autorité peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi dans un délai de quarante (45) jours suivant la réception de la demande.

Article 446 : Représentation d'un enfant mineur

Lorsque l'article 436 s'applique en ce qui concerne l'offre directe de services de la société de l'information aux mineurs, le traitement des données à caractère personnel relatives à un mineur est licite lorsque le mineur est âgé d'au moins seize (16) ans. Lorsque le mineur est âgé de moins de seize (16) ans, ce traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard du mineur.

Le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles.

Article 447 : Représentation d'un majeur incapable

En cas d'incapacité physique ou mentale dûment attestée par un professionnel des soins de santé, les droits, tels que fixés par les dispositions du présent Livre, d'une personne concernée majeure, sont exercés par le ou la conjoint (e) cohabitant (e), le partenaire cohabitant légal ou le partenaire cohabitant de fait.

Projet

Si cette personne ne souhaite pas intervenir ou si elle fait défaut, les droits sont exercés, en ordre subséquent, par un enfant majeur, un parent, un frère ou une sœur majeur de la personne concernée.

Si une telle personne ne souhaite pas intervenir ou si elle fait défaut, c'est un tuteur ad hoc qui veille aux intérêts de la personne concernée.

Cela vaut également en cas de conflit entre deux ou plusieurs des personnes mentionnées dans le présent alinéa.

La personne concernée est associée à l'exercice de ses droits autant qu'il est possible et compte tenu de sa capacité de compréhension.

Article 448 : Droit d'introduire une réclamation auprès de l'Autorité

Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès de l'Autorité, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation des dispositions du présent Livre.

L'Autorité informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article suivant.

Article 449 : Droit à un recours juridictionnel effectif contre l'Autorité

Toute personne concernée a le droit de former un recours effectif devant la juridiction administrative compétente lorsque l'Autorité ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de quatre vingt dix (90) jours, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article précédent.

Article 450 : Droit à un recours juridictionnel effectif contre un responsable du traitement ou un sous-traitant

Toute personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confèrent les dispositions du présent Livre ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation des dispositions du présent livre.

Article 451 : Droit à réparation et responsabilité

Toute personne ayant subi un dommage matériel ou moral du fait d'une violation des dispositions du présent Livre a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation des dispositions du présent Livre. Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations prévues par les dispositions du présent Livre qui incombent spécifiquement aux sous-traitants ou qu'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

Un responsable du traitement ou un sous-traitant est exonéré de responsabilité, au titre de l'alinéa 2, s'il prouve que le fait qui a provoqué le dommage ne lui est nullement imputable.

Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des alinéas 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des

Legibenin

responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective.

Lorsqu'un responsable du traitement ou un sous-traitant a, conformément à l'alinéa 4, réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées à l'alinéa 2.

Les actions judiciaires engagées pour exercer le droit à obtenir réparation sont intentées devant les juridictions compétentes.

CHAPITRE VI

DES SANCTIONS ET MESURES ADMINISTRATIVES

Article 452 : Avertissement et mise en demeure

L'Autorité peut prononcer un avertissement à l'encontre du responsable du traitement qui ne respecte pas les obligations découlant des dispositions du présent Livre.

Elle peut également mettre en demeure le responsable du traitement de faire cesser le manquement constaté dans un délai fixé qui ne peut excéder huit (08) jours.

Article 453 : Manquements graves

Constitue des manquements graves, au titre du présent code, le fait de :

1- procéder à une collecte déloyale de données à caractère personnel ;

2- communiquer à un tiers non autorisé des données à caractère personnel ;

3- procéder à la collecte de données sensibles, de données relatives à des infractions ou à un numéro national d'identification sans respecter les conditions légales ;

4- procéder à la collecte ou à l'utilisation de données à caractère personnel ayant pour conséquence de provoquer une atteinte grave aux droits fondamentaux ou à l'intimité de la vie privée physique concernée ;

5- empêcher les services de l'Autorité d'effectuer une mission de contrôle sur place ou faire preuve d'obstruction lors de la réalisation d'une telle mission.

Article 454 : Types de sanction

Lorsque le responsable du traitement ne se conforme pas à la mise en demeure, l'Autorité peut prononcer à son encontre, dans le respect du principe du contradictoire, les sanctions suivantes :

1- une sanction pécuniaire, à l'exception des cas où les traitements sont mis en œuvre par l'État ;

2- une injonction de cesser le traitement des données à caractère personnel ;

3- un retrait définitif ou temporaire de l'autorisation accordée en application des dispositions du présent Livre ;

4- un verrouillage de certaines données à caractère personnel.

Article 455 : Montant

Tic-Bénin

Le montant de la sanction pécuniaire prévue au point 1 de l'article précédent est proportionné à la gravité des manquements commis et aux avantages tirés de ce manquement.

Lors du premier manquement, il ne peut excéder cinquante millions (50 000 000) de francs CFA. En cas de manquement réitéré dans les cinq (05) années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder cent millions (100 000 000) de francs CFA ou, s'agissant d'une entreprise, cinq pour cent (5 %) du chiffre d'affaires hors taxes du dernier exercice clos dans la limite de cent millions (100 000 000) de francs CFA.

Lorsque l'Autorité a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce.

Article 456 : Injonction

Toute sanction prononcée par l'Autorité peut être assortie d'une injonction de procéder, dans un délai qui ne peut excéder huit (08) jours, à toute modification ou suppression utile dans le fonctionnement des traitements de données à caractère personnel, objet de la sanction.

Article 457 : Rapport

Les sanctions prévues dans les dispositions du présent Livre sont prononcées sur la base d'un rapport établi par l'Autorité. Ce rapport est notifié au responsable du traitement, qui peut faire des observations écrites ou orales dans un délai de quinze (15) jours dès la réception de la notification de l'Autorité et qui peut assister ou se faire représenter aux séances à l'issue desquelles la l'Autorité statue.

Les décisions prises par l'Autorité sont motivées et notifiées au responsable du traitement.

Article 458 : Recours

Les décisions prononçant une sanction peuvent faire l'objet d'un recours devant la juridiction administrative compétente.

Article 459 : Publication

Les sanctions prononcées peuvent être rendues publiques par l'Autorité.

CHAPITRE VII

DES DISPOSITIONS PENALES

Article 460 : Infractions pénales

Constituent des infractions au sens des dispositions du présent Livre, sans préjudice de celles prévues par le code pénal :

1- le fait d'entraver l'action de la l'Autorité :

- en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités ;

- en refusant de communiquer à ses membres ou aux agents habilités les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître ;

- en communiquant des informations qui ne sont pas conformes au contenu des enregistrements tel qu'il était au moment où la demande a été formulée ou qui ne présentent pas ce contenu sous une forme directement accessible ;

LegiBénin

2- toute personne physique ou morale qui, sans droit même par négligence, procède ou fait procéder à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre telles que prescrites par les dispositions du présent Livre ;

3- quiconque en connaissance de cause, décide de faire usage de données à caractère personnel collectées au moyen de données collectées par le procédé décrit au point (ii), sans en être l'auteur est également condamné comme s'il était l'auteur du traitement frauduleux ;

4- le fait, hors les cas où le traitement des données a été réalisé dans les conditions prévues par les dispositions des dispositions du présent Livre, de procéder ou de faire procéder à un traitement de données à caractère personnel parmi lesquelles, des données sensibles relatives à des infractions ou des données relatives au numéro d'identification national ;

5- le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans avoir mis en œuvre les mesures prescrites par les dispositions du présent Livre ;

6- le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite ;

7- le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner et/ou de manipuler ces informations ;

8- quiconque a transféré, fait ou laissé transférer des données à caractère personnel vers un État tiers sans qu'il ait été satisfait aux exigences prévues au Chapitre 2 du Titre II du présent Livre ;

9- quiconque, pour contraindre une personne à lui communiquer les renseignements obtenus par l'exercice du droit consacré par l'article 436 du présent code, ou à donner son autorisation au traitement de données à caractère personnel la concernant, a usé à son égard de voies de fait, de violence ou menaces, de dons ou de promesses ;

10- le fait de procéder à un traitement des données à caractère personnel concernant une personne physique malgré la demande de rectification ou l'opposition de cette personne, lorsque cette demande de rectification ou cette opposition est fondée sur des motifs légitimes ;

11- le fait de ne pas respecter les dispositions du présent Livre relatives à l'information des personnes ;

12- le fait de ne pas respecter les dispositions du présent Livre relatives aux droits d'accès ;

13- le fait de conserver des données à caractère personnel au-delà de la durée prévue pour la déclaration préalable adressée à l'Autorité sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques au sens du présent Livre ;

14- le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter sans autorisation de l'intéressé ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ;

15- le fait de participer à une association formée ou à une entente établie en vue de la commission d'une ou plusieurs infractions prévues par les dispositions du présent Livre.

Article 461 : Peines

Projet

Les infractions visées à l'article 445 du présent code sont punies d'une peine d'emprisonnement de six (06) mois à dix (10) ans et d'une amende de dix millions (10 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces deux peines seulement.

La complicité et la tentative sont punies des mêmes peines.

Si l'auteur de l'infraction au point 1 de l'article 460 procède ou fait procéder, par simple négligence, à des traitements de données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre telles que prescrites par les dispositions du présent Livre, seule une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA peut lui être infligée.

Le tribunal peut ordonner l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction.

Les décisions de condamnation devenues définitives prises en vertu de ce Chapitre sont publiées dans le Journal officiel de la République du Bénin ainsi que sur un support électronique aux frais du condamné.

En cas de condamnation pour une des infractions prévues à l'article 460 du présent code, la juridiction de jugement peut prononcer des peines à titre complémentaire.

Elle peut prononcer la confiscation des supports matériels des données à caractère personnel formant l'objet de l'infraction, tels que les fichiers manuels, disques et bandes magnétiques, à l'exclusion des ordinateurs ou de tout autre matériel, ou ordonner l'effacement de ces données ainsi que des sommes, avantages ou produits résultant de l'infraction et appartenant au condamné.

La confiscation ou l'effacement peuvent être ordonnés même si les supports matériels des données à caractère personnel n'appartiennent pas au condamné.

Les objets confisqués doivent être détruits lorsque la décision est passée en force de chose jugée.

Sans préjudice des interdictions énoncées par des dispositions particulières, en cas de condamnation pour une des infractions prévues à l'article 460 du présent code, la juridiction de jugement peut prononcer l'interdiction à titre de peine complémentaire. Cette interdiction implique une interdiction de gérer, personnellement ou par personne interposée, et pour deux (02) ans au maximum, tout traitement de données à caractère personnel.

Toute infraction à l'interdiction édictée par l'alinéa 10 ou toute récidive relative aux infractions visées dans le présent Chapitre sont punies d'un emprisonnement de un an (01) à dix (10) ans et d'une amende de dix millions (10 000 000) à cent millions (100 000 000) de francs CFA ou de l'une de ces deux peines seulement.

Le présent article n'empêchera pas l'adoption de toute mesure d'indulgence établie par les dispositions du présent Livre, comme la suspension ou une peine avec sursis, sauf pour les décisions visées aux alinéas 5 à 10.

Le responsable de traitement ou son représentant sera passible du paiement des amendes encourues par son sous-traitant.

TITRE III

DE L'AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Registered

CHAPITRE I

DE L'ORGANISATION ET DU FONCTIONNEMENT

Article 462 : Constitution

L'Autorité de protection des données à caractère personnel en abrégé "APDP", ci-après désignée Autorité, veille à l'application des dispositions du présent Livre et au respect de la vie privée en général sur le territoire de la République du Bénin.

Article 463 : Statut

L'Autorité est une structure administrative indépendante dotée de la personnalité juridique, de l'autonomie administrative et de gestion.

Elle exerce une mission de service public et ne reçoit d'instruction d'aucune autorité administrative et politique.

Article 464 : Composition

L'Autorité est composée de onze (11) membres ainsi qu'il suit :

1- trois (03) députés désignés par l'Assemblée nationale en tenant compte de sa configuration politique ;

2- un (01) membre du Conseil Economique et Social élu par ses pairs ;

3- deux (02) personnes qualifiées pour leur connaissance des applications informatiques ayant un diplôme sanctionnant au moins quatre (04) années d'études universitaires et totalisant au moins dix (10) années d'expérience, désignées par l'Assemblée nationale sur une liste de cinq (05) personnes retenues par le Bureau de l'Assemblée nationale, après appel à candidatures ;

4- une (01) personnalité désignée par le Président de la République ;

5- trois (03) magistrats dont deux (02) de la Cour suprême et un (01) de la juridiction des comptes de même degré ayant au moins quinze (15) années d'expérience professionnelle, élus par leurs pairs ;

6- un (01) avocat ayant au moins quinze (15) années d'expérience, élu par ses pairs.

L'Autorité est dirigée par un Bureau de trois (03) membres.

L'Autorité élit en son sein un Président, un vice-Président et un Secrétaire.

Article 465 : Commissaire du Gouvernement

Un commissaire du Gouvernement, désigné par le Président de la République en Conseil des ministres, siège auprès de l'Autorité.

Le commissaire peut, dans les dix (10) jours suivant une délibération, provoquer une seconde délibération.

Article 466 : Nomination

Les membres de l'Autorité, une fois désignés sont nommés par décret pris en Conseil des ministres.

Pour être nommé et rester membres de l'Autorité, les candidats doivent remplir les conditions suivantes :

Légi-Bénin

- être de nationalité béninoise ;

- jouir de leurs droits civils et politiques ;

- respecter les incompatibilités visées à l'article 473

Article 467 : Vacances

Le mandat d'un membre de l'Autorité prend fin pour cause de décès, d'incapacité physique ou mentale, de démission ou de révocation.

A la demande du Président, il est pourvu à son remplacement par sa structure d'origine. Un nouveau commissaire est nommé pour la période du mandat restant à courir, par décret pris en Conseil des ministres.

En cas de vacances dûment constatée du Président, le vice-Président assume provisoirement les fonctions de Président, conformément au Règlement intérieur.

La durée de l'exercice de ces fonctions intérimaires ne peut excéder une période de quatre vingt dix (90) jours.

Article 468 : Serments

Avant leur entrée en fonction, les membres de l'Autorité prêtent serment devant la Cour suprême siégeant en audience solennelle, en ces termes :

«Je jure solennellement de bien et fidèlement remplir ma fonction de membre de l'Autorité en charge de la protection des données à caractère personnel, en toute indépendance et impartialité de façon digne et loyale et de garder le secret des délibérations».

Les agents recrutés par l'Autorité de protection des données à caractère Personnel prêtent serment devant le Tribunal de première instance de Cotonou en ces termes :

«Je jure de bien et loyalement remplir mes fonctions d'agent de l'Autorité en charge de la protection des données à caractère personnel en toute indépendance et impartialité et de garder le secret des délibérations».

Article 469 : Durée du mandat

La durée du mandat des membres de l'Autorité est de cinq (05) ans renouvelable une (01) fois.

Article 470 : Président

Le Président est l'ordonnateur du budget, il assume la gestion quotidienne de l'Autorité, dirige le secrétariat, préside les réunions de l'Autorité en ses différentes formations ou délègue un autre membre à cette fin qui le représente. Il fait périodiquement rapport devant l'Autorité réunie en séances administratives.

En cas d'empêchement du Président, le vice-Président assure ses fonctions.

Article 471 : Règlement intérieur

L'Autorité adopte son Règlement intérieur qui fixe son mode de fonctionnement.

Elle établit dans son Règlement intérieur, notamment, les règles relatives à l'instruction, à la présentation des dossiers, au traitement des plaintes et aux procédures contradictoires.

Il est publié au Journal officiel

Article 472 : Vote

Le Benin

L'Autorité ne délibère valablement que si la majorité de ses membres au moins est présente. Elle décide à la majorité absolue. En cas de parité des voix, la voix du Président est prépondérante.

Article 473 : Incompatibilités

La qualité de membre de l'Autorité est incompatible avec celle de membre du Gouvernement, l'exercice de fonctions de dirigeant d'entreprise, ou la détention de participations dans les entreprises du secteur de l'informatique ou des communications électroniques.

Les membres de l'Autorité s'abstiennent de tout acte incompatible avec leurs fonctions et, pendant la durée de leur mandat, n'exercent aucune activité professionnelle incompatible, rémunérée ou non.

