ITU Publications
Période d'études 2018-2021

Union internationale des télécommunications
Secteur du développement

Commission d'Études 2 Question 4

Assistance aux pays en développement concernant la mise en œuvre des programmes de conformité et d'interopérabilité et lutte contre la contrefaçon d'équipements TIC et le vol de dispositifs mobiles

Rapport final sur la Question 4/2 de l'UIT-D

Assistance aux pays en développement concernant la mise en œuvre des programmes de conformité et d'interopérabilité et lutte contre la contrefaçon d'équipements TIC et le vol de dispositifs mobiles

Périodes d'études 2018-2021

Assistance aux pays en développement concernant la mise en œuvre des programmes de conformité et d'interopérabilité et lutte contre la contrefaçon d'équipements TIC et le vol de dispositifs mobiles: Rapport final sur la Question 4/2 de l'UIT-D

978-92-61-34132-9 (version électronique)
978-92-61-34142-8 (version EPUB)
978-92-61-34152-7 (version Mobi)

Libellé proposé: Assistance aux pays en développement concernant la mise en œuvre des programmes de conformité et d'interopérabilité et lutte contre la contrefaçon d'équipements TIC et le vol de dispositifs mobiles: Rapport final sur la Question 4/2 de l'UIT-D pour la période d'études 2018-2021. Genève: Union internationale des télécommunications, 2021. Licence: CC BY-NC-SA 3.0 IGO.

Crédits photos couverture: Shutterstock

Remerciements

Les commissions d'études du Secteur du développement des télécommunications de l'UIT (UIT-D) offrent un cadre neutre permettant à des experts issus du secteur public, du secteur privé, d'organisations de télécommunication et d'établissements universitaires du monde entier de se réunir, afin d'élaborer des outils pratiques et des ressources pour examiner les questions touchant au développement. À cette fin, les deux commissions d'études de l'UIT-D sont chargées d'élaborer des rapports, des lignes directrices et des recommandations sur la base des contributions soumises par les membres. La Conférence mondiale de développement des télécommunications (CMDT) décide de mettre à l'étude des Questions tous les quatre ans. Les membres de l'UIT, réunis à la CMDT-17 tenue à Buenos Aires en octobre 2017, ont décidé que pendant la période 2018-2021, la Commission d'études 2 serait chargée de l'étude de sept Questions, qui s'inscrivent dans le cadre général des "services et applications reposant sur les technologies de l'information et de la communication pour promouvoir le développement durable".

Le présent rapport a été élaboré au titre de la Question 4/2, intitulée **"Assistance aux pays en développement concernant la mise en œuvre des programmes de conformité et d'interopérabilité et lutte contre la contrefaçon d'équipements TIC et le vol de dispositifs mobiles"**, sous la supervision et la coordination générales de l'équipe de direction de la Commission d'études 2 de l'UIT-D, dirigée par M. Ahmad Reza Sharafat (République islamique d'Iran), Président, secondé par les Vice-Présidents suivants: M. Nasser Al Marzouqi (Émirats arabes unis) (qui a démissionné en 2018); M. Abdelaziz Alzarooni (Émirats arabes unis); M. Filipe Miguel Antunes Batista (Portugal) (qui a démissionné en 2019); Mme Nora Abdalla Hassan Basher (Soudan); Mme Maria Bolshakova (Fédération de Russie); Mme Celina Delgado Castellón (Nicaragua); M. Yakov Gass (Fédération de Russie) (qui a démissionné en 2020); M. Ananda Raj Khanal (République du Népal); M. Roland Yaw Kudozia (Ghana); M. Tolibjon Oltinovich Mirzakulov (Ouzbékistan); Mme Alina Modan (Roumanie); M. Henry Chukwudumeme Nkemadu (Nigéria); Mme Ke Wang (Chine); et M. Dominique Würges (France).

Ce rapport a été rédigé sous la direction du Rapporteur pour la Question 4/2, M. Cheikh Tidjani Oudaa (Mauritanie), en collaboration avec les Vice-Rapporteurs suivants: M. Ahmadou Dit Adi Cisse (Mali); Mme Amel Khiar (Algérie); M. Joseph Onaya (Kenya); M. Brillant Harivony Rakotoratsimanjefy (Madagascar); et M. Serigne Abdou Lahatt Sylla (Sénégal).

Nous remercions tout particulièrement les coordonnateurs des chapitres pour leur appui, leur travail inlassable et leurs compétences techniques.

Le présent rapport a été élaboré avec le concours des coordonnateurs du BDT, des éditeurs, ainsi que de l'équipe du Service de la production des publications et du secrétariat des commissions d'études de l'UIT-D.

Table des matières

Liste des tableaux et figures

Tableau

Figures

Résumé analytique

Une dépendance et une confiance mondiales à l'égard des dispositifs TIC

Les dispositifs des technologies de l'information et de la communication (TIC) sont essentiels pour accéder au monde numérique. Il est indispensable d'harmoniser les normes à l'échelle mondiale et de les respecter pour garantir l'interopérabilité des réseaux et les possibilités d'interconnexion entre les utilisateurs et les appareils.

Tous les pays mettent en œuvre des programmes de conformité et d'interopérabilité (C&I) et des techniques avancées de lutte contre la multiplication des équipements TIC de contrefaçon et le vol de dispositifs mobiles, certains progressant plus rapidement que d'autres.

Le Secteur du développement des télécommunications de l'UIT (UIT-D) aide les États Membres à évaluer les difficultés d'ordre technique et économique liées à la garantie de la conformité et de l'interopérabilité des dispositifs TIC, en mettant l'accent sur l'assistance aux États Membres de l'UIT, le renforcement des capacités et l'échange de bonnes pratiques entre ceux-ci. L'UIT-D collabore étroitement à ce titre avec le Secteur des radiocommunications de l'UIT (UIT-R) et le Secteur de la normalisation des télécommunications de l'UIT (UIT-T), afin de créer des synergies dans ces activités et obtenir de meilleurs résultats.

De plus, dans une société de plus en plus connectée au moyen de dispositifs TIC, la question de l'utilisation de cadres C&I demeure importante et fait l'objet de nombreux débats entre les développeurs, les fabricants, les importateurs, les opérateurs et les utilisateurs. Le rôle des autorités de régulation à cet égard est primordial pour concilier les niveaux de sécurité et de contrôle nécessaires.

Enfin, d'autres questions importantes concernent l'avenir de la conformité et de l'interopérabilité, à savoir l'émergence de nouvelles technologies découlant de l'Internet des objets (IoT) dans tous les secteurs d'activité, et les normes à prendre en considération lorsque les pays en développement mettent en œuvre ou revoient des cadres C&I.

Dans ce contexte, le présent rapport examine les bonnes pratiques permettant de trouver des solutions optimales.

Travaux de base dans le domaine de la conformité et de l'interopérabilité

Lors des périodes d'études précédentes, l'UIT a porté toute son attention sur la question importante de l'assistance aux pays en développement en matière de conformité et d'interopérabilité. Plusieurs documents notables ont été élaborés et sont toujours pertinents dans le cadre des travaux de l'UIT-D sur la Question 4/2. Le rapport précédent sur la Question 4/2 est consultable à l'adresse https://www.itu.int/pub/D-STG-SG02.04.1-2017, tandis que des éléments d'information portant sur d'autres activités de l'UIT-D en matière d'assistance aux pays en développement, telles que la base de données sur les systèmes C&I établis aux niveaux national et régional, les évaluations régionales et les activités de renforcement des capacités, sont disponibles à l'adresse https://itu.int/go/CI_Development.

Chapitre 1 – Les produits des technologies de l'information et de la communication permettent d'atteindre des Objectifs de développement durable

1.1 Importance des produits TIC pour la société

La transformation numérique entraîne des changements rapides qui touchent tous les secteurs d'activité et tous les aspects de notre quotidien. Sous l'effet direct de trois éléments fondamentaux des TIC jouant un rôle moteur, à savoir la mobilité, le large bande et l'informatique en nuage, on assiste à l'émergence d'une nouvelle économie fondée sur les services dans laquelle les chaînes de valeur sont repensées, les modèles économiques deviennent de plus en plus numériques, la distance n'est plus un obstacle et les particuliers peuvent de plus en plus échanger des biens et des services au lieu de les acheter et d'en être propriétaire, par exemple. Autant d'exemples qui illustrent la façon dont l'ère du numérique ouvre la voie à de nouveaux modèles économiques innovants et révolutionne notre quotidien[1].

Les principaux avantages des TIC sont l'amélioration de l'accès, de la connectivité et de l'efficacité au profit des particuliers, des communautés et des économies[2], comme indiqué ci-après:

- Accès à l'information et aux services: grâce aux dispositifs et à l'infrastructure des TIC et à l'utilisation de technologies telles que les téléphones mobiles, les réseaux de télécommunication cellulaire (par exemple les réseaux 3G et LTE) ou encore l'Internet et le large bande, les TIC permettent d'améliorer l'accès universel des particuliers à l'information et aux services partout dans le monde, aussi bien dans les zones rurales que dans les zones urbaines.
- Connectivité entre les particuliers et les organisations: la connectivité instantanée ou quasi-instantanée entre les particuliers, les organisations et les réseaux peut accroître la productivité et stimuler l'innovation dans de nombreux secteurs et de nombreuses communautés et permettre d'assurer les communications en temps réel qui sont nécessaires pour déployer rapidement des services essentiels.
- Meilleure efficacité grâce à l'amélioration de la productivité et à une utilisation rationnelle des ressources.
- Adoption de normes respectueuses de l'environnement qui s'inscrivent dans la lutte efficace contre le changement climatique.
- Les TIC peuvent permettre de réaliser des gains de productivité et d'en tirer parti, en offrant aux particuliers un meilleur accès à l'information et à la communication (par

[1] Comme l'a déclaré M. Hans Vestberg, P.-D. G d'Ericsson, dans l'avant-propos de la publication "ICT & SDGs – Final Report: How Information and communications technology can accelerate action on the Sustainable Development Goals". The Earth Institute, Université Columbia et Ericsson.

[2] Huawei. 2017 ICT Sustainable Development Goals Benchmark. Huawei, 2017.

exemple en ce qui concerne la réduction des ressources utilisées pour les déplacements ou la collecte manuelle des données), et en fournissant l'infrastructure nécessaire pour collecter et analyser de vastes ensembles de données (les mégadonnées, par exemple).

1.2 Les dispositifs TIC en tant que socle de l'économie sociale

Afin de mettre en œuvre des politiques cohérentes et de renforcer les initiatives de développement fondées sur les TIC, il est indispensable de disposer d'un cadre stratégique. Les TIC doivent être intégrées dans tous les aspects des politiques publiques et de l'activité économique. Pour ce faire, il sera nécessaire d'effectuer les actions suivantes:

- Élaborer des politiques publiques et des réglementations visant à permettre une utilisation pleine et entière des TIC.
- Développer et moderniser rapidement l'infrastructure TIC.
- Favoriser des partenariats public-privé pour créer de nouvelles start-up dans le secteur des TIC, afin de fournir des services adaptés aux circonstances locales.
- Traiter des questions d'interopérabilité des TIC.
- Renforcer les capacités en matière de gestion des systèmes TIC.
- Veiller à ce que les politiques et la réglementation suivent le rythme rapide de l'innovation et du déploiement des TIC.

1.3 Connecter et protéger les utilisateurs des TIC et les réseaux TIC via la conformité à des normes reconnues

Les investissements dans l'infrastructure et l'innovation constituent un catalyseur essentiel de la croissance et du développement économiques. Le progrès technologique est également un élément fondamental afin de trouver des solutions durables aux problèmes économiques et environnementaux, par exemple pour créer de nouveaux emplois et promouvoir l'efficacité énergétique. La promotion de secteurs d'activité durables et l'investissement dans la recherche scientifique et l'innovation sont autant de moyens importants de favoriser le développement durable[3].

ODD 9: Bâtir une infrastructure résiliente, promouvoir une industrialisation durable qui profite à tous et encourager l'innovation

Cibles:

9.1 – Mettre en place une infrastructure de qualité, fiable, durable et résiliente, y compris une infrastructure régionale et transfrontière, pour favoriser le développement économique et le bien-être de l'être humain, en mettant l'accent sur un accès universel, à un coût abordable et dans des conditions d'équité.

9.a – Faciliter la mise en place d'une infrastructure durable et résiliente dans les pays en développement en renforçant l'appui financier, technologique et technique apporté aux pays d'Afrique, aux pays les moins avancés, aux pays en développement sans littoral et aux petits États insulaires en développement.

[3] Programme des Nations Unies pour le développement (PNUD). Objectifs de développement durable. ODD 9: Industrie, innovation et infrastructure.

9.b – Soutenir la recherche-développement et l'innovation technologiques nationales dans les pays en développement, notamment en instaurant des conditions propices, entre autres, à la diversification industrielle et à l'ajout de valeur aux marchandises.

9.c – Accroître nettement l'accès aux technologies de l'information et de la communication et faire en sorte que tous les habitants des pays les moins avancés aient accès à Internet à un coût abordable d'ici à 2020.

Afin de protéger les utilisateurs des TIC et les réseaux TIC, il convient d'accorder une attention particulière aux éléments suivants:

- qualité;
- sécurité;
- interopérabilité;
- environnement radioélectrique exempt de brouillage;
- règles nationales;
- durabilité;
- fiabilité;
- résilience;
- accessibilité financière (grâce aux économies d'échelle rendues possibles par la conformité et l'interopérabilité).

Pour cela, il faut tenir compte des questions liées aux équipements et aux systèmes TIC, parmi lesquelles:

- les prescriptions et normes techniques;
- l'évaluation de la conformité;
- le contrôle des équipements;
- la surveillance après la mise sur le marché;
- la promotion des accords de reconnaissance mutuelle.

Des **modes d'évaluation innovants** de la conformité et de l'interopérabilité sont donc nécessaires, en tenant compte des éléments suivants:

- création ou partage de laboratoires de test;
- services de laboratoire virtuel;
- accords de reconnaissance mutuelle tenant compte des exigences et des limites aux niveaux local et régional;
- surveillance après la mise sur le marché;
- solutions intelligentes en matière de tests;
- harmonisation des normes.

Il convient d'effectuer les **tâches** suivantes:

- accroître la sensibilisation;
- mettre en place une plate-forme de contacts en réseau sur la conformité et l'interopérabilité à l'intention des Membres de l'UIT-D;
- promouvoir la collaboration, la recherche et l'échange de données d'expérience sur les sujets relevant de la Question;
- garantir la représentation des Membres de l'UIT-D dans d'autres instances s'occupant de la conformité et de l'interopérabilité (par exemple les réunions du groupe STAR (Groupe Alliances stratégiques et réglementation) du CASCO/ISO);

- réaliser un questionnaire visant à recueillir des données de pays et à suivre les progrès accomplis dans le domaine de la conformité et de l'interopérabilité;
- établir des lignes directrices;
- publier des recommandations.