Aucun membre de l'Autorité ne peut :

1- participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il détient un intérêt, direct ou indirect, exerce des fonctions ou détient un mandat ;

2- être présent lors de la délibération ou des vérifications sur les objets pour lesquels ils ont un intérêt personnel ou pour lesquels leurs parents ou alliés jusqu'au quatrième degré ont un intérêt personnel ;

3- participer à une délibération ou procéder à des vérifications relatives à un organisme au sein duquel il a, au cours des trente six (36) mois précédant la délibération ou les vérifications, détenu un intérêt direct ou indirect, exercé des fonctions ou détenu un mandat.

Après la cessation de leurs fonctions, les membres de l'Autorité sont tenus de respecter les devoirs d'honnêteté et de délicatesse quant à l'acceptation de certaines fonctions ou de certains avantages.

Article 474 : Inamovibilité et indépendance des membres de l'Autorité

Les membres de l'Autorité sont inamovibles pendant la durée de leur mandat.

Toutefois, en cas de faute grave dûment constatée de l'un des membres de l'Autorité ou de la perte de la qualité au titre de laquelle il a été élu ou désigné, il est mis fin à ses fonctions et procédé à son remplacement conformément aux dispositions du présent Livre et du Règlement intérieur de l'Autorité.

Le mandat du successeur ainsi désigné est limité à la période restant à courir. Ce dernier peut être désigné pour un seul mandat.

Dans les limites de leurs attributions, le Président et les membres ne reçoivent d'instructions de personne. Ils ne peuvent être relevés de leur charge en raison des opinions qu'ils émettent ou des actes qu'ils accomplissent pour remplir leurs fonctions.

Article 475 : Secret professionnel

Les membres et les agents de l'Autorité sont tenus au secret professionnel pour les informations dont ils ont connaissance dans le cadre ou à l'occasion de leurs fonctions.

Le personnel de l'Autorité ainsi que les experts et agents assermentés sont soumis, y compris après cessation de leurs activités, à l'obligation de secret professionnel à l'égard de toute information confidentielle, fait ou acte dont ils ont eu connaissance dans l'exercice de leurs fonctions officielles.

Legal Bénin

La violation des alinéas 1 ou 2 est punie des peines prévues par les dispositions du code pénal relatives au secret des correspondances.

Article 476 : Exception au devoir de discrétion

Les informaticiens appelés, soit à donner les renseignements à l'Autorité, soit à témoigner devant elle sont déliés autant que de besoin de leur obligation de discrétion.

Article 477 : Budget

Il est alloué annuellement à l'Autorité des crédits nécessaires à son bon fonctionnement. Ces crédits sont inscrits au budget de l'État.

L'Autorité peut recevoir des subventions de la part des organisations internationales dont l'Etat est membre et de tous autres organismes légalement constitués. Elle peut également bénéficier de ressources propres issues de l'exercice de ses activités.

Les budgets doivent être rendus publics.

Article 478 : Déclarations - Avis

L'Autorité reçoit, par voie postale ou par voie électronique, les déclarations de traitements informatiques et donne son avis dans les cas prévus par les dispositions du présent Livre.

Article 479 : Liste des traitements autorisés

L'Autorité tient à la disposition du public, la liste des traitements qui ont fait l'objet d'une autorisation.

Article 480 : Saisine de l'Autorité

L'Autorité peut être saisie par toute personne physique ou morale, agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée.

Article 481 : Plaintes - Rapport

L'Autorité reçoit, par voie postale ou par voie électronique, et instruit les plaintes conformément à sa mission.

Chaque année, elle présente au Président de la République et au Président de l'Assemblée nationale, un rapport rendant compte de l'exécution de sa mission.

Il doit être rendu public.

Article 482 : Recours

Les décisions de l'Autorité sont susceptibles de recours devant la juridiction administrative compétente.

CHAPITRE II

DES MISSIONS ET POUVOIRS DE L'AUTORITE

Article 483 : Formalités - Attributions – Pouvoirs - Devoirs

L'Autorité s'assure que les technologies de l'information et de la communication (TIC) ne comportent pas de menace au regard des libertés publiques et de la vie privée. Elle veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions du présent Livre.

LégiBenin

A ce titre, l'Autorité est en charge :

1- de répondre à toute demande d'avis ou recommandation portant sur un traitement de données à caractère personnel ;

2- d'émettre de sa propre initiative des avis motivés ou des recommandations sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée dans le cadre du présent Livre, ainsi que des lois contenant des dispositions relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel ;

3- d'informer les personnes concernées et les responsables de traitements de leurs droits et obligations ;

4- d'autoriser ou refuser les traitements de fichiers dans un certain nombre de cas, notamment les fichiers sensibles ;

5- de recevoir les formalités préalables à la création de traitements des données à caractère personnel et le cas échéant autoriser ces traitements ;

6- de recevoir, par la voie postale ou par voie électronique, les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informer leurs auteurs des suites données à celles-ci notamment si un complément d'enquête ou une coordination avec une autre autorité de protection nationale est nécessaire ;

7-. d'effectuer, sans préjudice de toute action devant les tribunaux, des enquêtes, soit de sa propre initiative, soit à la suite d'une réclamation ou à la demande d'une autre Autorité de protection nationale, et informe la personne concernée, si elle l'a saisie d'une réclamation, du résultat de ses enquêtes dans un délai raisonnable ;

8- d'informer sans délai l'autorité judiciaire pour certains types d'infractions dont elle a connaissance ;

9- d'informer, sans délai, le procureur de la République, conformément aux dispositions du code de procédure pénale, des violations des dispositions du présent Livre, constitutives d'infractions pénales ;

10- d'informer l'Assemblée nationale, le Gouvernement ou d'autres institutions politiques, ainsi que le public, de toute question relative à la protection des données à caractère personnel ;

11- de conduire de fréquentes consultations avec des parties prenantes sur des questions que l'Autorité considère comme pouvant nuire à la protection effective des données à caractère personnel pour les services, les installations, les appareils ou les annuaires au titre du présent Livre ;

12- de requérir des experts ou agents assermentés, en vue de participer à la mise en œuvre des missions de vérification portant sur tout traitement des données à caractère personnel sur le territoire de la République du Bénin ;

13- de veiller au respect des autorisations et consultations préalables ;

14- de prononcer la rectification, l'effacement ou la destruction de toutes les données lorsqu'elles ont été traitées en violation des dispositions du présent Livre et la notification de ces mesures aux tiers auxquels les données ont été divulguées ;

15- de demander au responsable du traitement ou au sous-traitant de satisfaire aux demandes d'exercice des droits prévus par les dispositions du présent Livre présentées par la personne concernée ;

Legi-Bénin

16- de prononcer des sanctions, administratives et pécuniaires, à l'égard des responsables de traitement ;

17- de mettre à jour un répertoire des traitements des données à caractère personnel et à la disposition du public ;

18- de surveiller les faits nouveaux présentant un intérêt, dans la mesure où ils ont une incidence sur la protection des données à caractère personnel, notamment l'évolution des technologies de l'information et des communications et celle des pratiques commerciales ;

19- d'informer le responsable du traitement ou le sous-traitant d'une violation alléguée des dispositions régissant le traitement des données à caractère personnel et, le cas échéant, d'ordonner au responsable du traitement ou son sous-traitant de remédier à cette violation par des mesures déterminées, afin d'améliorer la protection de la personne concernée ;

20- de conseiller les personnes physiques ou morales qui procèdent à des traitements des données à caractère personnel ou à des essais ou expériences de nature à aboutir à de tels traitements ;

21- d'autoriser ou refuser des transferts transfrontaliers de données à caractère personnel vers des Etats tiers ;

22- de sensibiliser le public aux risques, aux règles, aux garanties et aux droits relatifs au traitement des données à caractère personnel. Les activités destinées spécifiquement aux enfants, personnes âgées ou personnes gravement malades ou à tous ceux qui ne peuvent pas être en mesure de comprendre la portée des activités qui leur sont proposées, font l'objet d'une attention particulière ;

23- de faire des propositions de modifications législatives ou réglementaires susceptibles de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;

24- d'homologuer les codes de conduite et de recueillir et d'autoriser, le cas échéant, les projets, modifications ou prorogations desdits codes ;

25- de mettre en place des mécanismes de coopération avec les autorités de protection des données à caractère personnel d'États tiers dont le partage d'informations et l'assistance mutuelle ;

26- de participer aux négociations internationales en matière de protection des données à caractère personnel.

L'accomplissement des formalités auprès de l'Autorité est gratuit pour la personne concernée. Lorsque les demandes sont manifestement excessives, en raison, notamment, de leur caractère répétitif, l'Autorité peut, néanmoins, exiger le paiement de frais ou ne pas prendre les mesures sollicitées par la personne concernée. Il incombe à l'Autorité d'établir le caractère manifestement excessif de la demande.

Article 484 : Obligations d'information

L'Autorité informe par tous moyens appropriés, les autorités publiques, les organismes privés et les représentants de la société civile, des décisions, et avis qu'elle rend en matière de protection de la vie privée.

Article 485 : Pouvoir réglementaire

Legibenin

Pour exercer les missions qui lui sont confiées par les dispositions du présent Livre, l'Autorité dispose d'un pouvoir réglementaire lui permettant d'autoriser certains traitements, d'adapter des mesures de simplification ou de dispense de déclaration et de définir les modalités d'exercice des droits des personnes, en particulier en matière d'information.

Article 486 : Pouvoirs d'investigation

L'Autorité peut demander aux premiers présidents des cours d'appel ou aux présidents des juridictions administratives, de déléguer un magistrat de leur ressort, éventuellement assisté d'experts, pour des missions d'investigation et de contrôle effectuées sous sa direction.

Afin de conserver certaines données particulièrement susceptibles de perte ou de modification et utiles à la manifestation de la vérité, l'Autorité peut demander au président du tribunal de première instance, que celles-ci soient conservées conformément à la procédure prévue à l'article 78 bis du code de procédure pénale.

Article 487 : Demande d'information

L'Autorité peut enjoindre aux responsables de fichiers de lui communiquer toutes informations utiles sur les fichiers informatiques qu'ils utilisent.

Article 488 : Obligation de coopération

Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs et utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent, en principe, s'opposer à l'action de l'Autorité. Ils doivent prendre toutes mesures utiles afin de lui faciliter sa mission.

Article 489 : Accès aux locaux

Les membres de l'Autorité ainsi que les agents de ses services assurent le contrôle de la mise en œuvre du traitement. A cet effet, ils ont accès, de six (06) heures à vingt-et-une (21) heures, dans l'exercice de leur mission, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le procureur de la République territorialement compétent en est préalablement informé.

Le responsable de locaux professionnels privés est informé de son droit d'opposition à la visite. En cas d'opposition du responsable des lieux ou du responsable du traitement, la visite ne peut se dérouler qu'avec l'autorisation du président du Tribunal de première instance compétent ou du juge délégué par lui.

Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du président du Tribunal de première instance compétent ou du juge délégué par lui. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite.

La visite s'effectue sous l'autorité et le contrôle du président du Tribunal de première instance compétent ou du juge délégué par lui qui l'a autorisée, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle.

L'acte ayant autorisé la visite est exécutoire au seul vu de la minute. Il mentionne que le juge ayant autorisé la visite peut être saisit à tout moment d'une demande de suspension ou d'arrêt

LegiBenin

de cette visite. Elle indique le délai et la voie de recours. Elle peut faire l'objet, suivant les règles prévues par le code de procédure civile, d'un appel. Celui-ci connaît également des recours contre le déroulement des opérations de visite.

Les membres de l'Autorité et les agents mentionnés au premier alinéa de cet article peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie.

Ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles. Ils peuvent accéder aux programmes informatiques et aux données, ainsi qu'en demander la transcription par tout moyens approprié dans des documents directement utilisables pour les besoins du contrôle.

Ils peuvent, à la demande du Président de l'Autorité, être assistés par des experts désignés par l'autorité dont ceux-ci dépendent.

Seul un professionnel des soins de santé peut requérir la communication de données médicales individuelles incluses dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou à la gestion de service de santé, et qui est mis en œuvre par un membre d'une profession de santé.

A l'issue de la visite, il est dressé contradictoirement procès-verbal des vérifications et visites menées.

Le procès-verbal est adressé, pour observations, à l'Autorité.

Article 490 : Délais

Les différents délais prévus par les dispositions du présent Livre pour permettre à l'Autorité de statuer sont doublés en cas d'exercice par l'Autorité d'un des pouvoirs d'investigation prévus aux articles 487, 488 et 490 du présent code.

LégiBénin

LIVRE SIXIEME

DE LA CYBERCRIMINALITE ET DE LA CYBERSECURITE

TITRE I

DE LA LUTTE CONTRE LA CYBERCRIMINALITE

CHAPITRE I

DES PRINCIPES GENERAUX

Article 491 : Objet

Les dispositions du présent Livre fixent les règles et les modalités de lutte contre la cybercriminalité en République du Bénin. Elles fixent également le cadre institutionnel, les règles et les modalités d'utilisation de la cryptologie en République du Bénin.

Article 492 : Champ d'application

Les pouvoirs et procédures prévus dans le présent Titre aux fins d'enquêtes ou de procédures pénales spécifiques s'appliquent :

1- aux infractions pénales établies conformément au Titre I du présent Livre ;

2- à toutes les autres infractions pénales commises sur et au moyen d'un système informatique ;

3- à la collecte des preuves électroniques de toute infraction pénale.

Article 493 : Garantie des droits fondamentaux et des libertés

La mise en œuvre et l'application des pouvoirs et procédures prévus au présent Titre sont soumises aux conditions et sauvegardes prévues par le droit interne de la République du Bénin, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application du Pacte international relatif aux droits civils et politiques des Nations-Unies et de la Charte africaine des droits de l'homme et des peuples ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

Article 494 : Responsabilité des personnes morales

Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont responsables des infractions prévues par les dispositions du présent Livre lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

1- sur un pouvoir de représentation de la personne morale ;

2- sur une autorité pour prendre des décisions au nom de la personne morale ;

3- sur une autorité pour exercer un contrôle au sein de la personne morale.

Outre les cas déjà prévus à l'alinéa précédent, une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée à l'alinéa précédent a rendu possible l'Autorité des infractions prévues par les dispositions du présent Livre pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Les peines encourues par les personnes morales, pour les infractions visées au Titre I du présent Livre, sont les suivantes :

1- une amende dont le montant maximum est égal au quintuple de celui prévu pour les personnes physiques par la loi qui réprime l'infraction ;

2- la dissolution, lorsque la personne morale a été créée ou, lorsqu'il s'agit d'un crime ou d'un délit puni en ce qui concerne les personnes physiques d'une peine d'emprisonnement supérieure à cinq (05) ans, détournée de son objet pour commettre les faits incriminés ;

3- l'interdiction définitive ou pour une durée de cinq (05) ans au plus d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales ;

4- la fermeture définitive ou pour une durée de cinq (05) ans au plus d'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

5- l'exclusion définitive des marchés publics ou pour une durée de cinq (05) ans au plus ;

6- l'interdiction définitive ou pour une durée de cinq (05) ans au plus de faire appel public à l'épargne ;

7- l'interdiction pour une durée de cinq (05) ans au plus d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ou d'utiliser des cartes de paiement ;

8- la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;

Toute personne morale condamnée à l'une des peines ci-dessus énumérées a l'obligation d'afficher la décision prononcée ou de la diffuser par la presse écrite soit par tout moyen de communication au public par voie électronique.

CHAPITRE II

DE LA RESPONSABILITE DES ACTEURS DE L'INTERNET

SECTION I

DU REGIME GENERAL DE RESPONSABILITES

Article 495 : Obligation de conservation de données

Les fournisseurs de services en ligne détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires.

Ils fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 501.

Les magistrats et les fonctionnaires chargés de la mise en œuvre de l'exercice de l'action publique, les autorités administratives mentionnées à l'article 595 du présent code pourraient requérir auprès des fournisseurs de services en ligne, conformément à la loi, la conservation et la protection de l'intégrité ainsi que la communication des données mentionnées au premier alinéa.

Les dispositions prévues au Livre V du présent code sont applicables au traitement de ces données.

Article 496 : Responsabilité des opérateurs fournissant un accès à internet

Les opérateurs fournissant un accès à internet ne sont pas responsables du contenu des informations qu'ils transmettent et auxquelles ils donnent accès, s'il est satisfait à chacune des conditions suivantes :

1- ils ne sont pas à l'origine de la transmission ;

2- ils ne sélectionnent pas le destinataire de la transmission ;

3- ils ne sélectionnent, ni ne modifient, les informations faisant l'objet de la transmission.

Pour les besoins du présent article, les activités d'opérateurs fournissant un accès à internet visées à l'alinéa 1er comprennent notamment le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communications et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

Legi Benin

Les opérateurs fournissant un accès à internet informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, et leur proposent au moins un de ces moyens.

Article 497 : Responsabilité des fournisseurs de services en ligne

Les fournisseurs de services en ligne ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de leurs services, s'ils n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où ils en ont eu connaissance, ils ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du fournisseur de services en ligne.

Les fournisseurs de services en ligne ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de leurs services s'ils n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où ils en ont eu connaissance, ils ont agi promptement pour retirer ces informations ou en rendre l'accès impossible.

L'alinéa précédent ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa.

Le fait, pour toute personne, de présenter à un fournisseur de services en ligne un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'un (1) an d'emprisonnement et d'une amende de cinq millions (5 000 000) de francs CFA.

Article 498 : Notification de contenus illicites

La connaissance des faits litigieux est présumée acquise par le fournisseur de services en ligne, lorsqu'il lui est notifié les éléments suivants :

1- la date de la notification ;

3- si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ; si le notifiant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;

3- le nom et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;

4- la description des faits litigieux et, si possible, leur localisation précise ;

5- les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;

6- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification de ce que l'auteur ou l'éditeur n'a pu être contacté.

Article 499 : Absence d'obligation générale de surveillance

Les opérateurs fournissant un accès à internet et les fournisseurs de services en ligne ne sont pas soumis à une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des

Legal Bénin

activités illicites. Ils sont toutefois tenus à l'obligation de vigilance prévue à l'article 377 du présent code.

Le précédent alinéa est sans préjudice de toute activité de surveillance ciblée et temporaire demandée par les services de police, de gendarmerie ou l'autorité judiciaire.

Article 500 : Coopération à la lutte contre la cybercriminalité

Compte tenu de l'intérêt général attaché à la répression de l'apologie des crimes contre l'humanité, de l'incitation à la haine raciale ainsi que de la pornographie enfantine, les opérateurs fournissant un accès à internet et les fournisseurs de services en ligne doivent concourir à la lutte contre les infractions visées au présent Livre.

A ce titre, ils doivent mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance les faits qui en relèvent. Elles ont également l'obligation, d'une part, d'informer promptement les autorités compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre publics les moyens qu'elles consacrent à la lutte contre ces activités illicites.

L'autorité judiciaire peut enjoindre, en référé ou sur requête, à tout fournisseur de services en ligne, et à défaut, à tout opérateur fournissant un accès à internet, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service en ligne.

LégiBénin

Article 501 : Editeur de services de communications au public en ligne

Les personnes dont l'activité est d'éditer un service de communications au public en ligne mettent à disposition du public, dans un standard ouvert :

1- s'il s'agit de personnes physiques, leur nom, prénom, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au Registre du Commerce et du Crédit Mobilier ou un registre équivalent, le numéro de leur inscription ;

2- s'il s'agit de personnes morales, leur dénomination ou leur raison sociale, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au Registre du Commerce et du Crédit Mobilier ou un registre équivalent, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;

3- le nom du directeur et du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction ;

4- le nom, la dénomination ou la raison sociale et l'adresse et le numéro de téléphone du Fournisseur de services en ligne.

Les personnes éditant à titre non professionnel un service de communications au public en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du fournisseur de services en ligne, sous réserve de lui avoir communiqué les éléments d'identification prévus au présent article.

Les fournisseurs de services en ligne sont tenus à une obligation de confidentialité, pour tout ce qui concerne la divulgation de ces éléments d'identification ou de toute information permettant d'identifier la personne concernée. Cette obligation de confidentialité n'est pas opposable à l'autorité judiciaire, ni aux services d'enquête de police et de gendarmerie.

Article 502 : Sanctions

Est puni d'un (1) an d'emprisonnement et de cinquante millions (50 000 000) de francs CFA d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'activité de fournisseur d'accès à internet ou de fournisseur de services en ligne, de ne pas satisfaire à l'une quelconque des obligations définies aux articles 495 à 500 du présent code.

Est puni d'un (1) an d'emprisonnement et de cinquante millions (50 000 000) de francs CFA d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'activité d'éditeur de services de communications au public en ligne, de ne pas avoir respecté les prescriptions de l'article 501 du présent code.

SECTION II

DES REGIMES PARTICULIERS DE RESPONSABILITES

Article 503 : Fournisseurs de cache

Les fournisseurs de cache ne sont pas responsables des données et informations qu'ils traitent dans le cadre de leurs activités, pour autant que chacune des conditions suivantes soit remplie :

1- ils ne modifient pas l'information ;

2- ils se conforment aux conditions d'accès à l'information ;

3- ils se conforment aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisée dans le secteur ;

4- ils n'entravent pas l'utilisation légale de la technologie, largement reconnue et utilisée par le secteur, dans le but d'obtenir des données sur l'utilisation de l'information ;

5- ils agissent promptement pour retirer l'information stockée ou pour rendre l'accès à celle-ci impossible dès qu'ils ont effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'une autorité administrative ou judiciaire a ordonné de retirer l'information ou de rendre l'accès à cette dernière impossible.

Article 504 : Fournisseurs de liens hypertextes

Les fournisseurs de liens hypertextes ne sont pas responsables des informations auxquelles ils donnent accès, dès lors que :

1- ils suppriment ou empêchent rapidement l'accès aux informations après avoir reçu une injonction de l'autorité judiciaire, de retirer le lien hypertexte ; et que

2- lorsqu'ils ont pris connaissance ou conscience autrement que par une injonction de l'autorité judiciaire, d'informations illégales spécifiques stockées ou des activités illégales qu'exerceraient les destinataires de leurs services, informent rapidement les services de police, pour leur permettre d'évaluer la nature des informations ou des activités et, si nécessaire, d'ordonner le retrait du contenu.

Article 505 : Fournisseurs de moteurs de recherche

Les fournisseurs de services en ligne qui, de manière automatique ou sur la base des entrées effectuées par autrui, créent un index des contenus en ligne ou mettent à disposition des moyens électroniques pour rechercher les informations fournies par des tiers, ne sont pas responsables des résultats de recherche, à condition qu'ils :

Legi-Benin

1- ne soient pas à l'origine de la transmission ;

2- ne sélectionnent pas le destinataire de la transmission ; et

3- ne sélectionnent pas ou ne modifient pas les informations contenues dans la transmission.

Article 506: Activités d'hébergement

Un hébergeur n'est pas responsable des informations stockées à la demande d'un utilisateur du service qu'il fournit, à condition que :

1- lorsqu'il a connaissance d'informations illégales spécifiques stockées ou des activités illégales qu'exerceraient les destinataires du service, il informe rapidement les services de police ou judiciaires, afin de leur permettre d'évaluer la nature des informations et, si nécessaire, faire émettre une injonction pour en retirer le contenu. Aussi longtemps que les services de police et/ou judiciaires n'ont pas pris de décision concernant la copie, l'accessibilité et le retrait des données stockées, l'hébergeur peut uniquement prendre des mesures visant à empêcher l'accès à ces données ; ou

2- l'hébergeur retire, rend l'accès impossible ou désactive promptement l'accès aux données après avoir reçu des services de police ou judiciaires, une injonction de retirer les données.

L'alinéa 1er ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle de l'hébergeur.

LégiBénin

CHAPITRE III

DES ATTEINTES AUX RESEAUX ET SYSTEMES D'INFORMATION

Article 507 : Accès et maintien illégal

Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un système informatique est puni d'un emprisonnement de un (01) à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à un million (1 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque accède ou se maintient intentionnellement et sans droit, dans l'ensemble ou partie d'un système informatique, avec une intention frauduleuse est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès légal à un système informatique, est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement.

Lorsqu'il résulte des faits visés aux alinéas 1 à 3 soit la suppression, l'obtention ou la modification de données contenues dans le système informatique, soit une altération du fonctionnement de ce système informatique, les peines prévues dans ces alinéas seront doublées.

Lorsque les faits visés aux alinéas 1 à 3 sont commis en violation de mesures de sécurité, la peine est la réclusion criminelle à temps de dix (10) ans à vingt (20) ans et une amende de cinq millions (5 000 000) de francs CFA à cinq cent millions (500 000 000) de francs CFA.

L'accès, pour une durée déterminée, à des systèmes informatiques est autorisé sans que le secret professionnel ou bancaire puisse être opposé conformément aux dispositions du code de procédure pénale.

Article 508 : Atteinte aux données informatiques

Quiconque intercepte, divulgue, utilise, altère ou détourne intentionnellement et sans droit par des moyens techniques, des données informatiques lors de leur transmission non publique à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques, est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA.

Quiconque transfère sans autorisation des données d'un système informatique ou d'un moyen de stockage de données informatique est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cent millions (100 000 000) de francs CFA.

Si l'infraction visée à l'alinéa précédent est commise avec une intention frauduleuse, ou en rapport avec un système informatique connecté à un autre système informatique, ou en contournant les mesures de protection mises en place pour empêcher l'accès au contenu de la transmission non publique, les peines prévues à l'alinéa précédent sont doublées.

Une personne ne commet pas une infraction au sens du présent article, si :

1- l'interception est réalisée conformément à un mandat de justice ;

2- la communication est envoyée par ou est destinée à une personne qui a consenti à l'interception ;

3- un fonctionnaire habilité estime qu'une interception est nécessaire en cas d'urgence, dans le but de prévenir un décès, une blessure ou un dommage à la santé physique ou mentale d'une personne, ou d'atténuer une blessure ou un dommage à la santé physique ou mentale d'une personne ;

4- une personne morale ou physique est légalement autorisée pour les besoins de la sécurité publique ou de la défense nationale ; ou

5- une personne morale ou physique est légalement autorisée en vertu des dispositions du code de procédure pénale.

Article 509 : Atteinte à l'intégrité du système

Quiconque qui, intentionnellement et sans droit, directement ou indirectement provoque, par tout moyen technologique, une interruption du fonctionnement normal d'un système informatique est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque, suite à la commission des faits visés à l'alinéa 1er, cause un dommage à des données dans le système informatique concerné ou dans tout autre système informatique, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque, suite à la commission des faits visés à l'alinéa 1er, provoque une perturbation grave ou empêche, totalement ou partiellement, le fonctionnement normal du système informatique concerné ou de tout autre système informatique, est condamné à la réclusion criminelle à temps

Legibenin

de dix (10) ans à vingt (20) ans et à une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement.

Lorsque la commission des faits visés à l'alinéa 1er touche une ou plusieurs infrastructures sensibles, au sens du présent code, la personne responsable est condamnée à la réclusion criminelle à temps de dix (10) ans à vingt (20) ans et à une amende de cinq millions (5 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement.

La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes.

Article 510 : Atteinte à l'intégrité des données

Quiconque, intentionnellement et sans droit, directement ou indirectement endommage, efface, détériore, altère ou supprime des données informatiques est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement.

Si l'infraction visée à l'alinéa 1er est commise avec une intention frauduleuse ou dans le but de nuire, la peine d'emprisonnement est de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs à deux millions (2 000 000) de francs CFA ou l'une de ces peines seulement.

La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes.

Article 511 : Abus de dispositifs

Quiconque, intentionnellement et sans droit, produit, vend, obtient en vue de son utilisation, importe, exporte, diffuse ou met à disposition sous une autre forme, un quelconque dispositif, y compris des données informatiques ou des programmes informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre, est puni d'un emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque, intentionnellement et sans droit, possède au sens du présent code, dans l'intention de l'utiliser, un quelconque dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement.

Est puni d'une peine d'emprisonnement de deux (02) ans à cinq (05) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces peines seulement, tout officier ou fonctionnaire public, dépositaire ou agent de la force publique qui, à l'occasion de l'exercice de ses fonctions, hors les cas prévus par la loi ou sans respecter les formalités qu'elle prescrit, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission d'une ou plusieurs infractions visées au Titre I du présent Livre.

Article 512: Falsification informatique

Quiconque commet un faux, en introduisant, intentionnellement et sans droit, dans un système informatique, en modifiant, altérant ou effaçant des données, qui sont stockées, traitées ou

Legibenin

transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et ce dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si les données falsifiées étaient authentiques, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque cherchant à se procurer, pour lui-même ou pour autrui, avec une intention frauduleuse, un avantage économique illégal en introduisant dans un système informatique, en modifiant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation normale des données dans un système informatique, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque en connaissance de cause, décide de faire usage de données falsifiées, au sens des alinéas 1 et 2, sans en être l'auteur, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA ou de l'une de ces peines seulement, comme s'il était l'auteur de la falsification informatique.

La peine d'emprisonnement et l'amende sont applicables même si les conséquences sur le ou les systèmes informatiques visés aux alinéas précédents sont temporaires ou permanentes.

Article 513 : Fraude informatique

Quiconque, intentionnellement et sans droit, cause ou cherche à causer un préjudice patrimonial à autrui avec l'intention de procurer un avantage économique illégal à soi-même ou à une tierce partie, est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et d'une amende de cinq millions (5 000 000) à cinquante millions (50 000 000) de francs CFA :

1- en introduisant dans un système informatique, en modifiant, altérant ou effaçant des données qui sont stockées, traitées ou transmises par un système informatique ; ou

2- en perturbant le fonctionnement normal d'un système informatique ou des données y contenues.

CHAPITRE IV

DES INFRACTIONS LIEES A L'UTILISATION DES DONNEES

A CARACTERE PERSONNEL

Article 514 : Envoi de messages non sollicités

Tout message électronique non sollicité envoyé sur la base de la collecte de données à caractère personnel doit contenir un lien pouvant permettre au bénéficiaire de se désabonner.

Le non respect de cette disposition expose le contrevenant à une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA.

Article 515 : Tromperie

Quiconque utilise les éléments d'identification d'une personne physique ou morale dans le but de tromper les destinataires d'un message électronique ou les usagers d'un site internet en vue de les amener à communiquer des données à caractère personnel ou des informations

confidentielles est puni d'un emprisonnement de cinq (5) ans et d'une amende de vingt cinq millions (25 000 000) de francs CFA.

Article 516 : Détournement de fonds

Quiconque utilisera des données à caractère personnel ou des informations confidentielles communiquées dans le but de détourner des fonds publics ou privés est puni d'un emprisonnement de dix (10) ans et d'une amende de cent millions (100 000 000) de francs CFA.

Article 517 : Traitement non autorisé

Quiconque aura procédé à un traitement de données à caractère personnel soit sans avoir préalablement informé individuellement les personnes concernées de leur droit d'accès, de rectification ou d'opposition, de la nature des données transmises et des destinataires de celles-ci, soit malgré l'opposition de la personne concernée est puni selon les peines prévues à l'article 454 du présent code.

CHAPITRE V

DES ATTEINTES AUX PERSONNES ET AUX BIENS

SECTION I

DE LA PROTECTION DES MINEURS

Article 518 : Pédopornographie

Quiconque aura par le biais d'un système informatique, intentionnellement et sans droit, exposé, produit pour lui-même ou pour autrui, vendu, offert, loué, distribué, transmis, diffusé, publié ou mis à la disposition des emblèmes, objets, films, photos, diapositives ou autres supports visuels qui représentent des positions ou des actes sexuels à caractère pornographique, impliquant ou présentant des mineurs ou les aura, en vue du commerce ou de la distribution, la diffusion, fabriqués, détenus, importés ou fait importer, remis à un agent de transport ou de distribution, est puni de la réclusion de deux (02) ans à sept (7) ans et d'une amende de vingt millions (20 000 000) à cent millions (100 000 000) de francs CFA.

Quiconque acquiert, détient ou aura possédé au sens du présent code, intentionnellement et sans droit, de la pornographie enfantine au sens du présent code dans un système informatique ou un moyen de stockage de données informatique, est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende de cinquante millions (50 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque consulte habituellement ou en contrepartie d'un paiement un service de communication au public en ligne mettant à disposition de la pornographie enfantine au sens du présent code, par quelque moyen que ce soit est puni de dix (10) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende.

Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur et dont l'objectif est de faire passer la personne comme un mineur et ce même s'il est établi que cette personne était âgée de dix-huit (18) ans au jour de la fixation ou de l'enregistrement de son image.

La confiscation peut être appliquée à l'égard des infractions visées aux alinéas 1 et 2, même lorsque la propriété des choses sur lesquelles portent l'infraction n'appartiennent pas au condamné.