1.4 Les conséquences de la pandémie de COVID-19 sur les procédures d'homologation

La pandémie de COVID-19 a eu, et continue d'avoir, de nombreuses conséquences pour le commerce international et l'évaluation de la conformité des produits, notamment des dispositifs TIC. En raison de la fermeture des frontières et des difficultés d'accès aux installations (par exemple en ce qui concerne l'accès aux laboratoires de test physiques et les visites d'experts sur le terrain), les activités d'homologation ont été largement entravées. Il est alors devenu nécessaire de trouver des manières innovantes de certifier la conformité et la qualité des produits. Les régulateurs, les fabricants et les opérateurs se sont efforcés de mettre au point des solutions ad hoc pour assurer la continuité des activités et éviter les perturbations de la chaîne commerciale. Le moment est venu de tirer parti des technologies numériques pour trouver des solutions dans le domaine de l'évaluation de la conformité.

Chapitre 2 – Conformité et interopérabilité

2.1 Introduction

L'évaluation de la conformité vise à garantir la conformité des équipements TIC aux normes et spécifications techniques. Elle permet aux vendeurs et aux utilisateurs d'évaluer les performances des équipements lorsqu'ils seront intégrés dans un réseau avec d'autres dispositifs pour fournir un service sur le réseau. Les tests d'interopérabilité ont pour but de déterminer si deux produits ou plus respectent les spécifications techniques nécessaires pour garantir une intégration réussie en suivant des protocoles de communication précis.

Il est important d'effectuer des tests de conformité et d'interopérabilité pour identifier d'éventuelles fonctionnalités des équipements installés sur un réseau TIC qui ne seraient pas conformes aux normes sectorielles reconnues et qui pourraient ainsi compromettre la qualité du service de réseau fourni. La commercialisation de produits de pointe de grande qualité contribue au déploiement massif des technologies de réseau et des services de réseau associés.

2.2 Examen des questions/priorités essentielles dans les pays et les régions

Les problèmes de conformité et d'interopérabilité sont liés à diverses préoccupations et difficultés, notamment[4]:

- le comportement des services de signalisation des réseaux intelligents existants (problèmes d'interopérabilité) lorsque des équipements sont remplacés, et les problèmes de signalisation dans les réseaux mobiles (accès, centre du réseau, SMS);
- l'absence de conformité et d'interopérabilité entre des équipements vendus par différents fournisseurs;
- l'emploi d'interfaces ou de protocoles non normalisés dans les équipements de différents constructeurs;
- des équipements produits par le même fabricant, mais dont le logiciel a bénéficié de mises à jour différentes, ont des clients de protocole d'ouverture de session (SIP) incompatibles;
- un problème de conformité des décodeurs de différents fabricants de matériel destiné à la télévision par Internet;
- des problèmes de largeur de bande, c'est-à-dire de capacité de transmission de la voix, de données et de vidéos quand les utilisateurs ajoutent beaucoup de contenus sur le réseau existant;
- des difficultés d'interopérabilité des réseaux complexes pour parvenir à intégrer des équipements et des réseaux;
- des services mis en place avec certains prestataires ne disposent pas des infrastructures et des équipes de dépannage nécessaires pour assurer leur interopérabilité avec d'autres exploitants;

[4] UIT-D. Rapport final de la Commission d'études 2 de l'UIT-D sur la Question 4/2 pour la période d'études 2014-2017: "Assistance aux pays en développement concernant la mise en œuvre des programmes de conformité et d'interopérabilité". UIT, 2017.

- la définition d'une méthode permettant l'adoption de normes;
- la gestion des relevés de données de taxation pour la facturation;
- la mise en œuvre de nouvelles fonctionnalités et de nouveaux services sur toutes les plates-formes;
- l'existence de modèles de taxation différents;
- les nouvelles technologies ne peuvent pas fonctionner avec les équipements existants;
- aucun centre ou établissement d'essais;
- manque de personnel qualifié pour assurer les tâches de C&I;
- des problèmes de compatibilité avec des réseaux numériques à intégration de services (RNIS);
- des problèmes entre des terminaux d'utilisateurs différents;
- des problèmes d'interopérabilité entre des services et des terminaux d'utilisateurs;
- l'utilisation par certains fournisseurs d'interfaces propriétaires non normalisées;
- les coûts;
- le manque de capacités humaines et de possibilités de formation;
- la faiblesse des systèmes institutionnels;
- la méconnaissance de la normalisation;
- les problèmes d'interopérabilité.

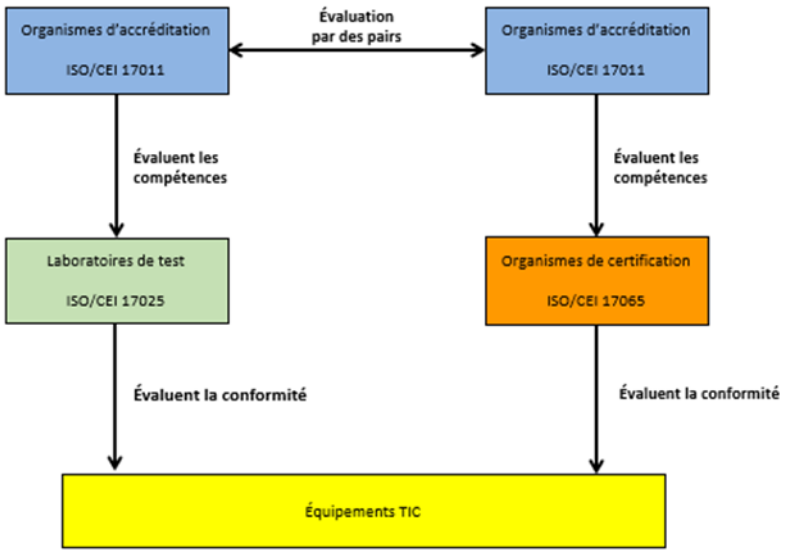
Activités d'évaluation de la conformité

L'évaluation de la conformité comprend les activités suivantes:

- Désignation et reconnaissance des organismes d'accréditation
- Désignation et reconnaissance des organismes de certification
- Désignation et reconnaissance des laboratoires de test
- Enregistrement et certification.

Les activités d'évaluation de la conformité sont présentées dans la **Figure 1** ci-dessous.

Figure 1 – Activités d'évaluation de la conformité



2.3 Spécifications et normes techniques

Les fournisseurs de services et les opérateurs définissent les normes et spécifications applicables aux équipements et aux systèmes qu'ils utilisent pour servir leurs clients. Les régulateurs nationaux établissent des réglementations, des normes et des spécifications applicables aux équipements et aux systèmes déployés sur le territoire national. Les utilisateurs, les fournisseurs de services et les régulateurs nationaux doivent obtenir la preuve incontestable que ces équipements et ces systèmes respectent les normes et les prescriptions adéquates ainsi que les spécifications d'interopérabilité[5].

Afin de favoriser l'élaboration de normes, guides et recommandations au niveau international, le Comité des obstacles techniques au commerce (OTC) de l'Organisation mondiale du commerce (OMC) a établi les six principes suivants[6]:

- Transparence
- Ouverture
- Impartialité et consensus
- Efficacité et pertinence
- Cohérence
- Dimension développement.

L'importance des normes

La conformité aux normes techniques:

- est essentielle pour l'interopérabilité des équipements et des réseaux;
- réduit les risques d'être contraint d'utiliser une technologie et de se retrouver piégé vis-à-vis d'un fournisseur donné;
- garantit la réalisation des objectifs légitimes, notamment de ceux portant sur la sécurité et l'absence de brouillages;
- favorise l'intégration régionale;
- favorise l'agrégation des marchés, la compétitivité et les échanges commerciaux.

Nouvelles procédures

Les nouvelles procédures associent:

- des déclarations de conformité des fabricants, des tests de conformité effectués par les laboratoires et la surveillance du marché;
- des normes mondiales et des accords de reconnaissance mutuelle (ARM) sur les normes et les procédures d'homologation applicables entre les pays ou au sein de groupes de pays.

---

5 UIT. Mise en place de systèmes pour la conformité et l'interopérabilité: Lignes directrices complètes. Février 2015.

6 OMC. Comité des obstacles techniques au commerce. Document G/TBT/9, novembre 2000.

2.4 Arrangements/accords de reconnaissance mutuelle sur l'évaluation de la conformité

2.4.1 Qu'est-ce qu'un arrangement/accord de reconnaissance mutuelle?

Un arrangement/accord de reconnaissance mutuelle sur l'évaluation de la conformité - désigné ci-après par le sigle ARM - est un arrangement/accord volontaire (sur des procédures et processus) entre des parties (des entités privées ou publiques) portant sur la reconnaissance des résultats d'évaluation de la conformité.

Un *accord* de reconnaissance mutuelle est un engagement juridique officiel entre des parties portant sur la reconnaissance des résultats d'évaluation de la conformité d'équipements de télécommunication. Il concerne des exigences réglementaires et est désigné ci-après par "ARM réglementaire". Ces accords sont souvent conclus sur une base bilatérale, régionale ou multilatérale entre deux gouvernements ou plus.

Un *arrangement* de reconnaissance mutuelle est un arrangement volontaire entre des parties portant sur la reconnaissance des résultats d'évaluation de la conformité d'équipements de télécommunication. Il concerne des exigences non réglementaires et est désigné ci-après par "ARM non réglementaire". Un cas d'arrangement de reconnaissance mutuelle est celui où des organismes d'accréditation s'engagent à reconnaître mutuellement les résultats d'évaluation de la conformité établis par des organismes d'évaluation de la conformité accrédités.

Les parties à un ARM sont tenues d'établir les processus et les procédures visant à mettre en œuvre l'ARM à des fins d'intérêt mutuel. Cette obligation s'applique aussi bien aux ARM réglementaires qu'aux ARM non réglementaires.

Un ARM ne remet pas en cause la compétence de l'autorité de régulation dont dépendent les parties à l'accord ou à l'arrangement. L'ARM devrait mentionner les différents organismes concourant à sa mise en œuvre:

- *Partie*: entité qui accepte de participer à l'ARM.
- *Autorité de désignation*: autorité publique ou organisme compétent reconnu nommé par une partie afin de désigner un organisme d'évaluation de la conformité chargé d'évaluer la conformité au titre de l'ARM.
- *Organisme d'accréditation*: organisme chargé d'évaluer et de reconnaître les compétences spécifiques des laboratoires de test et/ou des organismes de certification conformément aux normes internationales.
- *Organisme d'évaluation de la conformité*: organisme désigné pour effectuer, au titre de l'ARM, une évaluation de la conformité selon les exigences d'une autre partie en matière de télécommunications (il peut s'agir d'une tierce partie, du laboratoire de test d'un fournisseur ou d'un organisme de certification).
- *Comité mixte*: comité mis en place par les parties afin de gérer le lancement et la mise en œuvre de l'ARM, de l'adapter si nécessaire et de s'occuper de toute autre question relative à la bonne application de l'ARM, y compris les modifications et ajustements ultérieurs.
- *Autorité de régulation*: entité dotée de compétences juridiques responsable des télécommunications.

2.4.2 Rôle des ARM dans le système C&I

Les ARM servent à:

- reconnaître la compétence de parties tierces en matière d'exécution des processus nationaux réglementaires ou d'homologation;
- éviter les coûts des tests en double et favoriser la transparence;
- faciliter l'accès aux marchés étrangers;
- réduire les délais de mise sur le marché et les coûts de production;
- lutter contre les pratiques prédatrices et éliminer les obstacles à l'entrée sur le marché;
- rationaliser les procédures et les méthodes, et réduire ainsi sensiblement les coûts pour les producteurs présents sur plusieurs marchés.

Le but ultime: "un seul test, effectué une fois, valable dans le monde entier".

2.5 Infrastructure virtuelle

2.5.1 Tests virtuels[7]

Dans le secteur des TIC, les services sont de plus en plus fournis de manière virtuelle grâce à l'Internet. Cette évolution récente s'observe également en ce qui concerne les mécanismes émergents d'évaluation de la connectivité des équipements TIC sur les réseaux IP, et s'inscrit dans le cadre des exigences relatives aux nouveaux réseaux convergents.

Les laboratoires virtuels peuvent offrir des services de test rapides, financièrement abordables et durables aux pays en développement ne pouvant pas effectuer de tests eux-mêmes.

Deux solutions en matière de tests virtuels sont présentées ci-dessous: les tests d'interopérabilité et les tests d'homologation à distance.

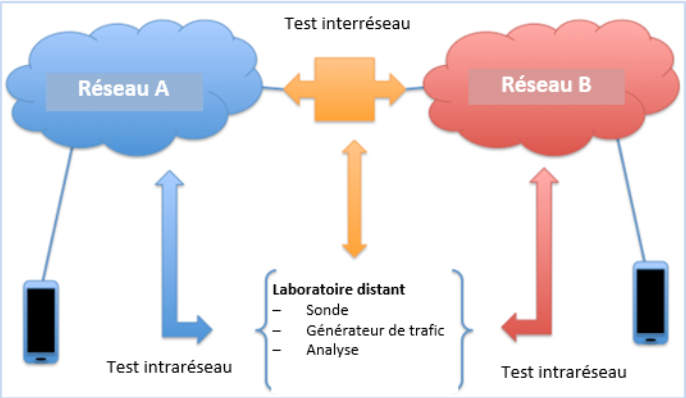
2.5.2 Tests d'interopérabilité à distance

Objectif: *évaluer l'interopérabilité des réseaux des opérateurs dans différents pays/régions*

L'expérience acquise à travers le monde confirme la nécessité de soumettre les produits et systèmes basés sur les TIC à des tests et des procédures de certification normalisés, afin d'éviter les nombreux problèmes qu'entraîne leur utilisation pour les usagers et les opérateurs.

[7] UIT-D. Rapport final de la Commission d'études 2 de l'UIT-D sur la Question 4/2 pour la période d'études 2014-2017. Op. cit.

Figure 2 – Test d'interopérabilité à distance



L'absence d'interopérabilité peut poser de nombreux problèmes, dont les suivants:

- Réduction du débit de communication.
- Manque de fiabilité des communications.
- Réduction de la durée de vie utile des dispositifs et des équipements.
- Forte consommation d'énergie.
- Interférences d'un service à l'autre (en particulier dans les systèmes sans fil).
- Équipements de qualité médiocre qui entravent l'évolution et la compatibilité avec les technologies et les protocoles nouveaux.
- Incompatibilité des équipements provoquant des goulets d'étranglement dans la communication souvent très difficiles à diagnostiquer.
- Fluctuations de fonctionnement du réseau en raison de l'absence de procédures permettant de surveiller les modifications des équipements et logiciels.
- Difficultés d'interconnexion entre les équipements des différents fabricants et entre les réseaux de pays différents.

Les tests virtuels peuvent être menés pour atteindre des objectifs concrets tels que les suivants: développement produit, certification par les autorités de régulation, tests de conformité préalable et d'interopérabilité des produits TIC, évaluation de conformité des dispositifs mobiles et des protocoles IP, et services sur le terrain.