Légi Bénin

La responsabilité pénale de l'auteur n'est pas en cause lorsque l'acte est commis dans un objectif de répression de la pédopornographie.

Une interdiction, telle que prévue par le code pénal, peut être prononcée par les tribunaux à titre de peine complémentaire.

Une interdiction à titre provisoire ou définitive de fréquenter certains endroits, établissements à qui l'on confie la garde des mineurs ou d'exercer certaines activités à même de mettre le condamné en rapport avec des mineurs, peut être prononcée par les tribunaux. Cette interdiction est prolongée en cas de récidive.

Sans avoir égard à la qualité de la personne physique ou morale de l'exploitant, propriétaire, locataire ou gérant, le tribunal peut ordonner la fermeture de l'établissement dans lequel les infractions ont été commises, pour une durée de un (01) mois à trois (03) ans.

Article 519 : Sollicitation de mineurs à des fins sexuelles

Un adulte qui propose intentionnellement, par le biais des technologies de communication et d'information, une rencontre à un enfant mineur, dans le but de commettre à son encontre une des infractions visées à l'article 518, est puni des mêmes peines que celles prévues à l'article 518, alinéa 1er.

Lorsque la proposition sexuelle a été suivie d'actes matériels conduisant à ladite rencontre, l'auteur commet une infraction aggravée et est puni de la réclusion criminelle à temps de dix (10) ans à vingt (20) ans et d'une amende de cent millions (100 000 000) à cinq cent millions (500 000 000) de francs CFA ou de l'une de ces peines seulement.

Article 520 : Facilitation de l'accès des mineurs à des contenus pornographiques

Une personne qui facilite l'accès des mineurs à des images, des documents, du son ou une représentation présentant un caractère de pornographie, par le biais des technologies de communication et d'information, est punie des mêmes peines que celles prévues par les dispositions du code pénal relatives à la corruption de la jeunesse.

Quiconque fabrique, transporte, diffuse par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine ou à inciter des mineurs à se livrer à des jeux les mettant physiquement en danger, soit de faire commerce d'un tel message, est puni des mêmes peines que celles prévues par les dispositions du code pénal relatives à la corruption de la jeunesse.

Lorsque les infractions prévues à l'alinéa précédent sont soumises par la voie de la presse écrite ou audiovisuelle ou de la communication au public en ligne, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

Article 521 : Délit de corruption de mineur

Quiconque favorisera la corruption d'un mineur au moyen d'un ou sur un réseau de communication électronique ou un système informatique est puni de dix (10) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende. Ces peines sont portées à douze (12) ans d'emprisonnement et trente cinq millions (35 000 000) de francs CFA d'amende lorsque les faits sont commis dans les établissements d'enseignement ou d'éducation ou dans les locaux de l'administration, ainsi que, lors des entrées ou sorties des élèves ou du public ou dans un temps très voisin de celles-ci, aux abords de ces établissements ou locaux.

LEGI-BOOK

Les peines sont portées à quinze (15) ans d'emprisonnement et cinquante millions (50 000 000) de francs CFA d'amende lorsque les faits ont été commis à l'encontre d'un mineur de moins de quinze (15) ans.

Article 522 : Prostitution de mineurs

Le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations de nature sexuelle de la part d'un mineur qui se livre à la prostitution, y compris de façon occasionnelle, est puni de vingt (20) ans d'emprisonnement et cinquante millions (50 000 000) de francs CFA d'amende lorsque la personne a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

SECTION II

DES INFRACTIONS SEXUELLES ET PROSTITUTION

Article 523 : Viol

Le viol est puni de vingt (20) ans de réclusion criminelle et de cinquante millions (50 000 000) de francs CFA d'amende lorsque la victime a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 524 : Infractions sexuelles

Les agressions sexuelles autres que le viol sont punies de dix (10) ans d'emprisonnement et vingt cinq millions (25 000 000) de francs CFA d'amende lorsque la victime a été mise en contact avec l'auteur des faits au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 525 : Prostitution des personnes vulnérables

Est puni des peines prévues à l'article 522 le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération ou d'une promesse de rémunération, des relations sexuelles de la part d'une personne qui se livre à la prostitution, y compris de façon occasionnelle, lorsque cette personne présente une particulière vulnérabilité, apparente ou connue de son auteur, due à une maladie, à une infirmité, à une déficience physique ou psychique ou à un état de grossesse.

SECTION III

DE LA FRAUDE AUX CARTES BANCAIRES

Article 526: Fraude aux cartes bancaires

Est puni de cinq (5) ans d'emprisonnement et d'une amende de dix millions (10 000 000) de francs CFA, le fait pour toute personne :

1- de contrefaire ou de falsifier une carte de paiement ou de retrait au moyen d'un ou sur un réseau de communication électronique ou un système informatique ;

2- de faire usage, en connaissance de cause, d'une carte de paiement ou de retrait contrefaite ou falsifiée au moyen d'un ou sur un réseau de communication électronique ou un système informatique ;

Bénin

3- d'accepter, en connaissance de cause, de recevoir un paiement au moyen d'une carte de paiement contrefaite ou falsifiée au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Est puni de huit (8) ans d'emprisonnement et de dix millions (10 000 000) de francs CFA d'amende, le fait pour toute personne, de fabriquer, d'acquérir, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés pour commettre les infractions prévues à l'alinéa 1er.

La confiscation, aux fins de destruction des cartes de paiement contrefaits ou falsifiés est obligatoire dans les cas prévus ci-dessus. Est également obligatoire la confiscation des matières, machines, appareils, instruments, programmes informatiques ou de toutes données qui ont servi ou étaient destinés à servir à la fabrication desdits objets, sauf lorsqu'ils ont été utilisés à l'insu du propriétaire.

Dans tous les cas prévus aux alinéas ci-dessus, le tribunal peut prononcer l'interdiction des droits civiques, civils et de famille ainsi que l'interdiction, pour une durée de cinq (5) ans au plus, d'exercer une activité professionnelle ou sociale.

CHAPITRE VI

DES AUTRES INFRACTIONS

Article 527 : Enregistrement d'images relatives à la commission d'infractions

Est constitutif d'un acte de complicité des atteintes volontaires à l'intégrité de la personne, le fait d'enregistrer sciemment, par quelque moyen que ce soit, sur tout support que ce soit, des images relatives à la commission d'infractions.

Le fait de diffuser l'enregistrement de telles images est puni de cinq (5) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende.

Le présent article n'est pas applicable lorsque l'enregistrement ou la diffusion résulte de l'exercice normal d'une profession ayant pour objet d'informer le public ou est réalisé afin de servir de preuve en justice.

Article 528 : Eléments pour fabriquer des engins de destruction

Le fait de diffuser, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, sauf à destination des professionnels, des procédés permettant la fabrication d'engins de destruction élaborés à partir de poudre ou de substances explosives, de matières nucléaires, biologiques ou chimiques, ou à partir de tout autre produit destiné à l'usage domestique, industriel ou agricole, est puni de dix (10) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende.

Lorsque ces procédés ont permis la commission de meurtre ou d'assassinat, la peine est de vingt (20) ans d'emprisonnement et d'une amende de cinquante millions (50 000 000) à cent millions (100 000 000) de francs CFA.

CHAPITRE VII

DE L'ATTEINTE AUX DROITS DE LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

LégiBénin

Article 529 : Dispositions existantes

Les dispositions du présent chapitre viennent compléter les dispositions de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins en République du Bénin.

Article 530 : Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

A l'article 2 de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins en République du Bénin, sont apportées les modifications suivantes :

«L'auteur de toute œuvre originale de l'esprit, littéraire ou artistique, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle, exclusif à tous et opposable à tous».

A l'article 8 de la loi n° 2005-30 du 10 avril 2006 relative à la protection des droits d'auteurs et des droits voisins en République du Bénin, sont apportées les modifications suivantes :

« Constituent les œuvres de l'esprit protégées par la présente loi :

- (…)
- les logiciels, y compris le matériel de conception préparatoire ;
- (…) ».

SECTION I

DE L'ATTEINTE AUX DROITS DE PROPRIETE INTELLECTUELLE

Article 531 : Sanctions

Sont punis d'une peine d'emprisonnement de trois (03) mois à deux (02) ans et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de FCFA, les atteintes à la propriété intellectuelle commises au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 532 : Oeuvres de l'esprit

Constitue une atteinte à la propriété intellectuelle, le fait, sans autorisation de l'auteur ou de ses ayants droit de reproduire, représenter ou de mettre à la disposition du public une œuvre de l'esprit protégée par le droit d'auteur ou un droit voisin au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 533 : Contrefaçon de marque, nom commercial, appellation d'origine, indication géographique

Constitue une atteinte à la propriété intellectuelle, le fait sans autorisation de l'auteur ou de ses ayants droit, de reproduire, d'utiliser, de vendre, de dénigrer, de dénaturer une marque, un nom commercial, une appellation d'origine ou une indication géographique appartenant à un tiers au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 534 : Contrefaçon de dessins et modèles

Constitue une atteinte à la propriété intellectuelle, le fait, sans autorisation de l'auteur ou de ses ayants droit de reproduire, de représenter ou de mettre à la disposition du public, un dessin ou un modèle protégé par le droit d'auteur ou un droit voisin au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

LégiBenin

Article 535 : Atteinte aux droits de propriété des brevets

Constitue une atteinte à la propriété intellectuelle le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation, un bien ou un produit protégé par un brevet d'invention au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 536 : Atteinte aux schémas de configuration de circuits intégrés

Constitue une atteinte à la propriété intellectuelle, le fait, en toute connaissance de cause, sans droit, de vendre ou de mettre à disposition du public par reproduction ou par représentation un schéma de configuration de circuits intégrés au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 537 : Atteinte à une mesure technique efficace

Est puni de sept cent mille (700 000) francs CFA d'amende, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace afin d'altérer la protection d'une œuvre par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant.

Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace, par l'un des procédés suivants :

1- en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ;

2- en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit, une application technologique, un dispositif ou un composant ;

3- en fournissant un service à cette fin ;

4- en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3 au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique.

Article 538 : Suppression d'un élément d'information sur le régime des droits pour porter atteinte au droit d'auteur

Est puni de sept cent mille (700 000) francs CFA d'amende, le fait de supprimer ou de modifier, sciemment et à des fins autres que la recherche, tout élément d'information sur le régime des droits, par une intervention personnelle ne nécessitant pas l'usage d'une application technologique, d'un dispositif ou d'un composant existant, conçus ou spécialement adaptés à cette fin, dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte.

Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour supprimer ou modifier, même partiellement, un

Legibenin

élément d'information sur le régime des droits, dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte, par l'un des procédés suivants :

1- en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ;

2- en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ;

3- en fournissant un service à cette fin ;

4- en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3 au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait sciemment, d'importer, de distribuer, de mettre à disposition du public sous quelque forme que ce soit ou de communiquer au public, directement ou indirectement, une œuvre dont un élément d'information sur le régime des droits a été supprimé ou modifié dans le but de porter atteinte à un droit d'auteur, de dissimuler ou de faciliter une telle atteinte.

Ces dispositions ne sont pas applicables aux actes réalisés à des fins de recherche ou de sécurité informatique.

Article 539 : Altération

Est puni de sept cent mille (700 000) francs CFA d'amende, le fait de porter atteinte sciemment, à des fins autres que la recherche, à une mesure technique efficace afin d'altérer la protection d'une interprétation, d'un phonogramme, d'un vidéogramme ou d'un programme par un décodage, un décryptage ou toute autre intervention personnelle destinée à contourner, neutraliser ou supprimer un mécanisme de protection ou de contrôle, lorsque cette atteinte est réalisée par d'autres moyens que l'utilisation d'une application technologique, d'un dispositif ou d'un composant existant mentionné au chapitre II du présent Livre.

Est puni de six (6) mois d'emprisonnement et de cinq cent mille (500 000) francs CFA d'amende, le fait de procurer ou proposer sciemment à autrui, directement ou indirectement, des moyens conçus ou spécialement adaptés pour porter atteinte à une mesure technique efficace, par l'un des procédés suivants :

1- en fabriquant ou en important une application technologique, un dispositif ou un composant, à des fins autres que la recherche ;

2- en détenant en vue de la vente, du prêt ou de la location, en offrant à ces mêmes fins ou en mettant à disposition du public sous quelque forme que ce soit une application technologique, un dispositif ou un composant ;

3- en fournissant un service à cette fin ;

4- en incitant à l'usage ou en commandant, concevant, organisant, reproduisant, distribuant ou diffusant une publicité en faveur de l'un des procédés visés aux points 1 à 3.

Ces dispositions ne sont pas applicables aux actes réalisés à des fins de sécurité informatique.

SECTION II

Légibenin

DES MOYENS D'ECHANGE ILLICITE ET TELECHARGEMENT SUR INTERNET

Article 540 : Personnes facilitant sur les réseaux, les échanges illicites d'éléments protégés

Est puni de trois (3) ans d'emprisonnement et de trois millions (3 000 000) de francs CFA d'amende, le fait :

1- d'éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés ;

2- d'inciter sciemment, y compris à travers une annonce publicitaire, à l'usage d'un logiciel mentionné au point 1, au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 541 : Atteinte aux droits d'auteur par un service de communication au public en ligne

En présence d'une atteinte à un droit d'auteur ou à un droit voisin occasionnée par le contenu d'un service de communication au public en ligne, le tribunal de première instance, peut ordonner à la demande des titulaires de droits sur les œuvres et objets protégés, de leurs ayants droit, toutes mesures propres à prévenir ou à faire cesser une telle atteinte à un droit d'auteur ou un droit voisin, à l'encontre de toute personne susceptible de contribuer à y remédier.

Article 542 : Obligation de l'abonné internet de veiller à ce que son accès internet ne fasse pas l'objet d'une utilisation type téléchargement illicite

La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits lorsqu'elle est requise.

Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles 544 et 545 ci-dessous.

Article 543 : En cas de téléchargement illicite : réponse graduée

En cas d'infraction définie à l'article 542 ci-dessus, l'organe national en charge du droit d'auteur et des droits voisins peut envoyer à l'abonné, sous son timbre et pour son compte, par la voie électronique et par l'intermédiaire de la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne ayant conclu un contrat avec l'abonné, une recommandation lui rappelant les dispositions de l'article ci-dessous, lui enjoignant de respecter l'obligation qu'elles définissent et l'avertissant des sanctions encourues. Cette recommandation contient également une information de l'abonné sur l'offre légale de contenus culturels en ligne, sur l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article ci-dessus ainsi que sur les dangers pour le renouvellement de la création artistique et pour l'économie du secteur culturel des pratiques ne respectant pas le droit d'auteur et les droits voisins.

En cas de renouvellement, dans un délai de six (6) mois à compter de l'envoi de la recommandation visée au 1er alinéa, de faits susceptibles de constituer un manquement à l'obligation définie à l'article ci-dessus, le Bureau béninois du droit d'auteur peut adresser une nouvelle recommandation comportant les mêmes informations que la précédente par la voie

électronique dans les conditions prévues au 1er alinéa. Elle doit assortir cette recommandation d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation de cette recommandation.

Les recommandations adressées sur le fondement du présent article mentionnent la date et l'heure auxquelles les faits susceptibles de constituer un manquement à l'obligation définie à l'article ci-dessus ont été constatés. En revanche, elles ne divulguent pas le contenu des œuvres ou objets protégés concernés par ce manquement. Elles indiquent les coordonnées téléphoniques, postales et électroniques où leur destinataire peut adresser, s'il le souhaite, des observations au Bureau de droit d'auteur et droit voisin et obtenir, s'il en formule la demande expresse, des précisions sur le contenu des œuvres ou objets protégés concernés par le manquement qui lui est reproché.

Article 544 : Sanctions du téléchargement illicite

Lorsque l'infraction définie à l'article 542 est commise au moyen d'un service de communication au public en ligne, les personnes coupables des infractions de contrefaçons peuvent en outre être condamnées à la peine complémentaire d'une amende de un million (1 000 000) de francs CFA.

Lorsque ce service est acheté selon des offres commerciales composites incluant d'autres types de services, tels que services de téléphonie ou de télévision, les décisions d'amende ne s'appliquent pas à ces services.

La prononciation de l'amende n'affecte pas, par elle-même, le versement du prix de l'abonnement au fournisseur du service.

Article 545 : Négligence caractérisée

La peine complémentaire définie à l'article précédent peut être prononcée selon les mêmes modalités, en cas de négligence caractérisée définie ci-dessous, à l'encontre du titulaire de l'accès à un service de communication au public en ligne auquel le Bureau béninois du droit d'auteur et droits voisins a préalablement adressé, par voie d'une lettre remise contre signature ou de tout autre moyen propre à établir la preuve de la date de présentation, une recommandation l'invitant à mettre en œuvre un moyen de sécurisation de son accès à internet.

La négligence caractérisée s'apprécie sur la base des faits commis au plus tard un (1) an après la présentation de la recommandation mentionnée à l'alinéa précédent.

Dans ce cas, l'amende maximale est de cinq cent mille (500 000) francs CFA.

Article 546 : Définition de la négligence caractérisée

Constitue une négligence caractérisée le fait, sans motif légitime, pour la personne titulaire d'un accès à des services de communication au public en ligne :

1- soit de ne pas avoir mis en place un moyen de sécurisation de cet accès ;

2- soit d'avoir manqué de diligence dans la mise en œuvre de ce moyen.

Les dispositions de l'alinéa 1er ne sont applicables que lorsque se trouvent réunies les deux conditions suivantes :

- lorsque le titulaire de l'accès s'est vu recommander par le Bureau béninois du droit d'auteur et des droits voisins de mettre en œuvre un moyen de sécurisation de son accès permettant de prévenir le renouvellement d'une utilisation de celui-ci à des fins de reproduction, de

Légi-Bénin

représentation ou de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits ;

- dans l'année suivant la présentation de cette recommandation, cet accès est à nouveau utilisé aux fins mentionnées au point 1 du présent alinéa.

CHAPITRE VIII

DES INFRACTIONS RELATIVES A LA PUBLICITE SUR INTERNET

Article 547 : Publicité en faveur des jeux d'argent et de hasard illicites

Le fait de faire de la publicité au moyen d'un ou sur un réseau de communication électronique ou un système informatique en faveur de jeux d'argent et de hasard sur internet non autorisés est interdit.

Quiconque contrevient à l'interdiction définie à l'alinéa précédent, est puni d'une amende de cinq cent mille (500 000) francs CFA.

La juridiction compétente peut porter le montant de l'amende au quadruple du montant des dépenses publicitaires consacrées à l'opération illégale.

CHAPITRE IX

DES CONTENUS ABUSIFS ET INFRACTIONS

DE PRESSE EN LIGNE

Légi Bénin

Article 548 : Diffusion de matériel raciste et xénophobe par le biais d'un système informatique.

Quiconque, intentionnellement, crée, télécharge, diffuse ou met à disposition sous quelque forme que ce soit, par le biais d'un système informatique du matériel raciste et xénophobe, au sens du présent code, est puni d'un emprisonnement de six (06) mois à sept (07) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA.

Article 549 : Menace avec une motivation raciste et xénophobe par le biais d'un système informatique

Quiconque profère, intentionnellement, une menace par le biais d'un système informatique, de commettre une infraction pénale telle que définie par le code pénal, envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou à un groupe de personnes qui se distingue par une de ces caractéristiques est puni d'un emprisonnement de six (06) mois à sept (07) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA.

Article 550 : Harcèlement par le biais d'une communication électronique

Quiconque initie une communication électronique qui contraint, intimide, harcèle ou provoque une détresse émotionnelle chez une personne, en utilisant un système informatique dans le but d'encourager un comportement grave, répété et hostile est puni d'une peine d'emprisonnement de un (01) mois à deux (02) ans et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de francs CFA, ou de l'une de ces deux peines seulement.

Quiconque aura harcelé, par le biais d'une communication électronique, une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée, est puni d'une peine d'emprisonnement de un (01) mois à deux (02) ans et d'une amende de cinq cent mille (500 000) francs CFA à dix millions (10 000 000) de FCFA, ou de l'une de ces deux peines seulement.

Quiconque initie ou relaie une fausse information contre une personne par le biais des réseaux sociaux ou toute forme de support électronique est puni d'une peine d'emprisonnement d'un (01) mois à six (06) mois et d'une amende de cinq cent mille (500 000) francs CFA à un million (1 000 000) de francs CFA, ou de l'une de ces peines seulement.

Si les faits visés aux alinéas 1 et 2 sont commis au préjudice d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits, les peines minimales prévues aux alinéas précédents seront doublées.

Article 551 : Injure avec une motivation raciste et xénophobe commise par le biais d'un système informatique

Quiconque profère, intentionnellement, une insulte publique par le biais d'un système informatique envers une personne en raison de son appartenance à un groupe qui se caractérise par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion ou l'opinion politique dans la mesure où cette appartenance sert de prétexte à l'un ou l'autre de ces éléments, ou un groupe de personnes qui se distingue par une de ces caractéristiques est puni d'un emprisonnement de six (06) mois à sept (07) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA.

Article 552 : Incitation à la haine et à la violence

Quiconque aura provoqué à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de l'appartenance à une race, à une couleur, à une origine nationale ou ethnique, à la religion, à l'appartenance sexuelle, ou à un handicap au moyen d'un ou sur un réseau de communication électronique ou un système informatique, est puni de un (01) an d'emprisonnement et de cinq millions (5 000 000) de francs CFA d'amende ou de l'une de ces deux peines seulement.

Article 553 : Incitation à la rébellion

La provocation directe à la rébellion au moyen d'un ou sur un réseau de communication électronique ou un système informatique est punie de six (06) mois d'emprisonnement et de deux millions (2 000 000) à dix millions (10 0000 000) de francs CFA d'amende.

Article 554 : Provocation de crime ou de délit

Seront punis comme complices d'une action qualifiée de crime ou de délit, ceux qui au moyen d'un ou sur un réseau de communication électronique ou un système informatique auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet.

Article 555 : Incitation à la commission d'une infraction

Seront punis de un (01) an d'emprisonnement et de cinq millions (5 000 000) de francs CFA d'amende, ceux qui, par l'un des moyens énoncés à l'article précédent, auront directement provoqué, dans le cas où cette provocation n'aurait pas été suivie d'effet, à commettre l'une des infractions suivantes au moyen d'un ou sur un réseau de communication électronique ou un système informatique :

1- les atteintes à la vie de la personne, les atteintes à l'intégrité physique de la personne et les agressions sexuelles, définies par le code pénal ;

2- les vols, les extorsions dangereuses pour les personnes, définis par le code pénal.

Article 556 : Négation, minimisation grossière, approbation ou justification d'un génocide ou de crimes contre l'humanité

Une personne qui diffuse ou met à disposition par le biais d'un système informatique des données qui nient, minimisent de manière grossière, approuvent ou justifient des actes constitutifs de génocide ou de crimes contre l'humanité tels que définis par le droit international et reconnus comme tels par une décision finale et définitive d'un tribunal national ou d'un tribunal international établi par des instruments internationaux pertinents et dont la juridiction est reconnue, est punie d'un emprisonnement de six (06) mois à sept (07) ans et d'une amende de un million (1 000 000) à dix millions (10 000 000) de francs CFA.

Article 557: Incitation ou provocation à la commission d'actes terroristes et apologie des actes terroristes

Quiconque aura, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, incité ou provoqué directement des actes de terrorisme est puni de dix (10) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende.

Article 558 : Infractions de presse par le biais d'une communication électronique

Une personne qui commet une infraction de presse, notamment une diffamation, une injure publique, une apologie de crime, par le biais d'un moyen de communication électronique public, est punie des mêmes peines que celles prévues par la loi n° 2015-07 du 20 mars 2015 portant code de l'information et de la communication en vigueur, quel qu'en soit le support.

Article 559 : Droit de réponse

Toute personne nommée ou désignée au moyen d'un ou sur un réseau de communication électronique ou un système informatique, dispose d'un droit de réponse, sans préjudice des demandes de correction ou de suppression du message qu'elle peut adresser au service.

Elle est présentée au plus tard dans un délai de trois (3) mois à compter de la mise à disposition du public du message justifiant cette demande.

Le directeur de la publication est tenu d'insérer dans les trois (3) jours de leur réception, les réponses de toute personne nommée ou désignée dans le service de communication au public en ligne sous peine d'une amende de cinq cent mille (500 000) francs CFA.

Article 560 : Divulgation des détails d'une enquête

Est puni d'un emprisonnement de un (01) mois à deux (02) ans, ou d'une amende maximale de cinq millions (5 000 000) de francs CFA ou de l'une de ces peines seulement, un fournisseur de services qui, dans le cadre d'une enquête pénale, reçoit une injonction stipulant explicitement que la confidentialité doit être maintenue, ou lorsqu'une telle obligation est énoncée par la loi, et qui, sans motif ou justification légitime, ou en se prévalant à tort d'un motif ou d'une justification légitime, divulgue de manière intentionnelle :

1- le fait qu'une injonction ait été émise ;

2- toute action réalisée aux termes de l'injonction ; ou

3- toute donnée collectée ou enregistrée aux termes de l'injonction.

Légi-Bénin

L'obligation de confidentialité prévue à l'alinéa 1 ne s'applique pas en cas de :

- consentement exprès de l'auteur ou du destinataire de la communication ;
- interception d'une communication privée sur mandat de justice.

CHAPITRE X

DES INFRACTIONS DE DROIT COMMUN COMMISES EN LIGNE

Article 561 : Vol de données informatiques

Une personne qui copie, intentionnellement et sans droit, avec une intention frauduleuse des données informatiques au préjudice d'un tiers est puni des mêmes peines que celles prévues dans les dispositions du code pénal relatives au vol.

Article 562 : Usurpation d'identité

Quiconque usurpe, intentionnellement et sans droit par le biais d'un système informatique, l'identité d'un tiers ou une ou plusieurs données permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur, à sa considération ou à ses intérêts, est puni d'un emprisonnement de un (01) an à cinq (05) ans et d'une amende de cinq millions (5 000 000) à cent millions (100 000 000) de francs CFA ou de l'une de ces peines seulement.

Quiconque, intentionnellement et sans droit, ou en se prévalant à tort d'un motif ou d'une justification légitime, en utilisant un système informatique à tout stade de l'infraction, transfère, possède ou utilise un moyen d'identifier une autre personne dans l'intention de commettre, d'aider ou d'encourager une activité illégale quelconque constituant un délit ou un crime, ou dans le cadre d'une telle activité, est puni d'un emprisonnement de un (01) an à cinq (05) ans et d'une amende de cinq millions (5 000 000) à cent millions (100 000 000) de francs CFA ou de l'une de ces peines seulement.

Si les faits visés aux alinéas précédents ont été commis au préjudice d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits, les peines minimales prévues aux alinéas précédents seront doublées.

Article 563 : Recel

Est puni d'un emprisonnement de cinq (05) ans à dix (10) ans et de cinq millions (5 000 000) à dix millions (10 000 000) de francs CFA d'amende, le fait pour toute personne, au préjudice des droits d'autrui, de détenir, d'utiliser ou de transmettre une chose en sachant que celle-ci provient d'une infraction au moyen d'un ou sur un réseau de communication électronique ou un système informatique. Est punie des mêmes peines, le fait pour toute personne, dans les mêmes conditions, de faire office d'intermédiaire afin de transmettre la chose.

Article 564 : Aggravation

Les peines sont portées à dix (10) ans d'emprisonnement et à vingt cinq millions (25 000 000) de francs CFA d'amende lorsque la personne se livre au recel au moyen d'un ou sur un réseau de communication électronique ou un système informatique, de manière habituelle ou lorsqu'elle s'y livre à l'occasion de l'exercice de sa profession.

Legi-Benin

Article 565 : Recel portant sur des données informatiques

Une personne qui, intentionnellement et sans droit, aura gardé, retenu ou détenu en tout ou en partie, des données informatiques enlevées, détournées ou obtenues à l'aide d'un crime ou d'un délit prévu par les dispositions du présent Livre, est punie des mêmes peines que celles prévues à l'article 563.

Dans les cas où le fait qui a procuré les objets recelés a été commis avec une ou plusieurs circonstances aggravantes, le receleur est puni des peines définies par les dispositions du présent Livre s'il est établi qu'il était au courant desdites circonstances.

L'amende pourra être élevée au-delà des dix millions (10 000 000) de francs CFA ou jusqu'à la moitié de la valeur des objets recélés.

Article 566 : Escroquerie

Quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses quelconques, se fait remettre ou délivrer des biens et valeurs par le biais d'un système informatique ou d'un réseau de communication électronique et a par un de ces moyens, escroqué tout ou partie de la fortune d'autrui est puni d'un emprisonnement de deux (02) ans à sept (07) ans et d'une amende égale au quintuple de la valeur mise en cause sans qu'elle soit inférieure à un million (1 000 000) de francs CFA.

Quiconque, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des manœuvres frauduleuses pour persuader de l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, pour faire naître l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique, ou pour abuser autrement de la confiance ou de la crédulité se sera fait remettre ou délivrer des données informatiques, et a par un de ces moyens escroqué tout ou partie de la fortune d'autrui, est puni d'un emprisonnement de deux (02) ans à sept (07) ans et d'une amende égale au quintuple de la valeur mise en cause sans qu'elle soit inférieure à un million (1 000 000) de francs CFA.

Les peines d'emprisonnement sont portées de dix (10) ans à vingt (20) ans et l'amende au quintuple de la valeur mise en cause sans qu'elle soit inférieure à vingt cinq millions (25 000 000) de francs CFA lorsque l'escroquerie est réalisée :

1- par un dépositaire de l'autorité publique ou un chargé de service public, dans l'exercice ou à l'occasion de ses fonctions ;

2- par une personne qui prend indûment la qualité de dépositaire de l'autorité publique ou chargé de service public ;

3- par une personne ayant fait appel au public en vue de l'émission d'actions, obligations, bons, parts ou titres quelconques soit d'une société, soit d'une entreprise commerciale ou industrielle ;

4- au préjudice d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits.

Les coupables d'infractions visées aux alinéas précédents peuvent se voir prescrire une interdiction, à titre de peine complémentaire, par les tribunaux compétents au sens de l'article 583 du présent code.

Article 567 : Infractions voisines de l'escroquerie

Togo Bénin

Est puni de trois millions (3 000 000) de francs CFA d'amende, le fait de vendre, d'offrir à la vente ou d'exposer en vue de la vente ou de la cession ou de fournir les moyens en vue de la vente ou de la cession au moyen d'un ou sur un réseau de communication électronique ou un système informatique, des titres d'accès à une manifestation sportive, culturelle ou commerciale ou à un spectacle vivant, de manière habituelle et sans l'autorisation du producteur, de l'organisateur, ou du propriétaire des droits d'exploitation de cette manifestation ou de ce spectacle.

Article 568 : Abus de confiance

Est puni des mêmes peines que celles prévues dans les dispositions du code pénal relatives à l'abus de confiance, le fait pour une personne, au moyen d'un ou sur un réseau de communication électronique ou un système informatique de détourner, au préjudice d'autrui, une chose quelconque qui lui a été remise au titre de l'un des contrats prévus par le code pénal relatif à l'abus de confiance et qu'elle a acceptée à charge de la rendre, de la représenter ou d'en faire un usage déterminé.

Article 569 : Abus de confiance sur des données informatiques

Quiconque ayant reçu des propriétaires, possesseurs, ou détenteurs, des données informatiques à titre de louage, de dépôt, de mandat, de nantissement, de prêt à usage ou pour un travail salarié ou non salarié, n'aura pas, après mise en demeure, exécuté son engagement de les rendre ou représenter ou d'en faire un usage ou un emploi déterminé, est puni des mêmes peines que celles prévues pour l'abus de confiance portant sur des biens corporels par les dispositions du code pénal.

Si les faits visés à l'alinéa précédent ont été commis en abusant des besoins, des faiblesses, des passions ou de l'ignorance d'un mineur ou d'une personne dont la situation de vulnérabilité en raison de l'âge, d'un état de grossesse, d'une maladie, d'une infirmité ou d'une déficience physique ou mentale était apparente ou connue de l'auteur des faits, les peines minimales prévues à l'alinéa précédent seront doublées.

Article 570 : Extorsion

Est puni de un (01) an à cinq (05) ans d'emprisonnement et de cinq cent mille (500 000) francs CFA à cinq millions (5 000 000) de francs CFA d'amende, le fait d'extorquer par violence, menace de violence ou contrainte, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'une chose quelconque au moyen d'un ou sur un réseau de communication électronique ou un système informatique.