Public cible: opérateurs de télécommunication, équipementiers et utilisateurs (intérêts multiples – clients, opérateurs, associations, régulateurs, etc.).

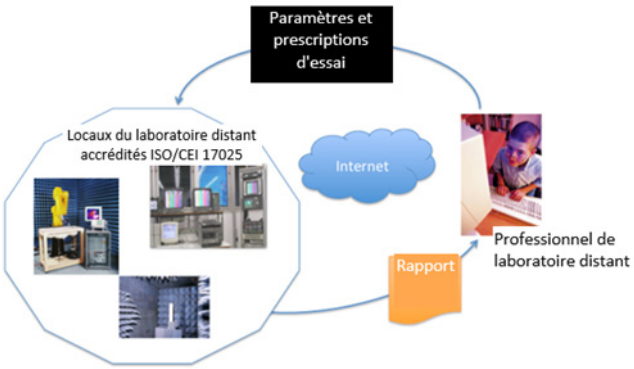
Afin de garantir une mise à jour rapide des infrastructures lorsque cela est nécessaire, il est souhaitable d'établir un partenariat solide et étroit avec les principaux fabricants de systèmes de test et de mesure.

2.5.3 Tests d'homologation à distance

Objectif: *Fournir un accès à des infrastructures physiques de test à distance à des fins d'homologation*

Les tests d'homologation à distance permettent le développement en laboratoire et la réalisation de tests de conformité préalable, de conformité et d'interopérabilité sur des échantillons de produits TIC en mode distant ou virtuel en utilisant les infrastructures d'autres laboratoires. Les échantillons seront fournis par d'autres entités (participation de la communauté).

Figure 3 – Test d'homologation à distance



Le niveau des services de laboratoire fournis peut évoluer par étapes:

- Étape 1: Formation à distance.
- Étape 2: Réalisation de tests sur les échantillons avec transmission vidéo de chaque étape et envoi de données pour l'élaboration de rapports.
- Étape 3: Le laboratoire local s'investit davantage dans la réalisation de tests sur certains types de produits, en particulier sur les produits du réseau central (dans le but de répondre au mieux aux besoins des infrastructures centrales).
- Étape 4: Mise à disposition d'infrastructures pour la réalisation des tests à distance (investissements dans des infrastructures de mesure adaptées).
- Étape 5: Conseil et formation en vue de se préparer à l'acquisition d'infrastructures de test au niveau local (si cela est jugé opportun).

Prescriptions: normes applicables, tests, évaluation, etc.

2.6 Surveillance du marché

La surveillance du marché des équipements de télécommunication déployés a pour objet de veiller à ce que les produits commercialisés ne provoquent pas de brouillages électromagnétiques, ne portent pas préjudice au réseau de télécommunication public, ne mettent pas en danger la santé ou la sécurité publique et ne portent pas atteinte à l'intérêt général de quelque façon que ce soit. Dans la pratique, la surveillance du marché consiste à prendre toutes les mesures nécessaires (y compris les interdictions, retraits et rappels) pour bloquer la diffusion de produits non conformes aux exigences définies dans la législation et les règlements pertinents, pour garantir la conformité des produits et pour appliquer des sanctions. La surveillance du marché est indispensable au bon fonctionnement du marché des télécommunications. Elle joue un rôle essentiel dans la protection des utilisateurs particuliers et professionnels contre les risques posés par des produits non conformes. Elle contribue de surcroît à protéger les entreprises responsables contre la concurrence déloyale d'acteurs économiques peu scrupuleux qui ne respectent pas les règles ou n'hésitent pas à sacrifier la qualité. Les organismes de régulation de nombreux pays imposent des obligations légales précises en matière d'organisation de la surveillance du marché. Généralement, les règlements énoncent clairement les obligations des autorités de surveillance du marché et précisent qu'elles doivent détenir les pouvoirs, les ressources et les connaissances nécessaires pour s'acquitter correctement de leurs fonctions. Des procédures doivent être mises en place pour traiter les plaintes, suivre les accidents, vérifier que des mesures correctives sont prises et réunir des connaissances scientifiques et techniques sur les questions de sécurité.

2.6.1 Principales parties prenantes

Les principales parties prenantes sont:

- les gouvernements/régulateurs;
- les organismes d'accréditation;
- les organismes d'évaluation de la conformité;
- les fabricants, les importateurs, les vendeurs et les prestataires de services.

2.6.2 Consultations portant sur les renseignements et l'expérience issus de la surveillance du marché

Les activités réalisées à cet égard incluent:

- l'échange d'informations et la consultation avec d'autres pays disposant déjà d'un programme de surveillance du marché et de moyens d'application, en particulier avec les pays d'une même région appartenant à la même communauté linguistique et éventuellement dotés d'une gestion du spectre et d'assignations de fréquences aux services communes;
- l'envoi de notifications ou d'avertissements préalables aux partenaires si des technologies et des produits devant être déployés dans un pays ou une région donné(e) risquent de poser des problèmes de conformité, et alerter les partenaires de la possible non-conformité de ces produits ou technologies avant leur déploiement à plus grande échelle afin de pouvoir les soumettre à des inspections et des contrôles plus approfondis.

2.7 Évaluation de la conformité des nouvelles technologies

Dans la mesure où les services et les applications TIC sont présents dans tous les aspects de la vie humaine et où l'explosion des nouvelles technologies (notamment de l'Internet des objets et de la 5G) devient une réalité, la conformité et l'interopérabilité constitueront un problème de taille pour les pays en développement qui ne s'y seront pas préparés à temps.

Le scénario attendu d'un monde où tous les objets seront connectés intensifie la demande en matière de conformité et d'interopérabilité. Les pays en développement sont à la recherche de solutions innovantes pour faire face aux différents problèmes qui se posent à eux et effectuent notamment les actions suivantes:

- Instauration de prescriptions techniques communes.
- Identification des principales références techniques au niveau international (normes).
- Élaboration de politiques permettant d'établir des cadres de C&I solides afin de promouvoir la collaboration dans un environnement TIC caractérisé par la multiplicité des parties prenantes (par exemple grâce à l'instauration de mécanismes prévoyant l'acceptation des déclarations des fournisseurs et la conclusion d'accords de reconnaissance mutuelle).

2.7.1 Les défis des nouvelles technologies

Les nouvelles technologies posent les défis suivants:

- Les problèmes d'interopérabilité nécessitent de déployer des efforts pour:
  - sensibiliser davantage le régulateur à ces technologies
  - faire comprendre que les réglementations ne doivent pas être perçues comme un obstacle à l'entrée.

- Les développeurs doivent saisir ce qu'est la C&I et connaître:
  - les coûts financiers
  - les coûts sur le plan de la sécurité et des ressources humaines.
- Les fonds et ressources disponibles pour les projets/produits sont limités:
  - coûts de certification
  - marchés relativement nouveaux.

2.7.2 Essais de conformité préalable

Les essais de conformité préalable nécessitent:

- une sensibilisation à la C&I:
  - correspondant à la conception d'un produit donné;
  - à chaque étape du processus de commercialisation d'un produit;
- une sensibilisation aux effets de la C&I:
  - évaluation des coûts (en temps, financiers et techniques) pour une start-up;
  - les réglementations doivent être perçues comme un avantage et non comme un obstacle.

2.7.3 Effets escomptés[8]

Il est possible d'améliorer les perspectives de succès grâce à la C&I en réalisant les actions suivantes:

- Favoriser une gamme de produits intelligente.
- Intégrer la C&I dès le début.
- Identifier les personnes et les ressources nécessaires et savoir à quel moment il faudra en disposer.

Grâce à la C&I, les régulateurs peuvent doper la croissance des nouveaux produits et des nouvelles entreprises:

- en plaidant pour des ARM transversaux;
- en favorisant des discussions éclairées avec les entrepreneurs.

[8] UIT. Session thématique sur la Question 4/2. 16 octobre 2019.

Chapitre 3 – Lutte contre la multiplication des dispositifs contrefaits, des dispositifs de mauvaise qualité et des dispositifs ayant subi une altération volontaire

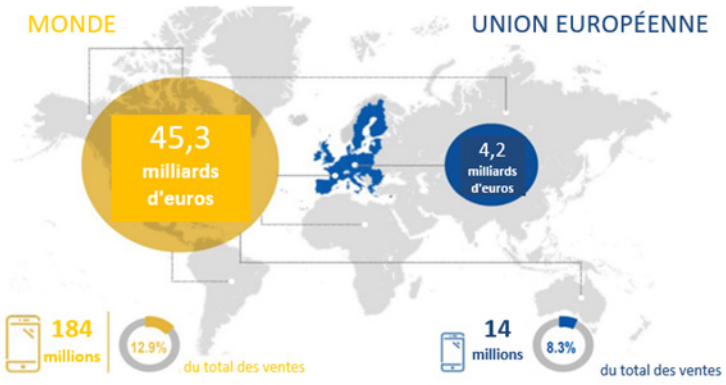
Aujourd'hui, le marché des dispositifs TIC contrefaits et le commerce de dispositifs mobiles contrefaits constituent un problème socio-économique mondial produisant des effets négatifs sur l'innovation, l'investissement, la croissance économique, la santé et l'emploi. De plus, les ressources risquent d'être détournées vers le crime organisé.

Dans la Résolution 79 (Rév.Buenos Aires, 2017) de la Conférence mondiale du développement des télécommunications de 2017 (CMDT-17), la lutte contre la multiplication des équipements et dispositifs de contrefaçon est considérée comme une priorité au titre de la Question 4/2. Le présent chapitre contient une description des problèmes posés par la contrefaçon des dispositifs de télécommunication/TIC et des lignes directrices pour les identifier et lutter contre leur utilisation.

3.1 Problèmes et enjeux

La contrefaçon des équipements de télécommunication/TIC, en particulier des téléphones mobiles, représente un défi pour les utilisateurs, les fabricants et les gouvernements à l'échelle mondiale, ainsi que pour l'innovation, l'investissement et la croissance économique. L'Office de l'Union européenne pour la propriété intellectuelle (EUIPO) a estimé à 45,3 milliards d'euros le montant des ventes manquées de smartphones en 2015 à cause de la contrefaçon[9].

Figure 4 – Ventes manquées en raison de faux smartphones dans l'UE et dans le monde



[9] EUIPO. Études sur les faux smartphones. Octobre 2018.

Les utilisateurs tirent certains avantages de la contrefaçon des terminaux qui conduisent à leur multiplication, dont les suivants:

- Les dispositifs contrefaits et les dispositifs ayant subi une altération volontaire peuvent être plus abordables financièrement que les dispositifs authentiques et permettent d'accéder à des réseaux.
- Ces dispositifs offrent aux utilisateurs des fonctionnalités pratiques (cartes SIM multiples, télévision, radio FM, entre autres) et d'autres services Internet sur mobile pratiques (messagerie instantanée, appels vidéo, navigation web, transferts d'argent, etc.) à faible coût.

Plusieurs facteurs sont à l'origine des effets négatifs des terminaux de contrefaçon sur la santé humaine, la qualité du réseau et des services et les finances, notamment les suivants:

- Les dispositifs qui ne sont pas fiables représentent une menace pour la santé humaine et l'environnement, car ils contiennent des matériaux dangereux (tels que le plomb ou le cadmium), affichent un débit d'absorption spécifique (DAS) élevé ou sont sujets à des explosions de batterie.
- Les dispositifs de contrefaçon sont à l'origine d'une dégradation de la qualité de service (problèmes d'accessibilité de la voix, appels manqués, problèmes de mobilité (transfert intercellulaire) ou encore débit moins élevé).
- Ces dispositifs entraînent des pertes financières pour les fabricants de terminaux authentiques (ventes manquées, éventuelle dégradation des prix).
- Ces dispositifs entraînent des pertes fiscales (recettes fiscales et taxes appliquées).
- Ces dispositifs constituent une infraction au droit de propriété intellectuelle et aux marques commerciales et sont à l'origine d'une concurrence déloyale.
- Ces dispositifs entraînent une perte de garantie et d'appui technique.
- Ces dispositifs produisent des effets négatifs sur le fonctionnement des réseaux de télécommunication étant donné que leur puissance est moins contrôlable.

L'entreprise Qualcomm a montré dans un rapport[10] que la contrefaçon des équipements a des répercussions négatives sur le fonctionnement des réseaux pour les raisons suivantes:

- La capacité de réseau est réduite: en effet, on observe une baisse de capacité de 23% pour les données LTE (Long-Term Evolution), de 6% pour les données HSPA (accès haut débit en mode paquet) et de 27% pour la téléphonie UMTS (système de télécommunications mobiles universelles).
- Les dernières fonctionnalités LTE sont moins prises en charge par les dispositifs de contrefaçon, telles que le regroupement des porteuses (LTE-CA), la technique MIMO 4 x 4 (technique d'entrées multiples et de sorties multiples), la modulation 256 QAM (modulation d'amplitude en quadrature), ce qui finit par nuire à l'expérience des utilisateurs en général.
- Les besoins en sites du réseau augmentent, occasionnant ainsi des dépenses d'investissement et d'exploitation supplémentaires qui auront des répercussions négatives sur la rentabilité des activités des opérateurs mobiles.

Les problèmes liés aux dispositifs de contrefaçon dont le code IMEI n'est pas valide sont notamment les suivants:

- Il n'est pas facile d'identifier les dispositifs mobiles de contrefaçon ni de les bloquer, car bon nombre d'entre eux ont des codes IMEI d'apparence authentique. Les contrefacteurs ont pour habitude d'utiliser des séries de numéros IMEI pour leurs produits qui correspondent

[10] Qualcomm. Lutte contre la contrefaçon et le vol de téléphones mobiles. Octobre 2018.

à ceux attribués à des fabricants de dispositifs autorisés, ce qui rend difficile la distinction entre les produits autorisés et les produits de contrefaçon.

- Ces dispositifs représentent une menace pour la sécurité publique, car ils pourraient favoriser des activités criminelles et terroristes.
- Les perturbations dues au blocage de dispositifs de contrefaçon déjà vendus pénalisent souvent les utilisateurs, et non ceux qui commercialisent des produits frauduleux.