Article 571 : Chantage

Quiconque extorque, en menaçant de révéler ou d'imputer des faits de nature à porter atteinte à l'honneur ou à la considération, soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'une chose quelconque au moyen d'un ou sur un réseau de communication électronique ou un système informatique, est puni de six (6) ans d'emprisonnement et de cinq millions (5 000 000) de francs CFA d'amende.

Article 572 : Jeux de hasard illicite en ligne

Quiconque, sans l'autorisation d'une autorité publique, organise publiquement ou propose un jeu de hasard ou met à disposition l'équipement nécessaire, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, est puni d'une peine d'emprisonnement de un (01) mois à trois (03) ans et d'une amende de cinq cent mille (500 000)

Legibenin

francs CFA à cinquante millions (50 000 000) de francs CFA, ou de l'une de ces peines seulement.

Les jeux de hasard sans autorisation d'une autorité publique, en club ou en réunion privée dans lesquels les jeux de hasard sont régulièrement organisés, sont qualifiés de jeux organisés publiquement.

Est puni d'un emprisonnement de trois (03) mois à cinq (05) ans et d'une amende de un million (1 000 000) à cent millions (100 000 000) de francs CFA, ou de l'une de ces peines seulement, quiconque, dans les cas mentionnés à l'alinéa 1er agit :

1- professionnellement ;

2- en tant que membre d'un groupe qui s'est constitué pour commettre en permanence de tels actes,

Quiconque recrute pour un jeu de hasard public est puni d'une peine d'une durée maximale d'un (01) an ou d'une amende ne dépassant pas cinquante millions (50 000 000) de francs CFA, ou de l'une de ces peines seulement.

Quiconque participe à un jeu de hasard public, est puni d'une peine de prison d'une durée maximale de six (06) mois et d'une amende de un million (1 000 000) à deux cent millions (200 000 000) de francs CFA, ou de l'une de ces peines seulement.

Article 573 : Blanchiment de capitaux

Le blanchiment de capitaux commis au moyen d'un ou sur un réseau de communication électronique ou un système informatique est puni conformément aux textes en vigueur.

Article 574 : Atteinte à la vie privée commise sur internet

Est puni de cinq (5) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende, le fait, au moyen d'un ou sur un réseau de communication électronique ou un système informatique, de volontairement porter atteinte à l'intimité de la vie privée d'autrui :

1- en captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2- en fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Article 575 : Atteinte au secret des correspondances commises sur internet

Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances émises, transmises ou reçues par la voie électronique arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni des mêmes peines que celles prévues dans les dispositions du code pénal relatives au secret des correspondances.

Est puni des mêmes peines, le fait de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.

Article 576 : Atteinte à la représentation de la personne

Legibenin

Est puni de cinq (5) ans d'emprisonnement et de vingt cinq millions (25 000 000) de francs CFA d'amende, le fait de publier sur internet, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention.

CHAPITRE XI

DE LA CONSTITUTION DES INFRACTIONS ET DES AMENAGEMENTS PARTICULIERS

SECTION I

DE LA CONSTITUTION ET DE LA CONSTATATION DES INFRACTIONS

Article 577 : Mode de preuve électronique

L'écrit sous forme électronique, en application du Livre II, est, pour les besoins de l'application du présent Livre, admis en preuve au même titre que l'écrit sur support papier et possède la même force probante que celui-ci, sous réserve que puisse être dûment identifié la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité et la pérennité.

Article 578 : La constatation et la poursuite des infractions

Les infractions prévues au présent Livre sont constatées et poursuivies conformément aux dispositions du code de procédure pénale et du présent code.

Article 579 : Prescription

Les règles et principes du code pénal relatifs à la prescription s'appliquent aux infractions visées au Titre I du présent Livre.

SECTION II

DES AUTEURS, CO-AUTEURS ET COMPLICES D'INFRACTIONS

Article 580 : Tentative

Le fait de tenter de commettre l'une des infractions visées au Titre I du présent Livre, est puni des mêmes peines.

Article 581 : Complice

Le fait d'inciter à commettre l'une des infractions visées au Titre I du présent Livre, d'y participer ou de s'en rendre complice est puni des mêmes peines.

Article 582 : Récidive

Legi-Bénin

Lorsqu'une des infractions visées au Titre I du présent Livre est commise dans les cinq (5) ans qui suivent le prononcé de la condamnation irrévocable pour l'une de ces infractions, la ou les peines sont doublées.

En cas de multiplicité d'infractions commises par le même contrevenant, l'amende prévue pour chaque infraction est appliquée autant de fois qu'il y a d'infractions distinctes constatées.

Article 583 : Circonstances aggravantes

Lorsqu'une infraction est commise par un membre d'une organisation criminelle ou d'une bande organisée en vue de commettre des infractions pénalement répressibles, la peine initialement prévue est doublée pour l'infraction elle-même ou si plusieurs infractions sont commises pour l'infraction la plus sévèrement réprimée.

Lorsque l'une des infractions prévues en vertu du présent Livre porte atteinte à des données informatiques ou aux systèmes informatiques liés à des infrastructures stratégiques ou sensibles, la peine initialement prévue s'élève jusqu'à la réclusion criminelle à perpétuité et jusqu'à cinq cent millions (500 000 000) de francs CFA d'amende ou l'une de ces deux peines seulement.

SECTION III

DES PEINES COMPLEMENTAIRES

Article 584 : Confiscation

En cas de condamnation pour l'une des infractions prévues au Titre I du présent Livre, la juridiction de jugement prononce la confiscation des matériels, des équipements, des instruments, des systèmes informatiques ou des données informatiques ainsi que des biens numéraires, avantages ou produits résultant de l'infraction.

Les décisions de condamnation prises en vertu de l'alinéa précédent sont publiées dans le Journal officiel de la République du Bénin ainsi que sur un support électronique aux frais du condamné.

Article 585 : Interdiction

En cas de condamnation pour l'une des infractions prévues au Titre I du présent Livre, la juridiction de jugement peut prononcer l'interdiction à titre de peine complémentaire, selon les modalités prévues au présent article. La peine d'interdiction comprend l'interdiction d'émettre des messages de communications électroniques et l'interdiction à titre provisoire ou définitif de l'accès au site ayant servi à commettre l'infraction voire à tout autre site quel qu'il soit, pour une durée de un (01) an à dix (10) ans.

Le tribunal peut faire injonction à toute personne responsable légalement du site ayant servi à commettre l'infraction et/ou à toute autre personne qualifiée de mettre en œuvre les moyens techniques nécessaires en vue de garantir l'interdiction d'accès, d'hébergement ou la coupure de l'accès au site incriminé.

Le tribunal peut prononcer à l'encontre du condamné pour les infractions prévues au Titre I du présent Livre, l'interdiction à titre définitif ou pour une durée de cinq (05) ans au plus, d'exercer toute activité en relation avec le secteur des communications électroniques ou d'exercer une fonction publique, un mandat électif ou une fonction dans une entreprise dont l'Etat est totalement ou partiellement propriétaire ou une activité socio-professionnelle, lorsque les faits ont été commis dans l'exercice ou à l'occasion de l'exercice des fonctions.

LégiBénin

Les tribunaux jugeant en matière correctionnelle pourront, s'ils le jugent nécessaire, interdire en tout ou en partie, l'exercice des droits civiques, civils et de famille suivants :

1- droit de vote et d'élection ;

2- droit d'éligibilité ;

3- droit d'être appelé ou nommé aux fonctions de juré ou autres fonctions publiques ou aux emplois de l'administration, ou d'exercer ces fonctions ou emplois ;

4- droit de port d'armes ;

5- droit de vote et de suffrage dans les délibérations de famille ;

6- droit d'être tuteur, curateur, si ce n'est de ses enfants et sur l'avis seulement de la famille ;

7- droit d'être expert ou témoins dans les actes ;

8- droit de déposer en justice, autrement que pour y donner de simples renseignements.

La violation des interdictions prononcées par les tribunaux est punie d'un emprisonnement de six (06) mois à trois (03) ans et d'une amende de trois cent mille (300 000) à cinq millions (5 000 000) de francs CFA.

Les décisions de condamnation prises en vertu du présent article sont publiées dans le Journal officiel de la République du Bénin ainsi que sur un support électronique aux frais du condamné.

LegiBénin

CHAPITRE XII

DES ENQUETES

Article 586 : Injonction de produire

Il est inséré dans le code de procédure pénale, un article 54 bis rédigé comme suit :

«Le procureur de la République, son substitut ou le juge d'instruction peut ordonner, par le biais d'une injonction de produire, à toute personne, tout établissement ou organisme privé ou public ou toute administration publique présentes sur le territoire de la République du Bénin ou fournissant des prestations de service en République du Bénin, susceptibles de détenir des documents intéressant l'enquête criminelle y compris ceux issus d'un système informatique ou un support de stockage informatique, de lui remettre ces documents, notamment sous forme numérique ou sous une version imprimée, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel.

Lorsque les réquisitions concernent des personnes mentionnées à l'article 102, la remise des documents ne peut intervenir qu'avec leur accord.

Le procureur de la République, son substitut ou le juge d'instruction peut ordonner, par le biais d'une injonction de produire, à un fournisseur de services présent sur le territoire de la République du Bénin offrant des prestations sur le territoire de la République du Bénin, de communiquer les données informatiques en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

Le procureur de la République, son substitut ou le juge d'instruction peut ordonner, par le biais d'une injonction de produire, à une personne présente sur le territoire de la République du Bénin ayant accès à un système informatique particulier et qui traite des données informatiques spécifiques provenant de ce système de les donner à une personne spécifique.

A l'exception des personnes mentionnées à l'article 102, le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende maximale de dix millions (10 000 000) de francs CFA. »

SECTION I

DES PERQUISITIONS

Article 587 : Données stockées dans un système informatique

Lorsque des données stockées dans un système informatique ou dans un support permettant de conserver des données informatisées sur le territoire béninois, sont utiles à la manifestation de la vérité, le juge d'instruction peut opérer une perquisition ou accéder à un système informatique ou à une partie de celui-ci ou dans un autre système informatique ou un support et aux données présentes dans ces derniers dès lors que ces données sont accessibles à partir du système initial ou disponible pour le système initial.

S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponible pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par le juge d'instruction, par voie de commission rogatoire internationale.

Legi Bénin

Article 588 : Requête

Les officiers de police judiciaire peuvent, par tout moyen, requérir toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition de leur remettre les informations permettant d'accéder aux données mentionnées.

Le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de deux cent mille (200 000) francs CFA.

Article 589 : Conditions de perquisition

Les perquisitions prévues à l'article 587 ne peuvent avoir lieu qu'avec le consentement exprès de la personne chez qui l'opération a lieu.

Cependant, si l'enquête est relative à un crime ou un délit puni de plus de cinq (5) ans de peine d'emprisonnement ou si la recherche de biens le justifie, le juge d'instruction peut, sur autorisation écrite, décider que la perquisition et la saisie seront effectuées sans l'assentiment de la personne.

Article 590 : Copie des données

Lorsque le juge d'instruction découvre dans un système informatique des données stockées qui sont utiles pour la manifestation de la vérité, mais que la saisie du support ne paraît pas souhaitable, ces données, de même que celles qui sont nécessaires pour les comprendre, sont copiées sur des supports de stockage informatique pouvant être saisis et placés sous scellés, elles peuvent être de plus rendues inaccessibles ou retirées du système informatique en question sous ordre du juge.

SECTION II

DE LA CONSERVATION RAPIDE DES DONNEES

Article 591 : Injonction de conserver et de protéger l'intégrité des données informatiques

Il est inséré dans le code de procédure pénale, un article 78 bis rédigé comme suit :

« En matière criminelle et en matière correctionnelle, lorsque les nécessités de l'information l'exigent, l'officier de police judiciaire ou le juge d'instruction peut, par le biais d'une notification écrite et :

- lorsqu'il y a des raisons de croire que les données informatiques stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification ; et
- que ces données informatiques sont utiles à la manifestation de la vérité,

ordonner à une personne, fournisseur de services en ligne visé à l'article 495 du présent code ou opérateur ou fournisseur de services de communication au public en ligne visés à l'article 34 du présent code, de conserver et de protéger l'intégrité des données informatiques stockées spécifiées dans la notification et qui se trouvent en sa possession ou sous son contrôle, pendant une durée de quatre vingt dix (90) jours maximum afin de permettre aux autorités désignées dans la notification écrite d'obtenir la divulgation des données et pour la bonne démarche des investigations judiciaires.

La durée exacte doit être indiquée dans la notification écrite et est renouvelable jusqu'à atteindre deux (02) ans maximum.

Le gardien des données ou une autre personne chargée de conserver et de protéger ces mêmes données est tenu de garder le secret de la mise en œuvre des procédures prises dans le cadre de l'alinéa 1er. Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel.

L'alinéa 2 ne s'appliquera pas lorsque l'obligation au secret a été levée par l'officier de police judiciaire ou le juge d'instruction, auteur de la notification écrite ».

Article 592 : Conservation et divulgation rapide de données relatives au trafic

Il est inséré dans le code de procédure pénale, un article 78 ter rédigé comme suit :

« En matière criminelle et en matière correctionnelle, lorsque les nécessités de l'information l'exigent, un officier de police judiciaire ou un juge d'instruction peut, lorsqu'il y a des raisons de croire que les données stockées dans un système informatique sont particulièrement susceptibles de perte ou de modification et que ces données sont utiles à la manifestation de la vérité, par le biais d'une notification écrite, exiger d'une personne contrôlant le système informatique, fournisseur de services en ligne visé à l'article 495 du présent code ou opérateur ou fournisseur de services de communication au public en ligne visés à l'article 34 du présent code, qu'elle divulgue ou conserve suffisamment de données de trafic associées à une communication électronique spécifique, afin d'identifier :

- le ou les fournisseurs de services ; et/ou
- la voie par laquelle la communication en question a été transmise.

Red Bean

Si la notification écrite requiert la conservation rapide, les principes de délais de l'article 35 de la présente loi s'appliquent.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret.

Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel.

L'alinéa 3 ne s'applique pas lorsque l'obligation au secret a été levée par l'officier de police judiciaire ou le juge d'instruction, auteur de la notification écrite ».

Article 593 : Collecte en temps réel des données relatives au trafic

Il est inséré dans le code de procédure pénale, un article 108 bis rédigé comme suit :

« En matière criminelle et en matière correctionnelle, lorsque les nécessités de l'information l'exigent, le juge d'instruction ou l'officier de police judiciaire commis par lui peut utiliser les moyens techniques appropriés pour collecter ou enregistrer en temps réel, sur le territoire de la République du Bénin, les données relatives au trafic de communications spécifiques, transmises au moyen d'un système informatique ou le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service, organisme placé sous l'autorité ou la tutelle du ministre chargé des communications électroniques ou tout agent qualifié d'un opérateur, en vue de procéder à l'installation d'un dispositif, dans le cadre de ses capacités techniques à collecter ou à enregistrer, transcrire en application de moyens techniques existant, ou à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer lesdites données informatisées.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel.

L'alinéa 2 ne s'appliquera pas lorsque l'obligation au secret a été levée par l'officier de police judiciaire ou le juge d'instruction, auteur de la notification écrite ou lorsque l'auteur ou le destinataire de la communication donne son consentement express ».

SECTION III

DE L'INTERCEPTION DES DONNEES INFORMATISEES

Article 594 : Interception et accès aux données par les autorités judiciaires

A l'article 108, alinéa 1er du code de procédure pénale, sont apportées les modifications suivantes :

« En matière criminelle et en matière correctionnelle, si la peine encourue est au moins égale à deux (02) ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances conformément aux dispositions de l'article 12 du présent code, y compris des données relatives au contenu, émises par voie de communications électroniques. »

A l'article 108, 5ème alinéa du code de procédure pénale, sont apportées les modifications suivantes :

« Le juge d'instruction ou l'officier de police judiciaire commis par lui peut requérir tout agent qualifié d'un service, organisme placé sous l'autorité ou la tutelle du Ministre chargé des

communications électroniques ou tout agent qualifié d'un opérateur, en vue de procéder à l'installation d'un dispositif d'interception. »

A l'article 108 du code de procédure pénale, deux nouveaux alinéas sont ajoutés après l'alinéa 5 :

« Un agent qualifié d'un service, organisme placé sous l'autorité ou la tutelle du Ministre chargé des communications électroniques ou tout agent qualifié d'un opérateur visé à l'alinéa précédent est tenu au secret.

Toute violation du secret est punie par les dispositions prévues par le code pénal relatives au secret professionnel. »

Article 595 : Interception et accès aux données par les autorités administratives

Pour les nécessités listées à l'article 596 du présent code, les autorités administratives qui seront désignées par voie règlementaire peuvent autoriser :

- les interceptions de correspondances émises par la voie des communications électroniques, conformément aux dispositions de l'article 12 du présent code ;

- la conservation et la protection de l'intégrité ainsi que le recueil, y compris en temps réel suivant les modalités prévues à l'article 78 ter du code de procédure pénale, des données et renseignements mentionnés aux articles 33 à 37 et à l'article 495 du présent code.

Les modalités de mise en œuvre des dispositions du présent article seront précisées par voie règlementaire.

Article 596 : Atteintes justifiant les interceptions et les accès aux données

Les opérations visées à l'article 595 du présent code peuvent être autorisées lorsqu'elles sont nécessaires :

- au maintien de l'indépendance nationale, de l'intégrité du territoire ou de la défense nationale ;

- à la préservation des intérêts majeurs de la politique étrangère de la République du Bénin ;

- à la sauvegarde des intérêts économiques, industriels et scientifiques majeurs de la République du Bénin ;

- à la prévention du terrorisme, des violences collectives de nature à porter gravement atteinte à la paix publique ou de la criminalité et de la délinquance organisées.

SECTION IV

DES COMPETENCES DES JURIDICTIONS BENINOISES EN MATIERE DE CYBERCRIMINALITE

Article 597 : Compétences

Legal Benin

Les juridictions béninoises sont compétentes lorsque :

1- l'infraction a été commise sur internet sur le territoire de la République du Bénin dès lors que le contenu illicite est accessible depuis la République du Bénin ;

2- la personne physique ou morale s'est rendue coupable sur le territoire de la République du Bénin, comme complice, d'un crime ou d'un délit commis à l'étranger si le crime ou le délit est puni à la fois par la loi béninoise et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère ;

3- les délits ont été commis par des Béninois hors du territoire de la République du Bénin si les faits sont punis par la législation du pays où ils ont été commis ;

4- tout délit puni d'emprisonnement, a été commis par un Béninois ou par un étranger hors du territoire de la République du Bénin lorsque la victime est de nationalité béninoise au moment de l'infraction.

CHAPITRE XIII

DE LA SECURITE DES RESEAUX

Article 598 : Essai de vulnérabilité

Les vendeurs de produits de technologies de l'information et de la communication devront faire réaliser par des experts en sécurité informatique indépendants agréés par le ministère en charge des communications électroniques, un essai de vulnérabilité et une évaluation de la garantie de sécurité, et devront informer les consommateurs de toutes les vulnérabilités décelées dans les produits de technologie de l'information et la communication ainsi que des solutions recommandées pour y remédier.

Leo-Bénin

Article 599 : Détections des évènements

Les opérateurs sont tenus de mettre en œuvre des systèmes qualifiés de détection des événements susceptibles d'affecter la sécurité de leurs systèmes d'information.

Les qualifications des systèmes de détection et des prestataires de service exploitant ces systèmes sont délivrés par le ministère en charge des communications électroniques.

Article 600 : Contrôles

Les opérateurs doivent soumettre leurs systèmes d'information à des contrôles destinés à vérifier le niveau de sécurité et le respect des règles de sécurité. Les contrôles sont effectués par l'agence nationale de sécurité des systèmes d'information, conformément aux dispositions de l'article 606 du présent code. Le coût des contrôles est à la charge de l'opérateur.

Article 601 : Sanction

Est puni d'une amende de dix millions (10 000 000) de francs CFA, le fait pour les mêmes personnes, d'omettre d'entretenir en bon état, les dispositifs de protection antérieurement établis.

Article 602 : Réponse à une attaque

Pour être en mesure de répondre à une attaque informatique, les services compétents de la République du Bénin peuvent détenir des équipements, des instruments, des programmes informatiques et toutes données susceptibles de permettre la réalisation d'une ou plusieurs des infractions en vue d'analyser leur conception et d'observer leur fonctionnement.

Les actes accomplis dans ce cadre et à ces fins ne peuvent faire l'objet d'aucune poursuite.

Article 603 : Sécurité des systèmes

Pour les besoins de la sécurité des systèmes d'information et des opérateurs, l'Agence Nationale de la Sécurité des Systèmes d'Information peut obtenir des opérateurs, l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués, afin de les alerter sur la vulnérabilité ou la compromission de leur système.

TITRE II

DU CADRE INSTITUTIONNEL

CHAPITRE I

DE L'AGENCE NATIONALE DE LA SECURITE DES SYSTEMES D'INFORMATION

Article 604 : Encrage institutionnel

Il est créé une Agence nationale de la sécurité des systèmes d'information « ANSSI-BENIN », ci-après désignée Agence.

L'Agence est un établissement de droit public à caractère administratif doté de la personnalité juridique, de l'autonomie administrative, financière et de gestion.

L'Agence est rattachée à la Présidence de la République.

Son siège est fixé à Cotonou. Toutefois, il peut être transféré en tout autre lieu du territoire national si les circonstances l'exigent, par décret pris en Conseil des ministres.

Article 605 : Compétences de l'Agence

La sécurité des systèmes d'information et des réseaux sur l'ensemble du territoire de la République du Bénin est du ressort de l'Agence.

Article 606 : Mission de l'Agence

L'Agence est en charge des missions suivantes :

- en matière de cryptologie, conformément aux dispositions de l'article 617 du présent code ;
- veiller à l'exécution des orientations nationales et de la stratégie générale de l'État en matière de sécurité des systèmes d'information et des réseaux ;
- suivre l'exécution des plans et des programmes relatifs à la sécurité des systèmes d'information et des réseaux dans les secteurs public et privé et à assurer la coordination entre les divers intervenants dans ce domaine ;
- apporter son concours aux services de l'État en matière de sécurité des systèmes d'information et des réseaux ;
- effectuer un contrôle général de la sécurité des systèmes d'information et des réseaux relevant des divers organismes publics et privés identifiés par voie règlementaire ;
- centraliser les demandes d'assistance à la suite des incidents de sécurité sur les systèmes d'informations et les réseaux ;

Legibenin

- assurer la veille technologique dans le domaine de la sécurité des systèmes d'information et des réseaux ;
- établir et maintenir une base de données des vulnérabilités ;
- élaborer des recommandations sur la sécurité des systèmes d'information et des réseaux et veiller à leur mise en œuvre dans les organismes publics ;
- diffuser des informations sur les précautions à prendre pour prévenir ou minimiser les risques d'incident ou leurs conséquences ;
- collaborer avec l'Office Central de Répression de la Cybercriminalité (OCRC) et toute autre entité publique dans le cadre de ses missions ;
- participer à la formation dans le domaine de la sécurité des systèmes d'information et des réseaux ;
- contribuer à l'élaboration des textes légaux et règlementaires relatifs à la sécurité des systèmes d'information et des réseaux ;
- contribuer, en ce qui concerne ses missions, à l'application des accords, traités et conventions relatifs à la lutte contre la cybercriminalité et la cybersécurité ratifiés par la République du Bénin ;
- veiller à l'exécution des dispositions légales et règlementaires relatives à la sécurité des systèmes d'information et des réseaux.

Article 607 : Composition organisation et modalités de fonctionnement de l'Agence

La composition, l'organisation et les modalités de fonctionnement de l'Agence sont précisés par décret pris en Conseil des ministres.

CHAPITRE II

DE L'OFFICE CENTRAL DE REPRESSION DE LA CYBERCRIMINALITE

Article 608 : Organe de lutte contre la Cybercriminalité

La structure de lutte contre les infractions cybernétiques est dénommée « Office central de répression de la cybercriminalité [« OCRC »].

L'OCRC, placé sous la tutelle du ministère en charge de la sécurité publique, a une compétence nationale.

Sont associés aux activités de cet Office, le ministère en charge de la défense nationale, le ministère en charge des finances et le ministère en charge des communications électroniques.

Article 609 : Compétences

L'OCRC a pour domaine de compétence, les infractions spécifiques à la criminalité liées aux technologies de l'information et de la communication.

Dans les conditions fixées à l'article suivant, sa compétence s'étend aux infractions dont la commission est facilitée ou liée à l'utilisation de ces technologies.

Article 610 : Missions et attributions

L'OCRC a pour missions :

LegiBénin

1- de veiller à la prise de mesures préventives contre la cybercriminalité ;

2- d'animer et de coordonner, au niveau national, la mise en œuvre opérationnelle de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication ;

3- d'effectuer conformément au code de procédure pénale les enquêtes sur les infractions visant ou utilisant les systèmes informatiques ainsi que les modes de traitement, de stockage et de communication de l'information ;

4- d'apporter son concours technique aux autres services de sécurité à l'occasion des enquêtes en cours nécessitant ses compétences techniques ou son expertise ;

5- d'assurer en liaison avec les services compétents, les actions de formation et d'information visant à renforcer les capacités opérationnelles des agents de tous les services concourant à la lutte contre ce fléau ;

6- d'intervenir d'initiative, sous la direction de l'autorité judiciaire saisie, chaque fois que les circonstances l'exigent, pour s'informer sur place des faits relatifs aux investigations conduites.

Article 611 : Organisation de l'OCRC

La composition, l'organisation et les modalités de fonctionnement de l'OCRC sont précisés par décret pris en Conseil des ministres.

Pour accomplir sa mission, l'OCRC centralise, analyse, exploite et communique aux services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects ainsi qu'aux autres administrations et services publics de l'Etat concernés, toutes informations relatives aux faits et infractions liés aux technologies de l'information et de la communication. Il établit également les liaisons utiles avec les organismes du secteur privé concernés.

Article 612 : Transmission d'informations

Dans le cadre de la législation applicable, notamment en matière de secret professionnel, les services de la police nationale, de la gendarmerie nationale, de la direction générale des douanes et droits indirects ainsi que les autres administrations et services publics de l'Etat concernés, adressent, dans les meilleurs délais, à l'OCRC les informations relatives aux infractions visées au présent livre dont ils ont connaissance.

Article 613 : Coopération

Pour les infractions relevant de sa compétence définie au 1er alinéa de l'article 609, l'OCRC constitue, pour la République du Bénin, le point de contact central dans les échanges internationaux. Il contribue au niveau national à l'animation et à la coordination des travaux préparatoires nécessaires et participe aux activités des organes et enceintes internationaux.

Sans préjudice de l'application des conventions internationales, il entretient les liaisons opérationnelles avec les services spécialisés des autres pays et avec les organismes internationaux en vue de rechercher toute information relative aux infractions ainsi qu'à l'identification et à la localisation de leurs auteurs.

Article 614 : Collaboration

L'OCRC collabore avec toutes les administrations publiques ou privées qui sollicitent son assistance technique ou son expertise pour se mettre à l'abri des méfaits criminels.

TITRE III

Legi-Bénin

DE LA CYBERSECURITE

CHAPITRE I

DE LA CRYPTOLOGIE

SECTION I

DE LA COMMISSION EN CHARGE DE LA CRYPTOLOGIE

Article 615 : Champ d'application

Le présent chapitre fixe le cadre légal et institutionnel applicable à la cryptologie en République du Bénin.

Les dispositions du présent chapitre ne s'appliquent pas aux moyens de cryptologie utilisés par les missions diplomatiques et consulaires visées par la Convention de Vienne sur les relations diplomatiques de 1961 ainsi qu'à ceux relatifs à la sécurité intérieure et extérieure de l'Etat du Bénin.

LegiBénin

SECTION II

DE LA COMMISSION EN CHARGE DE LA CRYPTOLOGIE

Article 615 : Commission de Cryptologie

L'ANSSI-BÉNIN désigne en son sein une commission en charge de la cryptologie en République du Bénin, ci-après désignée la «commission cryptologie».

Cette composition comprend au minimum cinq (05) membres. La commission cryptologie arrête son règlement intérieur fixant ses modalités de fonctionnement.

Ledit règlement intérieur n'entre en vigueur qu'après un avis motivé du ministre en charge des communications électroniques.

Article 617 : Compétences de la commission cryptologie

La commission cryptologie est compétente pour :

1- toute question relative au développement des moyens ou prestations de cryptologie en République du Bénin ;

2- analyser les projets de textes législatifs et réglementaires en matière de cryptologie ;

3- analyser les normes techniques adoptées dans le domaine de la sécurité des systèmes d'information en général et celui de la cryptologie en particulier ;

4- recevoir les déclarations conformément à l'article 620 ;

5- octroyer des autorisations conformément à l'article 621 ;

6- étudier les demandes d'agréments des prestataires de services de cryptologie ;

7- demander et recevoir la communication des descriptions des caractéristiques techniques des moyens de cryptologie ;

8- prononcer des sanctions administratives à l'encontre des contrevenants aux dispositions du présent Chapitre ;

9- défendre les intérêts de la République du Bénin dans les instances et organismes régionaux et internationaux traitant de la cryptologie ;

10- mener des enquêtes et procéder aux contrôles des prestataires de services de cryptologie et de produits de cryptologie fournis ;

11- réceptionner les fichiers électroniques signés par des clés de cryptologie publiques ;

12- analyser et tester les logiciels, les équipements et les algorithmes de cryptologie ;

13- auditer les produits de cryptologie.

Article 618 : Secret professionnel

La commission cryptologie et ses membres sont assujettis au secret professionnel.

Toute violation du secret professionnel est punie conformément aux dispositions du code pénal relatives au secret professionnel.

SECTION III

DES REGIMES JURIDIQUES

Article 619 : Liberté d'utilisation

L'utilisation, la fourniture, l'importation et l'exportation des moyens de cryptologie assurant exclusivement des fonctions d'authentification ou de contrôle d'intégrité sont libres, sous la réserve des obligations prévues au présent code.

Néanmoins, lorsque les moyens de cryptologie permettent d'assurer des fonctions de confidentialité, le principe de libre utilisation visé à l'alinéa 1er s'applique uniquement si les moyens s'appuient sur des conventions gérées par un prestataire agréé en vertu de l'article 621 du présent code.

Les prestations de services de cryptologie sont réservées aux prestataires de services de cryptologie, selon les modalités déterminées en vertu du présent chapitre.

Article 620 : Déclaration préalable

La fourniture ou l'importation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à une déclaration préalable auprès de la commission cryptologie, sous réserve des éventuelles dispenses de déclaration déterminée par décret pris en Conseil des ministres.

Le prestataire ou la personne procédant à la fourniture ou à l'importation d'un moyen de cryptologie tient à la disposition de la commission cryptologie une description des caractéristiques techniques des moyens de cryptologie utilisés.

Un décret pris en Conseil des ministres définit les conditions et délais dans lesquels la déclaration doit être réalisée, conformément à l'alinéa 1er du présent article.

LegiBénin

Il fixe notamment :

1- les conditions dans lesquelles sont réalisées ces déclarations, les conditions et les délais dans lesquels la commission cryptologie peut demander communication des caractéristiques des moyens de cryptologie, ainsi que la nature de ces caractéristiques ;

2- les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur transfert ou leur exportation peuvent être soit soumis au régime déclaratif et aux obligations d'information prévus à l'alinéa 1er, soit dispensés de toute formalité préalable.

Article 621 : Autorisation préalable

L'exportation de moyens de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité est soumise à l'autorisation de la commission cryptologie, sous réserve des dispenses de déclaration déterminée par décret.

Le prestataire ou la personne procédant à l'exportation d'un moyen de cryptologie tient à la disposition de la commission cryptologie une description des caractéristiques techniques de ce moyen de cryptologie.

Un décret pris en Conseil des ministres fixe les conditions dans lesquelles sont souscrites les demandes d'autorisation ainsi que les délais dans lesquels la commission cryptologie statue sur ces demandes. Il fixe notamment :

1- les conditions dans lesquelles sont formulées les demandes d'autorisation ainsi que les délais dans lesquels la commission cryptologie statue sur ces demandes ;

2- les catégories de moyens dont les caractéristiques techniques ou les conditions d'utilisation sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, leur transfert ou leur exportation peuvent être soit soumis au régime de l'autorisation préalable.

SECTION IV

DES PRESTATAIRES DE SERVICES DE CRYPTOLOGIE

Article 622 : Agrément préalable à la fourniture de services de cryptologie

Les prestataires de services de cryptologie doivent être agréés par la commission cryptologie.

Les conditions de délivrance de l'agrément aux prestataires de services de cryptologie ainsi que leurs obligations sont définies par décret pris en Conseil des ministres.