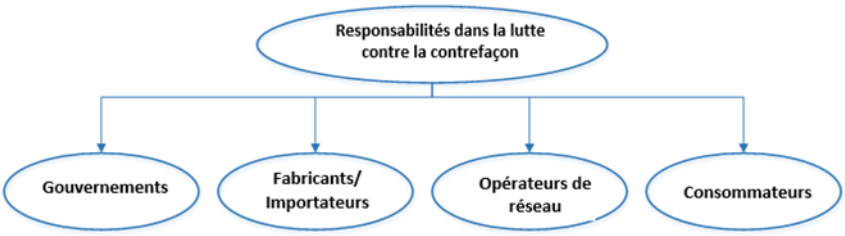
3.2 Définitions

- **Terminal**: installation connectée à un réseau de télécommunication et qui assure l'accès à un ou plusieurs services fournis par ce réseau (Recommandation UIT-R V.662-3)[11].
- **IMEI** (Identité internationale de l'équipement mobile): code unique attribué à chaque terminal mobile IMT-2000 par le fabricant et servant à identifier le terminal IMT-2000 auprès du réseau aux fins de validation de l'équipement terminal ou à d'autres fins similaires.
- **EIR** (Registre d'identité d'équipement): registre auquel peut être attribuée l'identité de l'équipement d'utilisateur pour des besoins d'enregistrement. La nature, l'objet et l'utilisation de ces informations nécessitent un complément d'étude.
- **Liste blanche**: répertoire des dispositifs dont l'utilisation est autorisée dans un pays donné (y compris les dispositifs ayant été importés ou fabriqués légalement dans ce pays).
- **Liste noire**: répertoire des dispositifs pour lesquels les services doivent être rejetés dans le réseau de télécommunication.

3.3 Lignes directrices

Il importe que tous les acteurs (c'est-à-dire les gouvernements, fabricants, opérateurs de réseau et consommateurs) travaillent en bonne intelligence pour lutter contre la multiplication des équipements de télécommunication/TIC contrefaits.

Figure 5 – Responsabilités dans la lutte contre la contrefaçon



Il est essentiel d'instaurer une collaboration afin de créer un cadre réglementaire et technique pour lutter contre la multiplication des produits de contrefaçon. Pour ce faire:

- les gouvernements et les régulateurs devraient élaborer des cadres réglementaires en vue d'appliquer des procédures normalisées, et déployer une plate-forme technique afin de veiller au respect de la réglementation; organiser des campagnes de sensibilisation portant notamment sur les risques qu'entraînent les dispositifs contrefaits pour les utilisateurs, tels que des risques sanitaires et une faible qualité de service; et encourager la surveillance de marché pour entraver le commerce de ces dispositifs sur le marché noir;

[11] Secteur des radiocommunications de l'UIT (UIT-R). Recommandation UIT-R V.662-3 (05/2000). Termes et définitions.

- les gouvernements devraient songer à réduire les taxes et les droits appliqués aux dispositifs TIC licites importés, ce qui pourrait aussi faire baisser le coût de possession;
- au niveau national, les régulateurs devraient collaborer avec les fabricants et les opérateurs de réseau pour déterminer l'étendue de l'utilisation de dispositifs de contrefaçon sur le marché local;
- il convient de doter les services de douane et de sécurité des moyens nécessaires pour lutter contre le trafic illicite et vérifier la légitimité des identificateurs des dispositifs à leur point d'importation;
- les fabricants et les importateurs devraient enregistrer tous les équipements importés et fabriqués localement et respecter les procédures d'homologation établies par le régulateur;
- les fabricants devraient renforcer la sécurité des codes IMEI en se conformant aux principes de conception technique en vue de la mise en œuvre de la sécurité des identités IMEI, et en participant à la procédure établie par la GSM Association (GSMA) pour notifier les vulnérabilités de sécurité des identités IMEI et y remédier;
- les opérateurs peuvent contribuer à la lutte contre la multiplication des dispositifs de contrefaçon en fournissant des données relatives au réseau de dispositifs au régulateur et aux acteurs du gouvernement; en établissant une base de données EIR qui contient la liste noire et la liste blanche des identités IMEI, afin de refuser l'accès au réseau aux dispositifs de contrefaçon; et en informant les abonnés du statut de leur dispositif par SMS, si nécessaire;
- les clients peuvent apporter leur contribution en vérifiant l'authenticité des dispositifs qu'ils envisagent d'acheter en recourant à des services de vérification fournis par d'autres acteurs; en enregistrant des dispositifs importés à titre individuel; et en signalant des dispositifs de contrefaçon aux autorités;
- un régime d'évaluation de la conformité devrait être établi, tout comme une base de données nationale centralisée qui contient toutes les informations sur les dispositifs (identifiants, spécifications techniques, cycle de vie des dispositifs, etc.) pour permettre une surveillance efficace du marché.

D'après l'expérience de pays tels que le Rwanda (voir la section 3.4.4), il semble que les principes suivants s'appliquent au niveau régional:

- Il importe pour les pays de conclure des accords de reconnaissance mutuelle sur l'évaluation de la conformité et la surveillance du marché.
- Un système centralisé de contrôle des équipements pourrait réduire considérablement le nombre de dispositifs de contrefaçon et de dispositifs de mauvaise qualité qui accèdent au marché.
- Des centres d'essai reconnus à l'échelle régionale pourraient jouer un rôle très important dans la mise en œuvre de l'évaluation de la conformité en délivrant des certifications et des déclarations de conformité du fournisseur.

3.4 Expérience nationale (études de cas)

Les contributions des États Membres et des parties prenantes se sont avérées essentielles pour préparer le présent rapport. Ces contributions reposent sur l'expérience nationale, des données et les pratiques existantes pour lutter contre la multiplication des dispositifs contrefaits.

Tous les contributeurs conviennent de la nécessité de créer des cadres politiques, juridiques et réglementaires applicables.

Certains contributeurs proposent de recourir à des solutions techniques existantes, telles que des normes internationales et des techniques de surveillance du marché, et de créer des bases de données et des plates-formes centrales pour bloquer les dispositifs contrefaits.

De plus, plusieurs contributeurs suggèrent de déployer des efforts supplémentaires aux niveaux régional et sous-régional, afin de mettre en commun les différentes techniques permettant de lutter contre la contrefaçon des dispositifs.

3.4.1 Madagascar

À Madagascar, 25% des dispositifs actifs sur les réseaux mobiles sont des produits de contrefaçon[12]. Même si ces dispositifs présentent certains atouts (ils sont financièrement abordables, permettent d'accéder à des services universels et de réduire la fracture numérique), leurs avantages sont contrebalancés par les différents risques qu'ils posent pour la santé humaine (par exemple s'agissant du niveau des émissions dangereuses), pour les opérateurs (qualité de service, brouillages, etc.) et pour l'économie du pays.

Afin d'éviter que le développement numérique ne se fasse au détriment de la santé humaine et de l'économie, Madagascar a adopté des mesures visant à:

- sensibiliser davantage les utilisateurs aux dangers que présentent les dispositifs contrefaits;
- fermer le marché noir et appliquer des mesures douanières;
- interdire les terminaux de contrefaçon et veiller à certifier les équipements TIC importés;
- utiliser une plate-forme pour l'analyse et l'identification des codes IMEI, et bloquer les dispositifs de contrefaçon à compter du 30 juin 2019.

3.4.2 Guinée

Dans sa contribution, le Gouvernement de la Guinée met en exergue les préoccupations liées à la certification des équipements et des infrastructures de télécommunications, ainsi qu'à l'interopérabilité des services de télécommunication[13]. Depuis 2015, le gouvernement a promulgué des lois sur les télécommunications qui ont restructuré le secteur. Ces réformes ont eu des effets bénéfiques, tels que l'augmentation de la réserve de numéros de téléphone, l'amélioration de la qualité de service, la contribution accrue du secteur au produit intérieur brut, le contrôle du marché du numérique et de la certification.

Le gouvernement applique des règles particulièrement strictes concernant la certification des équipements de télécommunication, ainsi que des contre-mesures et des sanctions pour décourager les malfaiteurs. L'évaluation de la conformité des équipements terminaux aux prescriptions essentielles est menée par l'Autorité de régulation des postes et des télécommunications (ARPT), qui exige des dossiers administratifs et techniques très détaillés. À l'issue de l'évaluation, des certificats de conformité sont délivrés. Les mesures suivantes ont été prises en Guinée:

- Suivi rigoureux et permanent des travaux de l'UIT en matière de normalisation.
- Participation de plusieurs acteurs, en particulier de l'ARPT, des services douaniers, des autorités fiscales et des ministères.
- Homologation d'équipements de télécommunication, valable pendant une période de cinq ans renouvelable.
- Mise en place d'un système d'étiquetage des équipements homologués.
- Saisie de l'équipement ou démantèlement des installations ayant subi la contrefaçon, aux frais de l'auteur de l'infraction.

---

[12] Document 2/45 (Madagascar) de la CE 2 de l'UIT-D.
[13] Document SG2RGQ/9(Rév. 1) (Guinée) de la CE 2 de l'UIT-D.

- Confiscation de l'équipement contrefait prononcée par une instance compétente.
- Sanctions pour défaut d'enregistrement: toute personne ou toute entité qui détient en vue de la vente ou de la distribution à titre gratuit ou onéreux, qui vend un équipement terminal ou un équipement radioélectrique prévu au titre de la loi, et le connecte à un réseau public de télécommunication/TIC, en violation du régime de certification ou en l'absence d'une approbation préalable, est passible d'une amende de 10 millions à 200 millions de francs guinéens.
- En cas de récidive, les amendes sont doublées.

3.4.3 Sénégal

Outre le fait qu'il lutte efficacement contre le piratage, la contrefaçon et le vol des dispositifs de télécommunication/TIC et qu'il prend des mesures pour s'adapter aux changements de l'environnement juridique, le Gouvernement du Sénégal, en collaboration avec des réseaux continentaux et intercontinentaux, des multinationales, des régulateurs des télécommunications/TIC et des fournisseurs de services Internet, a entrepris des initiatives importantes en vue de lutter contre ces fléaux des temps modernes, qui constituent un obstacle à l'innovation technologique, à la création d'emploi et de richesses, ainsi qu'aux investissements directs à l'étranger[14].

Le Sénégal a établi des mesures d'ordre juridique et réglementaire et a pris d'autres mesures afin de mieux protéger la propriété individuelle. On citera notamment:

- un cadre juridique fondé sur un ensemble de lois;
- un cadre réglementaire fondé sur un ensemble de décrets;
- une brigade nationale chargée de lutter contre le piratage et la contrefaçon;
- l'Agence sénégalaise pour la propriété industrielle et l'innovation technologique;
- l'Autorité de régulation des télécommunications et des postes (ARTP);
- l'autorité nationale des douanes;
- la participation d'entreprises nationales et multinationales de fabrication et de distribution de téléphones, de tablettes, de smartphones et de décodeurs.

3.4.4 Rwanda

Le Gouvernement du Rwanda, conscient des dangers qu'entraînent les dispositifs contrefaits pour le consommateur, l'industrie et l'économie, a élaboré une stratégie visant à lutter contre la multiplication des dispositifs de contrefaçon et établi une feuille de route à l'échelle régionale, en collaboration avec les États Membres appartenant à la Communauté est-Africaine (CEA)[15]. Le gouvernement a formulé les propositions suivantes:

- Des accords mutuels entre les États Membres de la CEA: examiner les instruments juridiques et réglementaires des États Membres en vue de conclure des accords de reconnaissance mutuelle visant à mener des activités d'évaluation de la conformité et renforcer la surveillance du marché.
- Un système de suivi centralisé: l'établissement d'un système de contrôle en temps réel reposant sur le verrouillage de carte SIM fondé sur le registre EIR, l'autorisation préalable de l'IMEI, l'autorisation de l'IMEI et les alertes du registre EIR constituerait la meilleure solution pour lutter contre la multiplication des dispositifs illicites au niveau régional.

[14] Document SG2RGQ/66(Rév. 1) (Sénégal) de la CE 2 de l'UIT-D [disponible en français].
[15] Document SG2RGQ/69 (Rwanda) de la CE 2 de l'UIT-D.

- Des centres de tests régionaux: la création de centres de tests régionaux accrédités délivrant des certifications et les déclarations de conformité des fournisseurs faciliterait l'évaluation de la conformité dans les États Membres de la CEA. Cela réduira les coûts de la certification pour les usines d'assemblage de la région et le coût du produit final. La conclusion d'accords mutuels entre les pays favorisera la création de laboratoires spécialisés dans différents pays.

3.4.5 Zimbabwe

Tous les opérateurs de réseau mobile au Zimbabwe disposent de moyens pour détecter la présence dans leurs réseaux de dispositifs de contrefaçon dont les codes IMEI ont été dupliqués et pour les désactiver. Cependant, compte tenu de l'importance des dispositifs de contrefaçon pour les revenus des opérateurs – ces dispositifs sont utilisés par la majorité des utilisateurs de réseau – il est rare que les dispositifs soient effectivement désactivés[16]. Les mesures suivantes ont néanmoins été prises au Zimbabwe afin de lutter contre la multiplication des dispositifs de contrefaçon et le vol de dispositifs mobiles:

- L'utilisation de tout dispositif qui ne répond pas aux prescriptions requises pour l'homologation est interdite.
- Tout abonné du service mobile qui achète une nouvelle carte SIM doit enregistrer celle-ci auprès de l'opérateur de réseau mobile avant qu'elle ne soit activée sur le réseau.
- Le pays s'est procuré une base de données pour l'enregistrement des abonnés visant à veiller à ce que toutes les cartes SIM activées dans le pays soient correctement enregistrées, ce qui facilite aussi la détection de dispositifs de contrefaçon et de téléphones mobiles frauduleux.
- Au niveau régional, l'Autorité indépendante des télécommunications d'Afrique du Sud (ICASA) possède un laboratoire d'essai indépendant qui teste et certifie tous les nouveaux équipements TIC.

3.4.6 Ghana

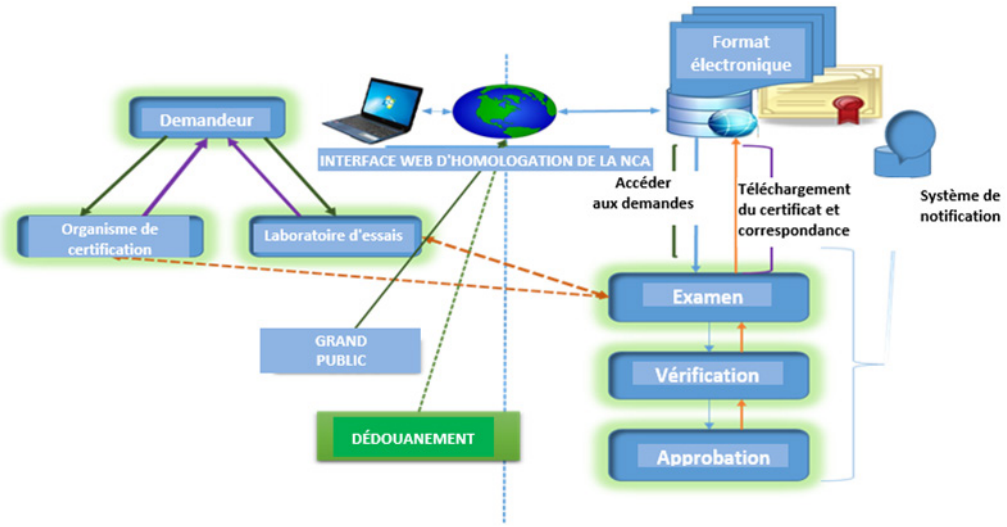
Au Ghana, des activités d'homologation sont menées pour protéger les dispositifs de télécommunication/TIC, les utilisateurs et les réseaux[17]. L'Autorité nationale des communications (NCA) a créé un régime d'homologation pour certifier les équipements de communication et tester leur conformité aux normes internationales:

- mise en œuvre d'une procédure d'homologation fondée sur la documentation technique contenant des rapports d'essais et des exigences de conformité concernant la protection des consommateurs, la protection de l'environnement, la perturbation des réseaux, l'intégrité et l'interopérabilité, ainsi que des dispositions visant à garantir la conformité au plan national d'attribution des bandes de fréquences;
- attribution du certificat d'homologation (TAC) et sceau de la NCA, et publication des informations relatives aux équipements sur le site web de la NCA;
- mise en place d'un système d'octroi de licences de distribution intégré dans le régime d'homologation, afin de rationaliser les activités des distributeurs d'équipements de communications électroniques et de veiller à ce que seuls des dispositifs TIC homologués soient utilisés;
- arrangements visant à renforcer la surveillance du marché national;

[16] Document SG2RGQ/85 (Zimbabwe) de la CE 2 de l'UIT-D.
[17] Document SG2RGQ/82 (Ghana) de la CE 2 de l'UIT-D.

– création de laboratoires d'essais pour effectuer des mesures relatives au débit d'absorption spécifique (DAS), aux champs électromagnétiques (CEM), à la télévision numérique de Terre (DTT) et aux radiofréquences et à la signalisation.

Figure 6 – Le processus d'homologation

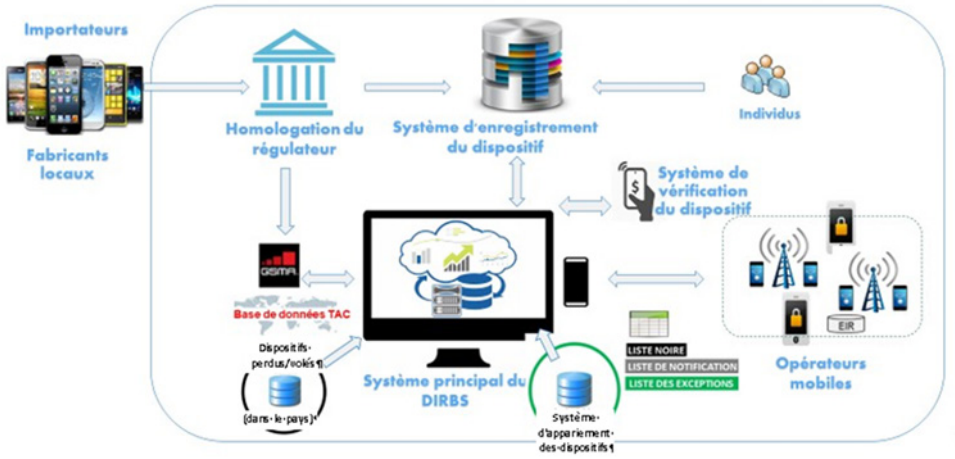


3.4.7 Pakistan

L'Autorité des télécommunications du Pakistan a lancé, en collaboration avec Qualcomm, une plate-forme technique à code source ouvert, appelée "Système d'identification, d'enregistrement et de blocage des dispositifs" (DIRBS), afin de veiller à ce que seuls les dispositifs homologués et licites puissent être exploités sur les réseaux mobiles du pays[18]. Le système DIRBS permet d'identifier tous les dispositifs; répertorie les dispositifs du parc installé; assure le suivi de l'activation de tous les nouveaux dispositifs; permet de lutter contre les dispositifs illicites et les dispositifs de contrefaçon, y compris contre le vol de dispositifs; et prévoit des exceptions et des cas d'amnistie.

[18] On trouvera de plus amples renseignements sur le système DIRBS sur le site web de l'Autorité des télécommunications du Pakistan (PTA) et de la Commission fédérale des recettes publiques du Pakistan.

Figure 7 – Système d'identification, d'enregistrement et de blocage des dispositifs (DIRBS)



3.4.8 La GSM Association

La GSM Association (GSMA) tient la base de données des numéros d'identité internationale d'équipement mobile. Cette base de données mondiale et centralisée rassemble des informations de base sur des séries de numéros IMEI de millions de dispositifs mobiles[19].

La GSMA propose un service de "vérification de dispositifs" aux commerçants, aux recycleurs et aux assureurs, ainsi qu'aux autorités chargées de l'application de la loi (dans certains marchés, les consommateurs peuvent aussi accéder directement au service). En consultant le registre sur le statut des dispositifs, les utilisateurs peuvent alors savoir instantanément si le dispositif a été déclaré perdu ou volé par des opérateurs de réseau mobile du monde entier membres de la GSMA.

La GSMA vise à connecter le plus d'opérateurs de réseau mobile possibles à la base de données des identités IMEI.

La GSMA et l'Organisation mondiale des douanes (OMD) se sont associées en septembre 2016 pour lutter contre le commerce de dispositifs mobiles de contrefaçon et frauduleux. L'intégration de la base de données des identités IMEI permettra de recouper et de filtrer les renseignements concernant les dispositifs de contrefaçon identifiés au moyen de leur identité IMEI au point d'importation.

3.4.9 Brésil

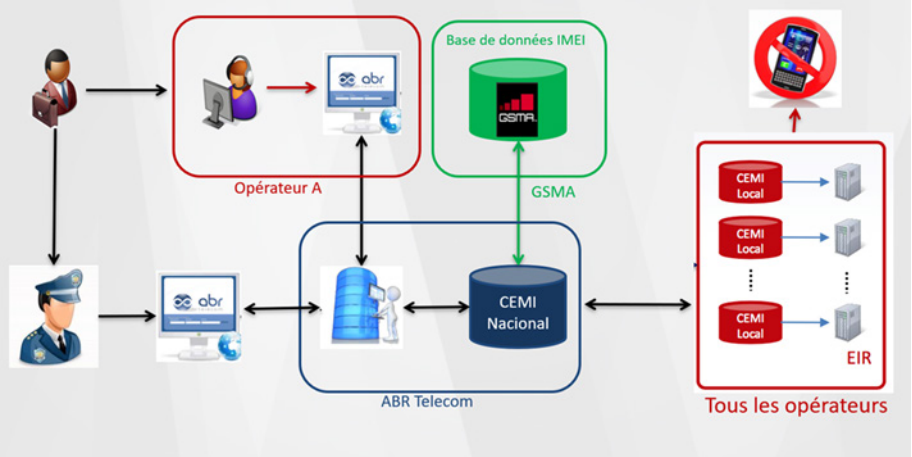
Afin de lutter contre l'utilisation d'identifiants uniques volés, falsifiés et non certifiés, le Gouvernement du Brésil a lancé l'initiative *Celular Legal*, coordonnée par l'*Agência Nacional*

[19] Document SG2RGQ/80 (GSM Association (GSMA)) de la CE 2 de l'UIT-D.

de Telecomunicações (ANATEL) et dans laquelle toutes les parties prenantes sont mobilisées[20]. Les mesures appliquées dans le cadre de cette initiative s'articulent autour de deux modules:

- Le module CEMI (*Cadastro de Estações Móveis Impedidas*) permet aux opérateurs mobiles et à la police de bloquer les dispositifs volés à la demande de l'utilisateur.

Figure 8 – Déroulement des opérations du module CEMI



- Le module SIGA (*Sistema Integrado de Gestão de Aparelhos*) est utilisé pour identifier et bloquer les dispositifs ayant un lien avec d'autres types de fraude: altération, clonage, dispositifs non certifiés, identifiants uniques incohérents, etc. L'initiative *Celular Legal* est assortie d'un outil en ligne permettant de vérifier le statut d'un dispositif au moyen de son code IMEI[21].

3.4.10 Oman

Parmi les dispositifs mobiles enregistrés sur le réseau national d'Oman, près de 2 millions possèdent une identité IMEI non valide. Certains numéros IMEI ont été reproduits une dizaine de fois, puisque plus de 10 dispositifs disposent du même numéro IMEI[22]. Cela pose un problème technique en matière d'enregistrement de ces dispositifs sur les réseaux locaux, alourdit la charge financière imposée à l'ensemble des consommateurs et sape la confiance à l'égard de ces produits.

Les régulateurs sont disposés à veiller à ce que tous les dispositifs TIC distribués et importés disponibles sur le marché soient pleinement conformes aux ordres et aux décisions de l'autorité de réglementation. Pour ce faire, l'organisme de contrôle de l'Autorité de réglementation des télécommunications (TRA) est chargé de veiller à ce que l'utilisation des équipements TIC commercialisés sur le marché national soit compatible avec les normes et spécifications techniques applicables et conforme à celles-ci.

La TRA a mis à la disposition des consommateurs un service d'assistance et des opérateurs locaux leur permettant de vérifier leur code IMEI. L'organisation est toujours confrontée à des difficultés, notamment à l'impossibilité d'accéder à une base de données internationale

[20] João Zanon, Combating to the use of stolen and counterfeit ICT devices. *Atelier de l'UIT-D sur le thème de la lutte contre la contrefaçon d'équipements TIC*, Genève, 4 octobre 2018.
[21] *Agência Nacional de Telecomunicações* (ANATEL). Cellular Legal.
[22] Document 2/326 (Oman) de la CE 2 de l'UIT-D.

des identités IMEI, car contrairement aux fabricants et aux opérateurs d'un pays donné, les régulateurs ne peuvent pas accéder sans restriction à la base de données de la GSMA.

3.4.11 Normes et recommandations internationales

- ISO 12931:2012: Critères de performance des solutions d'authentification utilisées pour combattre la contrefaçon des biens matériels.
- ISO 16678:2014: Lignes directrices pour l'identification interopérable d'objets et systèmes d'authentification associés destinés à décourager la contrefaçon et le commerce illicite.
- UIT-T Q.5050 (03/2019): Lutte contre la contrefaçon et le vol de dispositifs TIC.
- UIT-T Y.4808 (08/2020): Cadre de l'architecture d'entité numérique pour la lutte contre la contrefaçon dans l'Internet des objets.

Chapitre 4 – Le vol de dispositifs mobiles

4.1 Introduction

L'utilisation accrue de dispositifs mobiles dans le monde s'est accompagnée d'une hausse de l'utilisation de dispositifs volés, aussi bien au niveau national qu'international. Il est nécessaire de mettre en œuvre des initiatives mondiales afin d'empêcher les dispositifs volés d'accéder aux réseaux du monde entier.

Compte tenu de l'étendue des dommages causés par l'utilisation de dispositifs frauduleux dans tout l'écosystème, les gouvernements et les secteurs d'activité se mobilisent davantage pour trouver des solutions. Les gouvernements appliquent des réglementations portant sur toute une série de questions, notamment les suivantes:

- le vol de mobiles;
- les risques en matière de sécurité;
- les pertes de recettes fiscales;
- la vie privée des consommateurs;
- la qualité du réseau;
- les droits de propriété intellectuelle.

Depuis de nombreuses années, la GSMA est à l'avant-garde d'initiatives sectorielles relatives au partage de données afin d'empêcher les dispositifs mobiles volés ou perdus d'accéder aux réseaux du monde entier. Sur la base du code IMEI unique, la GSMA répertorie les dispositifs suspects, c'est-à-dire ceux déclarés comme étant perdus ou volés, dans une liste noire qui est à disposition des opérateurs du monde entier[23].

4.2 Problèmes et enjeux

Le vol de dispositifs est un problème mondial qui nécessite une coordination et des mesures transfrontières afin de rendre le vol peu intéressant sur le plan économique. Bien que des initiatives sectorielles produisent des effets positifs, il est nécessaire de déployer des efforts supplémentaires, car à ce jour, la plupart des activités reposent sur des normes mondiales non-propriétaires, et certains pays doivent encore mettre en adéquation leurs actions avec les pratiques sectorielles mondiales. À cet égard, les pays doivent adopter une approche commune en matière d'harmonisation mondiale avec les pratiques sectorielles. L'inaction compromet l'efficacité de certaines des mesures mises en œuvre.

Les exigences visant à remédier au vol de dispositifs relèvent des catégories suivantes.

Réglementation et application

- instaurer un cadre réglementaire;

[23] Document SG2RGQ/80 (GSMA) de la CE 2 de l'UIT-D.

- mettre en œuvre des procédures opérationnelles normalisées;
- créer et gérer une plate-forme technologique permettant de faire appliquer les réglementations;
- mener des campagnes de sensibilisation.

Plate-forme technique

- classement des dispositifs existants:
  - analyser les données des dispositifs à partir des informations sur le réseau;
  - classer les dispositifs en fonction de leur numéro IMEI (valide/non valide, unique/répété)
- autorisation des dispositifs existants:
  - associer les numéros IMEI existants à l'identité internationale d'abonné mobile (IMSI) et au numéro international d'abonné mobile (MSISDN);
- enregistrement des nouveaux dispositifs:
  - exiger que les dispositifs soient homologués et possèdent des identifiants uniques;
  - enregistrer seulement les dispositifs importés et fabriqués localement possédant des identifiants uniques et valides;
- détection des numéros IMEI frauduleux:
  - analyser les données du réseau;
  - identifier les dispositifs dont le numéro IMEI est frauduleux;
- possibilité de bloquer l'accès au réseau:
  - surveiller l'accès des dispositifs non conformes/non enregistrés en contrôlant le réseau.

Mise en œuvre du système technique[24]

- un système commode pour toutes les parties prenantes, en particulier pour les consommateurs;
- un système autonome réduisant la nécessité d'intégration dans le réseau mobile et d'interopérabilité qui entraîne des coûts inutiles, des contraintes de capacité et des charges pour les opérateurs en termes de ressources;
- pas d'exigence de rattachement strict entre le dispositif et le consommateur;
- un système flexible/configurable permettant de s'adapter aux réglementations nationales sans qu'une personnalisation soit nécessaire.

4.2.1 Délits et fraudes concernant les dispositifs

Les délits et les fraudes dont les dispositifs font l'objet ont des répercussions négatives sur plusieurs groupes de parties prenantes:

- les consommateurs peuvent subir des préjudices liés au vol et risquent de perdre leur bien et leurs données personnelles;

[24] Mohammad Raheel Kamal. An Open Source CEIR to Combat Counterfeit and Stolen ICT Devices. *Troisième atelier régional de la Commission d'études 11 de l'UIT-T pour l'Afrique sur "Les défis liés à la contrefaçon de dispositifs TIC et aux tests de conformité et d'interopérabilité en Afrique"*. Tunis, 30 septembre 2019.

- les gouvernements sont confrontés à une hausse de la délinquance et à une baisse des recettes fiscales;
- les commerçants achètent à leur insu des biens volés et font face à des problèmes de fonctionnement du réseau;
- les assureurs voient leurs frais liés aux opérations d'assurance augmenter et leurs assurés se retrouvent propriétaires de biens volés;
- les opérateurs perdent des abonnés et des subventions, et déboursent des frais d'opérations d'assurance;
- les autorités chargées de l'application de la loi sont confrontées au crime organisé et à un épuisement de leurs ressources humaines.