Article 623 : Exceptions

La commission cryptologie peut prévoir des exceptions à cette obligation d'agrément préalable pour les prestations cryptologie dont les caractéristiques techniques ou les conditions de fourniture sont telles que, au regard des intérêts de la défense nationale et de la sécurité intérieure ou extérieure de l'Etat, cette fourniture peut être dispensée de toute formalité préalable.

Article 624 : Présomption et exonération de responsabilité

Leo-Benin

Le prestataire de services de cryptologie est entièrement responsable du préjudice causé aux personnes :

- leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions ;
- qui se sont fiées raisonnablement au service de cryptologie fourni.

Toute clause contractuelle contraire est réputée non écrite.

Le prestataire de services de cryptologie peut toutefois dégager ou limiter sa responsabilité s'il parvient à démontrer l'absence de négligence ou de faute intentionnelle.

Les prestataires de services de cryptologie sont exonérés de toute responsabilité à l'égard des personnes qui font un usage non autorisé de leurs services, pour autant que les conditions d'utilisation précisent clairement les usages autorisés et non autorisés et soient aisément accessibles aux utilisateurs.

Les prestataires de services de cryptologie doivent obligatoirement contracter une police d'assurance couvrant les risques liés à l'exercice de leurs activités.

SECTION V

DES SANCTIONS

Article 625 : Types de sanctions

Lorsqu'un prestataire de services de cryptologie, même à titre gratuit, ne respecte pas les obligations auxquelles il est assujetti en application du présent Chapitre, la commission cryptologie peut, après audition de l'intéressé et après qu'il ait eu la possibilité de présenter ses observations, prononcer :

1- l'interdiction d'utiliser ou de mettre en circulation le moyen de cryptologie concerné. Le moyen de cryptologie concerné pourra être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites, dans les conditions prévues dans les dispositions du présent Chapitre ;

2- le retrait provisoire de l'autorisation accordée, pour une durée comprise entre un (01) et douze (12) mois ;

3- le retrait définitif de l'autorisation accordée ;

4- des amendes dont le montant est fixé en fonction de la gravité des manquements commis et en relation avec les avantages ou les profits tirés de ces manquements. Ces montants ne peuvent être supérieurs à ceux prévus à l'article 626, alinéa 2.

L'interdiction de mise en circulation prévue à l'alinéa 1er point 1 est applicable sur l'ensemble du territoire national. Elle emporte en outre pour le fournisseur l'obligation de procéder au retrait :

- auprès des diffuseurs commerciaux, des moyens de cryptologie dont la mise en circulation a été interdite ;

LégiBénin

- des matériels constituant des moyens de cryptologie dont la mise en circulation a été interdite et qui ont été acquis à titre onéreux, directement ou par l'intermédiaire de diffuseurs commerciaux.

Le moyen de cryptologie concerné peut être remis en circulation dès que les obligations antérieurement non respectées auront été satisfaites.

Article 626 : Violation de l'obligation de communication des caractéristiques techniques

Est puni d'un emprisonnement de six (06) mois à deux (02) ans et d'une amende de cinq cent mille (500 000) francs CFA à deux millions (2 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque n'aura pas satisfait à l'obligation de communication à la commission cryptologie d'une description des caractéristiques techniques du moyen de cryptologie dans les conditions prévues par les dispositions du présent chapitre et de ses textes d'application.

Article 627 : Violation de l'obligation de déclaration ou d'obtention d'agrément

Est puni d'un emprisonnement de six (06) mois à cinq (05) ans et d'une amende d'un million (1000 000) à cinq millions (5 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque fournit ou importe un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans satisfaire à l'obligation de déclaration préalable auprès de la commission cryptologie, sans préjudice de l'application du code des douanes.

Est puni d'un emprisonnement d'un (01) an à cinq (05) ans et d'une amende de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque fournit des prestations de cryptologie sans avoir obtenu préalablement l'agrément de la commission cryptologie.

Article 628 : Violation de l'obligation d'autorisation

Est puni d'un emprisonnement d'un (01) an à cinq (05) ans et d'une amende de un million (1 000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque aura exporté un moyen de cryptologie n'assurant pas exclusivement des fonctions d'authentification ou de contrôle d'intégrité sans avoir obtenu préalablement l'autorisation de la commission cryptologie, sans préjudice de l'application du code des douanes.

Article 629 : Violation d'une interdiction administrative

Est puni d'un emprisonnement d'un (01) an à cinq (05) ans et d'une amende de un million (1 000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque aura mis à la disposition d'autrui par la vente ou la location un moyen de cryptologie ayant fait l'objet d'une interdiction administrative d'utilisation et de mise en circulation, sans préjudice de l'application du code des douanes.

Article 630 : Obstacle à une enquête

Est puni d'un emprisonnement d'un (01) an à cinq (05) ans et d'une amende de un million (1 000 000) à vingt millions (20 000 000) de francs CFA ou de l'une de ces deux peines seulement, quiconque aura fait obstacle au déroulement des enquêtes prévues au sens des articles 634 et 635 du présent code ou refusé de fournir des informations ou documents y afférents, sans préjudice de l'application du code des douanes.

Article 631 : Circonstances aggravantes

Lex-Bénin

Lorsqu'un moyen de cryptologie a été utilisé pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission, le maximum de la peine privative de liberté encourue, prévu par le code pénal, est relevé ainsi qu'il suit :

1- réclusion criminelle à perpétuité lorsque l'infraction est punie de trente (30) ans de réclusion criminelle ;

2- trente (30) ans de réclusion criminelle lorsque l'infraction est punie de vingt (20) ans de réclusion criminelle ;

3- vingt (20) ans de réclusion criminelle lorsque l'infraction est punie de quinze (15) ans de réclusion criminelle ;

4- quinze (15) ans de réclusion criminelle lorsque l'infraction est punie de dix (10) ans d'emprisonnement ;

5- dix (10) ans d'emprisonnement lorsque l'infraction est punie de sept (07) ans d'emprisonnement ;

6- sept (07) ans d'emprisonnement lorsque l'infraction est punie de cinq (05) ans d'emprisonnement ;

7- le double lorsque l'infraction est punie de trois (03) ans d'emprisonnement au plus.

Les dispositions de l'alinéa 1er ne sont pas applicables à l'auteur ou au complice de l'infraction qui, à la demande des autorités compétentes, leur a remis la version intelligible des messages chiffrés, ainsi que les conventions secrètes nécessaires au déchiffrement.

Togo-Pedia

Article 632 : Refus de production de convention secrète

Est puni de trois (03) ans d'emprisonnement et d'un million (1 000 000) à vingt millions (20 000 000) de francs CFA d'amende, le fait pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application du code de procédure pénale.

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention permet d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq (05) ans d'emprisonnement et de cinq millions (5 000 000) à vingt millions (20 000 000) de francs CFA d'amende.

Article 633 : Peines complémentaires

Les personnes physiques ou morales coupables de l'une des infractions prévues à la présente section encourent également les peines complémentaires suivantes :

1- la confiscation, suivant les modalités prévues par le code pénal, de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution.

Le tribunal peut également prononcer la confiscation des moyens de cryptologie au profit des forces armées pour les besoins de la sécurité publique et de la défense nationale ;

2- l'interdiction, suivant les modalités prévues par le code pénal d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;

3- la fermeture, dans les conditions prévues par le code pénal, pour une durée de cinq (5) ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ;

4- l'exclusion, dans les conditions prévues par le code pénal et pour une durée de cinq (05) ans au plus, des marchés publics.

Article 634 : Recherche et constatation des infractions

Toute infraction visée dans les dispositions du présent chapitre est recherchée et constatée par procès-verbal soit par les officiers de police judiciaire et le cas échéant par le juge d'instruction conformément au code de procédure pénale, soit par des agents de l'administration des douanes, conformément aux dispositions du code des douanes.

Le ministre en charge des communications électroniques dans ses attributions peut également, par arrêté, nommer des agents assermentés par la commission cryptologie qui seront habilités à rechercher et constater par procès-verbal, les infractions aux dispositions du présent chapitre et de ses textes d'application.

Article 635 : Code de procédure pénale

Il est inséré dans le code de procédure pénale un article 78 quater rédigé comme suit :

« Le juge d'instruction ou un officier de police judiciaire délégué par le procureur de la République, peut ordonner aux personnes dont il présume qu'elles ont une connaissance particulière du système informatique qui fait l'objet de la recherche ou des services qui permettent de protéger ou de crypter, notamment par le biais d'un moyen de cryptologie, des données qui sont stockées, traitées ou transmises par un système informatique, de fournir des informations sur le fonctionnement de ce système et sur la manière d'y accéder ou d'accéder aux données qui sont stockées, traitées ou transmises par un tel système ou le cas échéant la convention secrète de déchiffrement, dans une forme intelligible.

Le juge d'instruction peut ordonner à toute personne appropriée de mettre en fonctionnement elle-même le système informatique ou, selon le cas, de rechercher, rendre accessibles, copier, rendre inaccessibles ou retirer les données pertinentes qui sont stockées, traitées ou transmises par ce système, dans la forme qu'il aura demandée. Ces personnes sont tenues d'y donner suite, dans la mesure de leurs moyens.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément aux dispositions relatives au secret professionnel du code pénal.

L'Etat est civilement responsable pour le dommage causé de façon non intentionnelle par les personnes requises à un système informatique ou aux données qui sont stockées, traitées ou transmises par un tel système. »

SECTION VI

DES MESURES DE CONTROLE ET SANCTIONS

Article 636 : Procédure d'avertissement

Lorsqu'une infraction au présent chapitre ou à l'un de ses textes d'application est constatée, les services compétents, ou les agents habilités adressent au contrevenant un avertissement le mettant en demeure de mettre fin au comportement constitutif d'infraction.

LegiBenin

L'avertissement est notifié au contrevenant dans un délai de quinze (15) jours à compter de la date de la constatation des faits, par envoi recommandé avec accusé de réception ou par la remise d'une copie, sous quelque support que ce soit, du procès-verbal de constatation des faits.

L'avertissement mentionne :

1- les faits imputés et là où les dispositions du présent Chapitre ou l'un des textes d'application, qui ont été enfreintes ;

2- le délai dans lequel il doit y être mis fin ;

3- qu'en l'absence de suite donnée à l'avertissement, les agents habilités peuvent aviser le procureur de la République ou appliquer le règlement par voie de transaction prévu au présent chapitre.

Article 637 : Recherche et constatation des actes interdits

Sans préjudice des compétences et attributions des officiers de police judiciaire, les agents habilités recherchent et constatent les infractions visées au présent chapitre.

Les procès-verbaux dressés par ces agents font foi jusqu'à preuve du contraire. Une copie est adressée au contrevenant, par envoi recommandé avec accusé de réception, dans les quarante cinq (45) jours à dater de la constatation des faits.

Sans préjudice de leur subordination à l'égard de leurs supérieurs dans l'administration, les agents visés à l'alinéa 1er exercent les pouvoirs qui leur sont conférés en vertu du présent article sous la surveillance du procureur général pour ce qui concerne les tâches de recherche et de constatation de délits visés par les dispositions du présent Livre.

Le procès-verbal visé à l'alinéa 2 du présent article n'est transmis au procureur de la République que lorsqu'il n'a pas été donné suite à l'avertissement.

En cas d'application de l'article 638, le procès-verbal n'est transmis au procureur de la République que lorsque le contrevenant n'a pas accepté la proposition de transaction.

Article 638 : Règlement transactionnel

Lorsque le dommage éventuellement causé à un tiers a été entièrement réparé, les agents habilités des services compétents peuvent, au vu des procès-verbaux et constatant une infraction aux dispositions du présent chapitre, proposer aux contrevenants le paiement d'une somme qui éteint l'action publique.

Le Conseil des ministres, par décret, fixe les tarifs ainsi que les modalités de paiement et de perception. La somme prévue conformément à l'alinéa 1er ne peut être inférieure au montant minimum prévu pour cette infraction et ne peut être supérieure au montant maximum prévu pour cette infraction.

Le paiement effectué dans le délai indiqué éteint l'action publique, et les sommes payées sont restituées au contrevenant, sauf si auparavant une plainte a été adressée au Procureur de la République ou le juge d'instruction a été requis d'instruire ou le tribunal a été saisi du fait.

Article 639 : Affichage

Le tribunal peut ordonner l'affichage du jugement ou du résumé qu'il rédige, pendant le délai qu'il détermine, aussi bien à l'intérieur qu'à l'extérieur des établissements du contrevenant et aux frais de celui-ci, de même que la publication du jugement ou du résumé aux frais du contrevenant par la voie des journaux ou de toute autre manière.

Togolex

LIVRE SEPTIEME

DES DISPOSITIONS TRANSITOIRES ET FINALES

TITRE PREMIER

DES DISPOSITIONS TRANSITOIRES

Article 640 : Validité des licences et autorisations en cours

Les licences et autorisations visées au Livre I et délivrées avant l'entrée en vigueur de la présente loi, conservent leur validité jusqu'à leur date d'expiration ou de modification.

Article 641 : Délais de mise en conformité

Les licences, autorisations et déclarations visées au Livre I et délivrées avant l'entrée en vigueur de la présente loi, devront être mises en conformité avec elle dans un délai de six (06) mois à compter de la date de son entrée en vigueur.

Les personnes physiques ou morales visées et/ou dont l'activité relève des dispositions de la présente loi, bénéficient d'un délai transitoire de six (06) mois à compter de sa date d'entrée en vigueur, pour se mettre en conformité avec toutes les dispositions nouvelles prévues par la présente loi.

Ce délai est allongé, le cas échéant, de durées égales aux délais nécessaires aux autorités publiques béninoises pour assurer la mise en conformité des personnes visées à l'alinéa précédent, aux dispositions nouvelles prévues par la présente loi, notamment dans les cas où l'autorisation, la réponse ou la réaction des autorités publiques béninoises est attendue, aux fins de mise en conformité.

Article 642 : Modalités de mise en conformité

Les modalités de mise en conformité des licences, cahiers de charges et conventions d'exploitation des opérateurs sont précisées par décret pris en Conseil des ministres.

Article 643 : Délai octroyé en cas de prospection directe

Un délai d'un (01) an à compter de la date d'entrée en vigueur de la présente loi est octroyé afin que les personnes physiques ou morales pratiquant la prospection directe au sens des articles 332 à 337 du présent code, et souhaitant utiliser des coordonnées de personnes légalement recueillies avant l'entrée en vigueur de la présente loi, puissent obtenir le consentement de ces personnes, dans l'objectif de les utiliser à des fins de prospection directe.

A l'expiration de ce délai, les personnes visées à l'alinéa précédent sont présumées avoir refusé l'utilisation ultérieure de leurs coordonnées personnelles à des fins de prospection directe si elles n'ont pas manifesté expressément leur consentement aux personnes physiques ou morales pratiquant la prospection directe.

Article 644 : Entrée en vigueur des dispositions de l'article 464

La nouvelle composition de l'APDP n'entre en vigueur qu'à l'expiration du mandat en cours.

Article 645 : Mandats en cours

Les mandats des organismes de l'ARCEP-Bénin, de l'ABSU-SEP et de l'APDP (ex CNIL) actuellement en cours, vont jusqu'à leur terme nonobstant l'entrée en vigueur de la présente loi.

Légi-Bénin

Article 646 : transfert de personnel, de patrimoine et de contrats

Les personnels du Secrétariat exécutif de l'ex-ARCEP-Bénin, de l'ex-ABSU-CEP et de l'ex-CNIL, leurs patrimoines ainsi que les contrats en cours d'exécution y compris les contrats de travail, sont respectivement transférés à l'ARCEP-Bénin, à l'ABSU-CEP et à l'APDP créées par la présente loi.

TITRE II

DES DISPOSITIONS FINALES

Article 647 : Dispositions abrogatoires

La présente loi portant code du numérique en République du Bénin abroge toutes dispositions antérieures contraires notamment celles :

- de la loi n° 2014-14 du 14 juillet 2014 relative aux communications électroniques et à la poste en République du Bénin, à l'exception des dispositions relatives au secteur postal ;

- de la loi n° 2009-09 du 24 mai 2009 portant protection des données à caractère personnel en République du Bénin.

La présente loi sera exécutée comme loi de l'Etat.-

Porto-Novo, le 13 juin 2017

P/le Président de l'Assemblée nationale, et PO,

le deuxième Vice-Président,

Robert GBIAN

Légi Bénin