4.2.2 Rôles et responsabilités des parties prenantes

Plusieurs parties prenantes peuvent jouer un rôle important dans la lutte contre le vol de dispositifs.

Les **gouvernements** peuvent élaborer un cadre réglementaire, appliquer des procédures opérationnelles normalisées, déployer et gérer des technologies afin de veiller au respect de la réglementation, et mener des campagnes de sensibilisation.

Les **fabricants et les importateurs** peuvent faire homologuer leurs dispositifs auprès des gouvernements et des régulateurs, et enregistrer l'intégralité des dispositifs devant être importés et des dispositifs fabriqués localement.

Les **opérateurs** peuvent communiquer aux gouvernements des données de réseau relatives aux dispositifs, assurer la tenue du registre d'identité d'équipement (EIR), inscrire sur liste noire les codes IMEI valides/non valides et autoriser des exceptions, et informer les abonnés du statut de leur dispositif par SMS, s'il y a lieu.

Les **consommateurs** peuvent connaître le statut de leur dispositif (par SMS, sur une application ou une interface web), enregistrer les dispositifs importés à titre individuel, signaler aux autorités le vol de leur dispositif et présenter des preuves (factures) de possession de dispositifs authentiques, s'il y a lieu.

4.2.3 Les outils indispensables pour lutter contre le vol de dispositifs

Plusieurs mesures peuvent être appliquées aux réseaux et aux dispositifs pour lutter contre le vol de dispositifs.

Protection des dispositifs:

- offrir la possibilité de supprimer des contacts et des photos et de bloquer les paiements par mobile;
- intégrer une fonctionnalité de réinitialisation pour restaurer toutes les données;
- intégrer une fonctionnalité de suppression des données à distance.

Protection des réseaux:

- empêcher les téléphones volés d'accéder au réseau.

Vérification du statut du dispositif:

- vérifier le statut du dispositif avant sa réutilisation;

– faire du vol de téléphones une pratique non rentable.

4.3 Lignes directrices

Mobilisation multipartite

Les utilisateurs peuvent signaler le vol de leur dispositif aux opérateurs de réseau, activer des fonctionnalités anti-vol sur leurs dispositifs et, dans les pays où les opérateurs ont accès à la liste noire des identités IMEI de la GSMA, être invités à vérifier le statut du numéro IMEI des dispositifs d'occasion qu'ils prévoient d'acheter[25].

Les opérateurs de réseau mobile peuvent bloquer l'utilisation des dispositifs volés sur leur réseau, accéder à la liste noire des identités IMEI de la GSMA pour échanger et recueillir des données inscrites sur la liste noire, et inciter leurs fournisseurs de dispositifs à protéger convenablement l'intégrité de la mise en œuvre des identités IMEI dans leurs produits.

Les fabricants de dispositifs et les propriétaires de marques peuvent garantir l'intégrité des codes IMEI de tous leurs produits, concevoir des dispositifs plus sécurisés (en rendant impossible la reprogrammation des codes IMEI) et intégrer une fonctionnalité de neutralisation pour permettre aux utilisateurs de désactiver à distance les dispositifs perdus ou volés.

Les opérateurs de boutiques d'applications peuvent obtenir les codes IMEI des dispositifs volés auprès de la GSMA et les utiliser pour interdire aux dispositifs déclarés volés d'accéder à leurs boutiques.

Tous les acteurs (c'est-à-dire les gouvernements, fabricants, opérateurs de réseau et consommateurs) doivent travailler en bonne intelligence pour lutter contre le vol de dispositifs mobiles, notamment en effectuant les actions suivantes:

- Échanger avec les autorités chargées de l'application de la loi et les mobiliser.
- Surveiller les canaux de distribution pour lutter contre le trafic de dispositifs volés.
- Obtenir un appui législatif et judiciaire en ce qui concerne les initiatives de lutte contre le vol.
- Se concentrer sur les dispositifs et incommoder les consommateurs le moins possible.
- Insister davantage sur les efforts collectifs où tous les pays apportent une contribution.
- Adopter des mesures visant à soutenir les capacités existantes au lieu d'en créer de nouvelles ou de les affaiblir.
- Évaluer et commenter l'efficacité des approches adoptées.
- Analyser les mesures prises pour identifier ce qui fonctionne et ce qui ne fonctionne pas.
- Adopter des technologies et solutions nouvelles pour combler les lacunes.

Les gouvernements et les régulateurs doivent travailler de concert pour veiller à ce qui suit:

- Les opérateurs créent des registres EIR pour bloquer les dispositifs volés sur les réseaux locaux.
- Les lignes directrices sur les bonnes pratiques visant à bloquer les dispositifs et échanger des données sont appliquées.

---

[25] James Moran (GSMA). Combating device crime together – Best practice to combat mobile device theft. *Atelier de l'UIT sur les stratégies mondiales de lutte contre la contrefaçon et le vol d'équipements TIC*. Genève, 23 juillet 2018.

- Les registres EIR des opérateurs sont reliés à la base de données des identités IMEI pour garantir le blocage des dispositifs volés à l'échelle internationale.
- La sécurité des identités IMEI est renforcée et les problèmes les concernant sont signalés et résolus.
- Les codes IMEI sont vérifiés par les agents chargés de l'application de la loi, les agents douaniers, les commerçants et les consommateurs.
- Des poursuites sont engagées contre les auteurs d'infraction (altération des identités IMEI, vol et commerce de dispositifs frauduleux).
- Des mesures visant à sensibiliser les consommateurs et favoriser la neutralisation à distance sont adoptées.
- Des indicateurs permettant de mesurer l'avancée des efforts sont adoptés et des rapports sont présentés.

4.4 Expériences nationales (études de cas)

4.4.1 République centrafricaine

Dans le cadre de sa politique de développement des infrastructures TIC, le Gouvernement de la République centrafricaine a ouvert le marché des TIC à quatre opérateurs de téléphonie mobile et à un opérateur de téléphonie fixe pour s'assurer de couvrir au maximum le territoire national et offrir des services de qualité à la population[26].

Le défaut de mise en œuvre de cette politique par l'Autorité de régulation des communications électroniques et de la Poste (ARCEP) a conduit à un développement non réglementé des infrastructures, à des difficultés en matière d'évaluation de la conformité et de l'interopérabilité des équipements TIC, et à une progression de la contrefaçon et du vol de terminaux mobiles. Les investissements et les revenus du secteur en ont subi les conséquences.

Pour remédier à ces problèmes, le Gouvernement de la République centrafricaine:

- a adopté et promulgué la loi sur les communications électroniques et ses textes d'application;
- a adopté et promulgué la loi créant l'Autorité de régulation des communications électroniques et de la Poste (ARCEP);
- a présenté un projet de loi sur la cybercriminalité et la cybersécurité;
- a créé un centre de contrôle de trafic, de lutte contre la fraude et de localisation des terminaux mobiles;
- a créé le Secrétariat permanent de la gouvernance des communications électroniques pour assurer la veille technologique;
- a réalisé le projet international de la dorsale d'infrastructure en fibre optique reliant la capitale Bangui à la République du Congo et au Cameroun;
- a mis en place le projet national de digitalisation "Centrafrique digitale 2025";
- a mis en place un plan national stratégique pour le développement des infrastructures large bande à très haut débit;
- a créé une agence nationale des TIC et un data center national.

La République centrafricaine recommande que l'UIT fournisse une assistance et un appui afin d'aider les pays à renforcer les capacités en ce qui concerne les programmes de conformité

[26] Document SG2RGQ/144 (République centrafricaine) de la CE 2 de l'UIT-D.

et d'interopérabilité, et de la lutte contre la contrefaçon des produits et le vol d'équipements mobiles.

4.4.2 Mexique

Pour lutter contre le vol d'équipements terminaux mobiles, l'Institut fédéral des télécommunications (IFT), l'organisme national de réglementation dans le domaine des télécommunications et de la radiodiffusion du Mexique, a mis en place des obligations réglementaires. Plusieurs initiatives ont été lancées à l'échelle nationale et internationale pour contrôler les codes IMEI[27].

Au niveau international, le Gouvernement du Mexique, par l'intermédiaire de ses ministères et de ses départements, a signé des conventions bilatérales et régionales pour échanger des informations sur les codes IMEI des dispositifs volés ou perdus et interdire leur réutilisation. Un accord a été conclu avec la GSMA pour mettre en œuvre le système de vérification des codes IMEI des dispositifs, qui permet aux utilisateurs de dispositifs mobiles de consulter la base de données des codes IMEI de la GSMA en temps réel.

Au niveau national, l'IFT a publié au Journal officiel une disposition technique (IFT-011-2017) contenant des lignes directrices relatives à la collaboration en matière de sécurité et de justice, qui traitent de la suspension des services pour les dispositifs ou équipements terminaux mobiles déclarés volés ou perdus. L'IFT a renforcé cette collaboration en mettant en œuvre des dispositions techniques comportant des spécifications applicables aux terminaux mobiles reliés aux réseaux de télécommunication et à la vérification de la conformité et qui portent sur:

- l'évaluation de la conformité;
- l'actualisation du certificat de conformité;
- la création d'une base de données des codes IMEI des dispositifs homologués;
- le contrôle de la conformité aux prescriptions relatives à la certification.

L'IFT contrôle la conformité aux prescriptions figurant dans la disposition technique susmentionnée en suivant les méthodes de test décrites dans la disposition.

4.4.3 Université iranienne des sciences et des technologies

Afin de lutter contre la fraude et la vente et l'utilisation de dispositifs illicites, dont les téléphones volés et les téléphones pour lesquels les droits de douane n'ont pas été payés, la République islamique d'Iran a mis au point un plan d'enregistrement des téléphones mobiles en 2017[28].

Lorsqu'il est mis en marche pour accéder à un service, le dispositif fait l'objet d'une évaluation; si les informations demandées concernant ce dispositif sont introuvables parmi les informations relatives aux dispositifs licites, il sera identifié comme illicite et inscrit sur une liste noire.

Dans le système commercial global de la République islamique d'Iran, les téléphones importés sont enregistrés aux frontières douanières, où un code d'activation unique est attribué à chaque dispositif. L'université iranienne des sciences et des technologies a créé le système HAMTA,

[27] Document 2/166 (Mexique) de la CE 2 de l'UIT-D.
[28] Document 2/83 (République islamique d'Iran) de la CE 2 de l'UIT-D.

une base de données en ligne qui permet d'activer le dispositif grâce à un code unique et qui offre aux utilisateurs les deux principales fonctionnalités suivantes:

- L'affichage du statut des téléphones mobiles actuellement actifs dans le pays, qui permet de vérifier qu'un dispositif est authentique, licite et activé.
- L'activation des téléphones nouveaux et importés en toute légalité.

Les données sur les équipements enregistrés dans le système HAMTA sont communiquées à l'Autorité de régulation des télécommunications de la République islamique d'Iran et aux opérateurs mobiles. Seuls les dispositifs enregistrés authentifiés par le système HAMTA sont considérés comme licites et sont autorisés à accéder aux services fournis par les opérateurs, tous les autres étant inscrits sur liste noire.

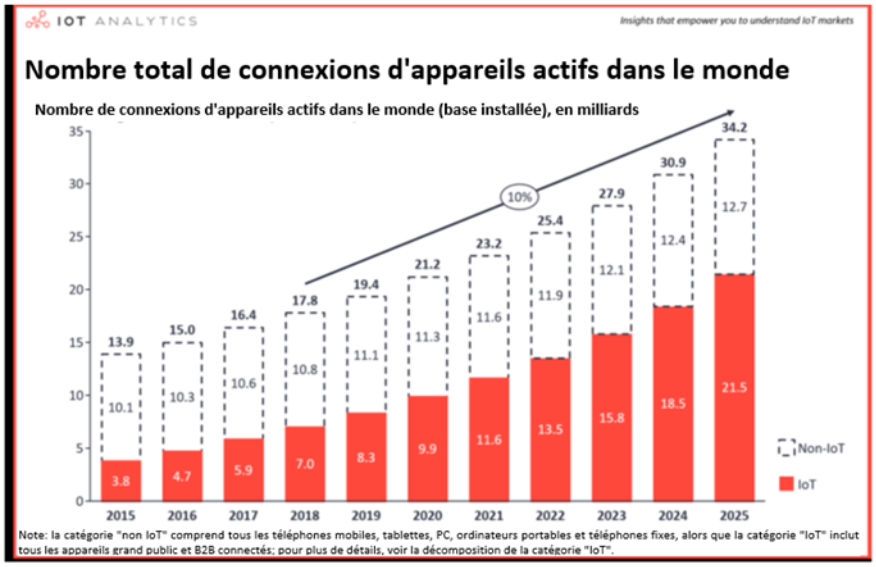
Chapitre 5 – Internet des objets et C&I

5.1 Introduction

Selon l'UIT, l'Internet des objets (IoT) est défini comme "une infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physique ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution"[29,30].

Les technologies de l'IoT sont présentes dans plusieurs secteurs d'activités et touchent à la vie quotidienne de l'individu via des plates-formes qui traitent les données provenant de milliards d'appareils connectés. Une étude réalisée par IoT Analytics montre que le nombre total de connexions d'appareils actifs dans le monde augmentera considérablement. En 2020, sur 21,2 milliards de connexions d'appareils actifs dans le monde, il existe 9,9 milliards de connexions IoT, ce dernier chiffre pouvant atteindre 21,5 milliards en 2025[31].

Figure 9 – Nombre d'appareils actifs connectés dans le monde



Source: IoT Analytics Research 2018.

5.2 Impact de l'IoT sur la C&I et l'état de préparation aux TIC

Des enjeux et défis sont engagés pour répondre aux exigences spécifiques de l'IoT telles que la qualité, la fiabilité, la couverture, une faible consommation, etc.

[29] Recommandation UIT-T Y.2060 (06/2012), Présentation générale de l'Internet des objets.
[30] Recommandation UIT-T Y.2069 (07/2012), Termes et définitions applicables à l'Internet des Objets.
[31] IoT Analytics, "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating", août 2018.

5.2.1 Les enjeux de l'IoT

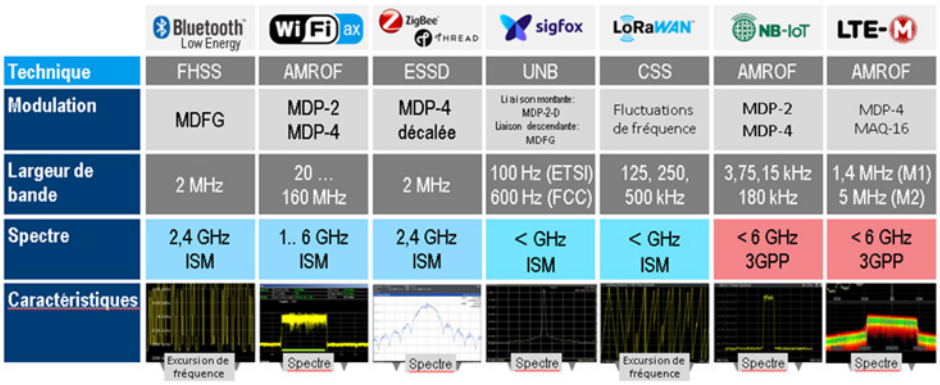
Il ne suffit pas d'avoir de bons capteurs qui récoltent les données; il faut également s'assurer de disposer d'une bonne connectivité pour les transmettre et d'une plate-forme qui les analyse et les traite.

Certains des nombreux défis de l'IoT revêtent un intérêt particulier, dont les suivants.

Le choix de la technologie, un facteur crucial de réussite pour l'IoT

Dans le futur, les applications IoT nécessitant une couverture et une mobilité totales se focaliseront sur les technologies cellulaires, telles que les technologies LTE-M et NB-IoT basées sur la 4G et sur la 5G. Les autres s'appuieront sur des technologies à faibles puissances fonctionnant dans les bandes sans licences, telles que Sigfox ou LoRaWAN. La majorité des applications utiliseront des technologies sans fil à courte ou moyenne portée, telles que les technologies Bluetooth®, WLAN/Wi-Fi et Zigbee. Les technologies sans fil pour l'IoT sont présentées dans la **Figure 10**[32].

Figure 10 – Technologies sans fil pour l'IoT



Une conception qui répond aux exigences de l'IoT telles que la qualité, la fiabilité, la couverture étendue, la latence, etc.

La conception doit aussi répondre aux attentes des utilisateurs, notamment en matière de confidentialité et de protection des données personnelles, et instaurer la confiance en utilisant les normes de sécurité dans l'écosystème de l'IoT.

La nécessité de la certification des dispositifs et plates-formes IoT

Les plates-formes et dispositifs doivent être certifiés en évaluant leur conformité aux réglementations et normes internationales.

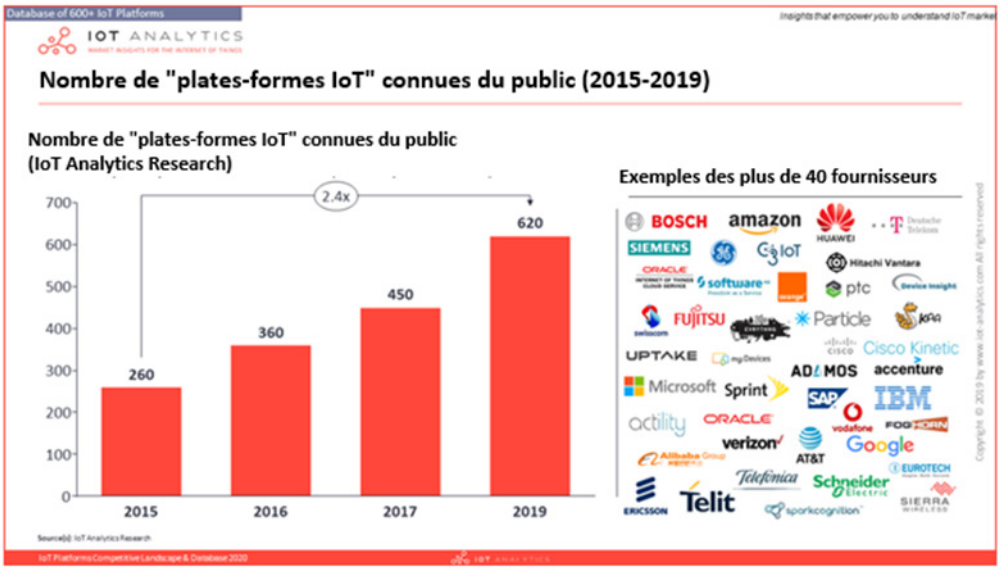
[32] Joerg Koepp (Rohde & Schwarz, Allemagne), "Ensuring reliable and secure communication in a hyper-connected world", *session sur le thème "Conformité et interopérabilité des TIC: défis pour les pays en développement" organisé à l'occasion de la réunion sur la Question 4/2 de l'UIT-D*. Genève, 16 octobre 2019.

5.2.2 Les contraintes de l'IoT

L'IoT se base essentiellement sur l'objet (le capteur), le réseau (la connectivité), les données et les applications d'exploitation. Les contraintes qui en découlent sont les suivantes:

– **Multiples plates-formes IoT:** des statistiques réalisées par IoT Analytics révèlent que l'on dénombrait **620** plates-formes IoT et plus de 40 fournisseurs en 2019 (voir **Figure 11**)[33].

Figure 11 – Nombre de plates-formes IoT connues du public

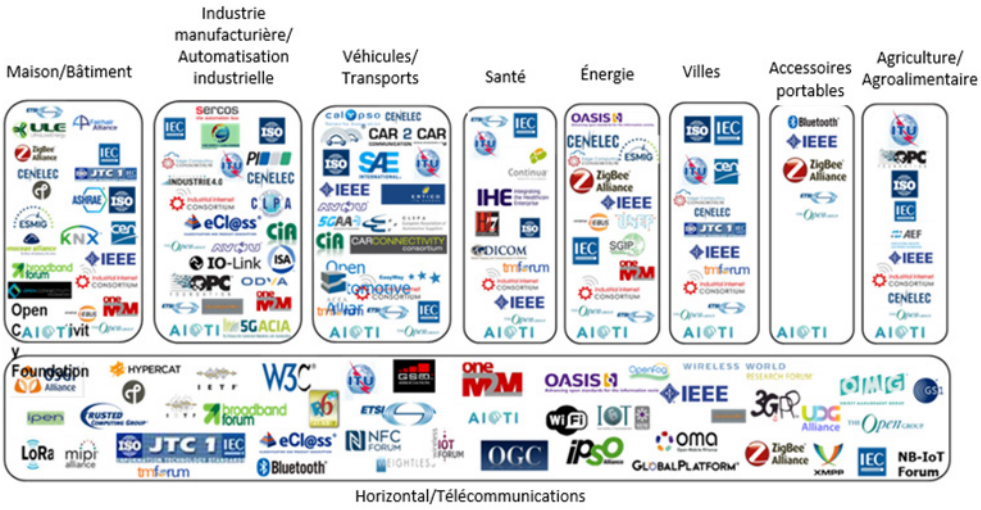


Source(s): IoT Analytics Research.

– **Multiples protocoles IoT**: les protocoles qui régissent les échanges de données sont multiples selon les organisations de normalisation et les fabricants des produits IoT. Chaque norme IoT dispose de son propre cadre normatif et les professionnels des technologies de l'information doivent choisir parmi une multitude de propositions (voir **Figure 12**)[34].

[33] IoT Analytics, "IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally", décembre 2019.
[34] Alliance pour l'innovation dans le domaine de l'internet des objets (AIOTI), "IoT LSP Standard Framework Concepts", Release 2.9, 2019.

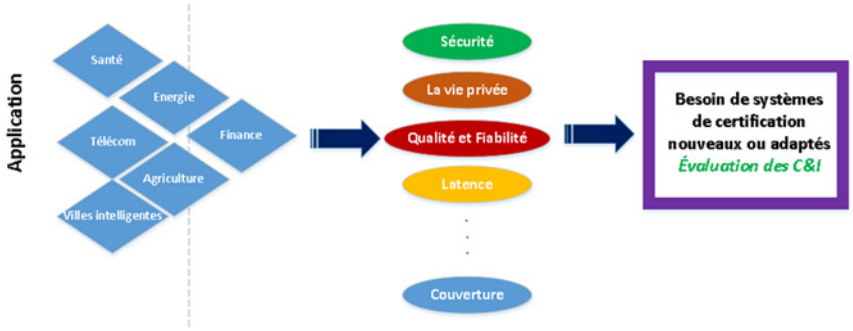
Figure 12 – Le paysage des organisations et des alliances chargées de l'élaboration des normes IoT (domaine horizontal et vertical)



Source: Groupe AIOTI WG3 (Normalisation de l'IoT) – Version 2.9.

Actuellement, avec une myriade de normes et de solutions incompatibles, l'IoT est loin d'être normalisé[35]. Au vu de la multiplication des plates-formes IoT et des protocoles qui assurent les communications des objets, les normes techniques de l'IoT ont évolué dans des situations diverses impliquant des applications et des parties prenantes différentes dont les objectifs et les exigences divergent. Le grand défi est donc de garantir l'interopérabilité, l'évolutivité, la vigueur des normes internationales et la sécurité de bout en bout (voir **Figure 13**).

Figure 13 – Besoin de schémas de certification adaptés

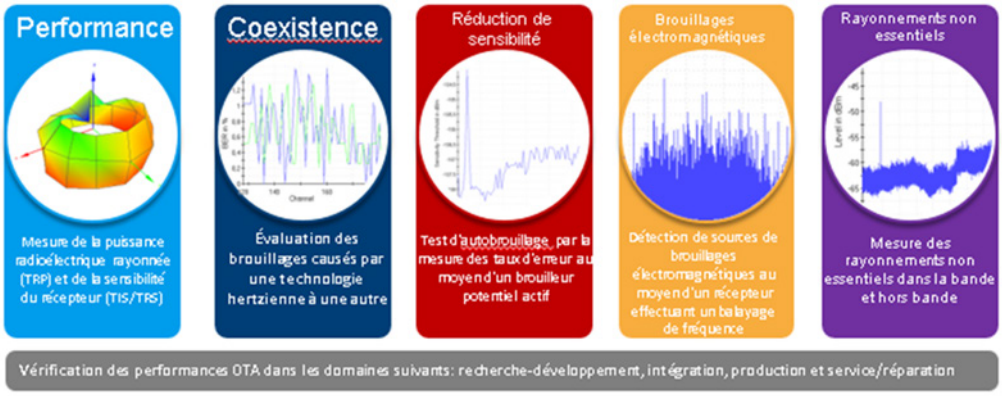


5.2.3 Exemple de test IoT de Rohde & Schwarz

Pour Rohde & Schwarz, les mesures OTA (Over The Air) contribuent à garantir les performances et le respect de la réglementation. Les tests se focalisent sur la performance, la coexistence, les tests de brouillage, les brouillages électromagnétiques et les mesures des rayonnements non essentiels dans la bande et hors bande (voir **Figure 14**)[36].

[35] UIT. Document UIT-T SG20-TD1722, *webinaire de l'UIT sur le thème "Accélérer la transformation des villes grâce aux normes"*, 25 juin 2020.
[36] Joerg Koepp (Rohde & Schwarz). Op. cit.

Figure 14 – Mesures OTA



5.2.4 Les organisations de normalisation

L'adoption d'une approche unifiée concernant les systèmes IoT dans le but de renforcer le développement de l'industrie a amené les organisations de normalisation à œuvrer en faveur de l'établissement d'une architecture type qui assure l'interopérabilité des systèmes, des applications, des appareils et des capteurs.

Union internationale des télécommunications

L'UIT-T a élaboré la série de Recommandations Y "Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes". La Commission d'études 20 (CE 20) de l'UIT-T travaille sur des normes internationales qui favorisent l'interopérabilité entre les infrastructures numériques et les applications IoT.

En mars 2020, l'UIT a publié la Recommandation UIT-T Y.4459[37], qui présente une architecture d'entité numérique. Celle-ci définit un ensemble minimum de composants architecturaux et de services nécessaires pour fournir une information générique et une interopérabilité de service. Elle facilitera l'interopérabilité de l'identification, la description, la représentation, l'accès, le stockage et la sécurité des appareils IoT. Ce cadre d'architecture encourage l'utilisation d'une interface de sécurité et de gestion commune à travers différentes applications IoT.

En ce qui concerne les tests C&I, la Commission d'études 11 (CE11) de l'UIT-T et la Commission de direction pour l'évaluation de la conformité collaborent avec la CE20 sur un modèle de réseau pour les tests de l'IoT[38].

Organisation internationale de normalisation et Commission électrotechnique internationale

En 2018, l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) ont publié la norme ISO/IEC 30141, une norme d'harmonisation établissant

---

37 Recommandation UIT-T Y.4459 (12/2020), "Digital entity architecture framework for Internet of things interoperability".

38 Kofi Ntim. Yeboah-Kordieh (Ghana), "ITU-T SG11 Work Updates And Activities", *atelier sur le thème "Conformité et interopérabilité des TIC: défis pour les pays en développement" organisé à l'occasion de la réunion sur la Question 4/2 de l'UIT-D*. Genève, 16 octobre 2019.

une architecture de référence pour l'IoT, décrit comme "l'assemblage complexe de milliards d'appareils intelligents connectés via l'Internet"[39].

En 2019, l'ISO et la CEI ont publié la norme ISO/IEC 21823-1[40], qui donne une vue d'ensemble de l'interopérabilité telle qu'elle s'applique aux systèmes IoT.

Institute of Electrical and Electronics Engineers

L'Institute of Electrical and Electronics Engineers (IEEE) a publié la norme 2413-2019 "IEEE Standard for an Architectural Framework for the Internet of Things (IoT)"[41]. La norme P2413.1 fournit un plan architectural pour la mise en œuvre de la ville intelligente en tirant parti de l'interaction inter-domaines et de l'interopérabilité entre divers domaines et composants d'une ville intelligente[42]. Cette norme s'appuie sur un cadre architectural pour l'IoT défini dans le projet de norme IEEE P2413, qui s'appuie sur la norme internationale ISO/IEC/IEEE 42010.

5.3 Réglementations et politiques relatives à l'IoT et aux TIC

Les régulateurs doivent être conscients des incidences de la C&I sur l'IoT. Même si les laboratoires de test contribuent à assurer la qualité de fonctionnement, la conformité et l'interopérabilité des produits, les réglementations sont également nécessaires.

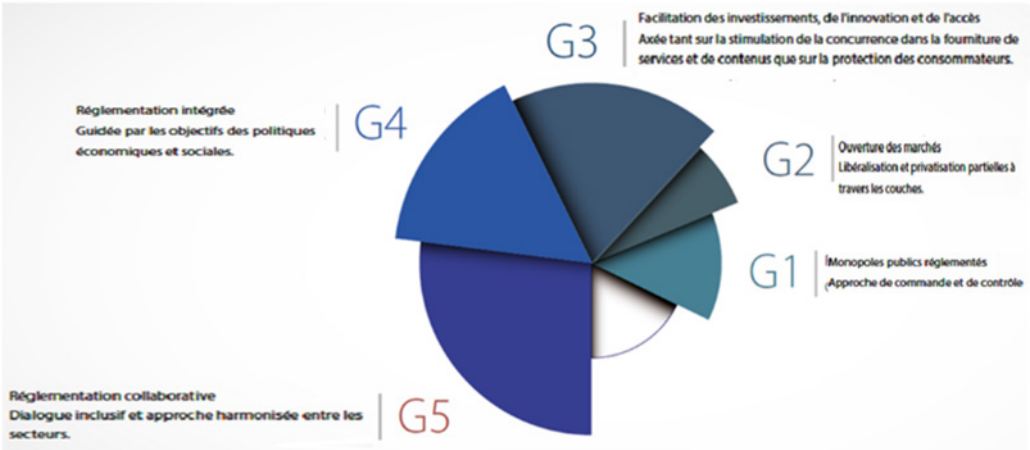
Aujourd'hui, les technologies IoT sont déployées dans plusieurs secteurs d'activité au niveau des entités privées et publiques: la santé, les télécommunications, l'éducation, l'agriculture, la finance, les médias et les villes intelligentes. Ainsi, la création d'un environnement réglementaire intersectoriel adapté à l'IoT est primordiale. Il s'agit de la réglementation de cinquième génération, à savoir la réglementation collaborative.

5.3.1 Aperçu de la réglementation collaborative

La réglementation a déjà beaucoup évolué de la première à la quatrième génération: 1) monopoles réglementés; 2) réformes de base et ouverture du marché; 3) réglementation d'un environnement propice à l'innovation; et 4) accès à la quatrième génération de réglementation intégrée qui traite les problèmes liés à l'Internet (voir **Figure 15**)[43].

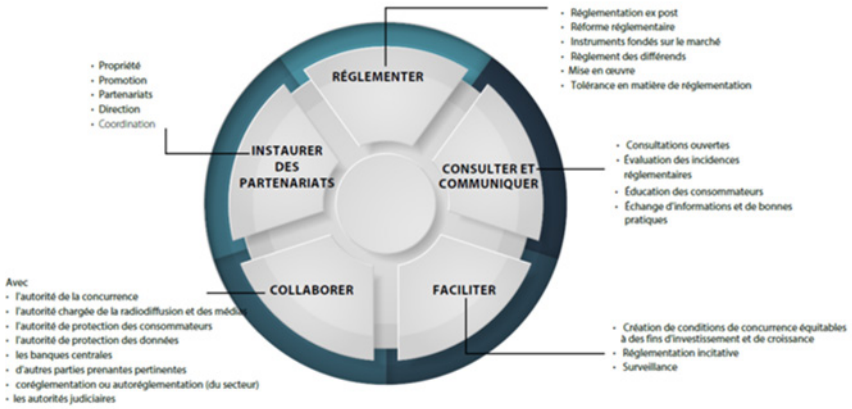
[39] ISO/IEC 30141:2018, "Architecture de référence de l'Internet des objets (IoT RA)", août 2018,
[40] ISO/IEC 21823-1:2019, "Internet des objets (IoT) – Interopérabilité des systèmes IoT – Partie 1: Cadre méthodologique", février 2019.
[41] IEEE 2413-2019, "Standard for an Architectural Framework for the Internet of Things (IoT)", mai 2019.
[42] IEEE P2413-1, "Standard for a Reference Architecture for Smart City (RASC)", août 2018.
[43] UIT-D. "Perspectives d'évolution de la réglementation des TIC dans le monde", 2017.

Figure 15 – Générations de réglementation des TIC – cadre conceptuel



La cinquième génération, dite réglementation collaborative, est souple et basée sur le consensus. La réglementation collaborative favorise l'innovation, l'efficacité, la qualité de service, le partage des données et la sécurité, et surmonte des obstacles tels que l'interopérabilité. De plus, elle se base sur le partage d'expertise, les principes directeurs, les meilleures pratiques et l'identification de mécanismes de coopération entre les secteurs afin de relever plus efficacement les défis communs (voir **Figure 16**)[44].

Figure 16 – La réglementation collaborative



Les lignes directrices relatives aux bonnes pratiques de 2019 du Colloque mondial des régulateurs (GSR) de l'UIT ont été axées sur la réglementation collaborative pour garantir la réussite de la transformation digitale[45].

---

44 Ibid.

45 UIT. Colloque mondial des régulateurs (GSR), "Lignes directrices relatives aux bonnes pratiques de 2019", Port-Vila, 2019.

5.3.2 Réglementation de l'IoT

De nombreux gouvernements encouragent l'innovation dans le domaine de l'IoT et veulent réformer leur cadre réglementaire pour ne pas entraver son évolution. Cependant, comme il existe toujours une incertitude réglementaire concernant le marché de l'IoT, les innovations et les ajustements réglementaires se feront d'une manière progressive.

L'IoT diffère de la connectivité que les régulateurs des TIC s'efforcent de permettre. La connectivité est le service principal, tandis que l'IoT englobe aussi les applications, les appareils et capteurs associés.

En général, même si toutes les réglementations s'appliquent à l'IoT, cette technologie peut donner lieu à des exigences supplémentaires. Les politiques et les réglementations doivent aborder les problèmes liés à l'IoT tels que:

- la confidentialité, la protection des données et la sécurité;
- les normes et l'interopérabilité des systèmes, les plates-formes et les objets connectés;
- la gestion du spectre et l'octroi de licences (dans de nombreux cas, les appareils IoT utilisent des technologies sans fil);
- la numérotation et la portabilité de numéro;
- la nécessité de la transition de l'IPv4 vers l'IPv6;
- les coûts, la fiabilité, la qualité de service et la qualité de l'expérience;
- les mesures relatives à la gestion de la concurrence.

Les réglementations sur les TIC deviennent de plus en plus complexes en raison de problèmes liés à la sécurité, à la confidentialité et à la protection des données. De nombreux pays peuvent avoir besoin de mettre à jour leurs réglementations obsolètes ou trop restrictives, et les problèmes d'interopérabilité nuisent aux efforts déployés à plus grande échelle.

Afin d'améliorer l'interopérabilité et de réduire les coûts, les professionnels plaident en faveur d'un écosystème IoT ouvert reposant sur des plates-formes, applications et normes open source non-propriétaires qui favorise ainsi la croissance économique et l'innovation.

5.4 Conclusion

La normalisation est indispensable pour créer un marché unique pour l'IoT dans lequel tous les appareils peuvent communiquer entre eux quel que soit l'endroit où ils sont connectés. La normalisation améliore l'interopérabilité, la compatibilité, la fiabilité et la sécurité, favorise l'émergence de nouveaux écosystèmes et l'innovation, et renforce la compétitivité.

Les régulateurs doivent être conscients de l'impact des nouvelles technologies IoT et de l'importance de leur rôle dans le développement de ces technologies, et créer de nouvelles opportunités en instaurant la nouvelle ère de la réglementation collaborative dans laquelle ils agissent davantage en tant que facilitateurs, travaillent à l'amélioration de la connectivité et collaborent avec d'autres acteurs pour promouvoir l'utilisation des TIC dans tous les domaines.

En conclusion, une stratégie qui repose sur un cadre réglementaire progressif peut protéger et élever toutes les parties prenantes en déployant des compétences, des financements et d'autres ressources. De plus, elle peut promouvoir cette nouvelle technologie et favoriser un marché concurrentiel et une innovation rapide.

Chapitre 6 – Transmission des informations, du savoir-faire et des connaissances

6.1 Besoins de formation et opportunités pédagogiques en matière de C&I

La C&I nécessite un ensemble de compétences spécialisées, et les programmes C&I doivent être menés par des professionnels formés. De plus, certains défis sont inhérents à ce domaine, notamment les suivants:

- L'absence de programmes pédagogiques complets et formels sur la C&I. De grandes institutions forment les membres du personnel à la C&I en les associant à des travailleurs expérimentés. Bien que cette approche puisse être utile, elle n'offre généralement qu'une faible expérience et aucun contrôle formel de la qualité n'est effectué. De plus, les institutions plus petites ne peuvent pas adopter cette approche.
- Les professionnels confrontés aux questions de conformité et d'interopérabilité, à savoir les régulateurs, les titulaires de licences, les demandeurs de certificats (importateurs et fabricants) et les responsables de la conformité doivent comprendre clairement les enjeux liés au droit, à la technologie, au commerce international et à l'économie.
- Les produits technologiques en évolution rapide constituent un défi permanent pour les cadres C&I (par exemple dans le domaine de l'IoT et de la configuration des logiciels).

Dans sa Résolution 177 (Rév. Dubaï, 2018), la Conférence de plénipotentiaires de l'UIT a souligné la nécessité de continuer d'organiser des activités de renforcement des capacités en cours d'emploi dans le domaine de la C&I, en collaboration avec des institutions reconnues et en s'appuyant sur l'écosystème de l'Académie de l'UIT, y compris les activités relatives à la prévention des brouillages radioélectriques causés ou subis par les équipements TIC[46].

Les expériences vécues en 2020 ont démontré qu'il était urgent de développer l'apprentissage numérique à l'échelle mondiale au moyen de réseaux TIC fiables. À la suite de la pandémie de COVID-19, l'utilisation des TIC à des fins éducatives revêt plus que jamais un intérêt public. Tel que proposé dans la Résolution 177 (Rév. Dubaï, 2018), l'Académie de l'UIT offre des solutions de formation en ligne à l'intention des formateurs que la communauté mondiale des professionnels de la C&I devrait examiner.

[46] UIT. Résolution 177 (Rév. Dubaï, 2018) de la Conférence de plénipotentiaires sur la conformité et l'interopérabilité.

6.2 Répondre aux besoins liés à l'acquisition et à la rétention des connaissances

Il convient d'envisager d'utiliser une plate-forme collaborative reposant sur des mécanismes d'assurance qualité pour favoriser le développement d'un ensemble plus vaste de compétences, en s'appuyant sur l'exemple de la proposition de l'UIT en faveur de la création d'un programme de formation dans le domaine de la conformité et de l'interopérabilité (CITP)[47].

Le CITP s'inspire des activités de formation en matière de C&I organisées antérieurement avec succès en collaboration avec les laboratoires partenaires, telles que les activités de formation régionales en cours d'emploi sur les programmes et les domaines de tests C&I[48]. Le programme tient compte également des enseignements tirés des publications de l'UIT, notamment du rapport sur la Question 4/2 pour la période d'études 2014-2017[49], et des lignes directrices publiées[50].

Les travaux visant à mettre au point le CITP s'appuient sur le modèle créé par le mécanisme d'assurance qualité de l'Académie de l'UIT, qui comporte un ensemble de matériels de haut niveau élaborés par des experts du domaine, un processus d'évaluation par les pairs, ainsi que des modèles de rédaction des descriptifs et des grandes lignes de programmes de formation conçus par des formateurs professionnels.

Une proposition de structure de formation offrant des parcours de formation adaptés est présentée ci-dessous:

---

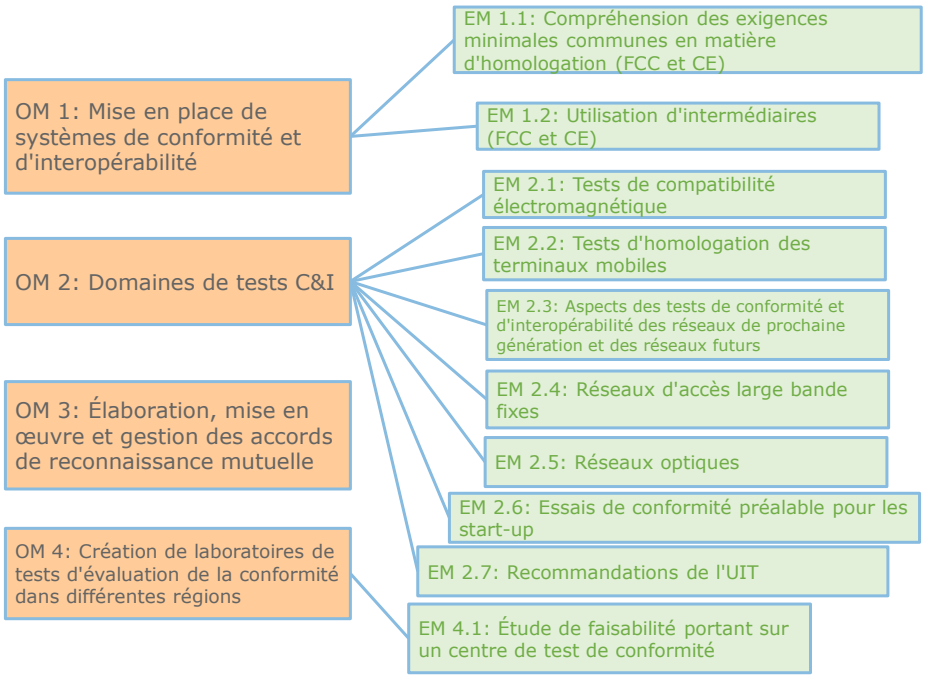
47 Ces concepts ont été présentés en octobre 2019 au titre de la Question 4/2 dans le Document SG2RGQ/194 + Annexe (Coordonnateur du BDT pour la Question 4/2) de la CE 2 de l'UIT-D.

48 UIT-D. Manifestations sur la conformité et l'interopérabilité.

49 UIT-D. Rapport final de la Commission d'études 2 de l'UIT-D sur la Question 4/2 pour la période d'études 2014-2017. Op. Cit.

50 UIT-D. Publications et rapports – Conformité et interopérabilité.

Figure 17 – Modules de formation du CITP (OM: modules obligatoires; EM: modules au choix)



La structure de la formation s'articule autour de quatre thèmes principaux et se divise en sous-thèmes pour permettre aux apprenants de choisir leur parcours de formation et s'assurer de leur transmettre les connaissances qu'ils souhaitent acquérir.

1) **Définition et mise en place de systèmes/cadres pour la conformité et l'interopérabilité**

   Ce module est axé sur la compréhension des exigences techniques minimales et l'utilisation des structures C&I existantes et d'intermédiaires afin de trouver le bon équilibre entre la confiance à l'égard des dispositifs TIC et le contrôle de ceux-ci.

2) **Domaines de tests couvrant un vaste ensemble de services de laboratoire**

   Le champ d'application des domaines de tests est potentiellement infini et peut couvrir des questions telles que l'adoption des nouvelles technologies et le soutien apporté aux jeunes développeurs pour que leurs produits bénéficient d'une reconnaissance internationale.

   Il est évident qu'il convient de mettre en place des modules de formation pour répondre aux besoins et priorités existants.

3) **Collaboration régionale et harmonisation dans le domaine des normes et des processus d'homologation, notamment dans le cadre d'accords de reconnaissance mutuelle**

   Comme indiqué dans le chapitre précédent, la collaboration est essentielle, et ce module met en avant le partage de ressources et les mécanismes déjà mis en place pour certifier la conformité des produits TIC aux prescriptions techniques nationales et internationales.

4) **Création et gestion des laboratoires de tests**

   Ce module se concentre sur les procédures qualité et les évaluations stratégiques, comme l'optimisation de la planification organisationnelle.

6.3 Conclusions

En résumé, il est nécessaire d'effectuer une analyse approfondie en tenant compte des indications suivantes pour élaborer un programme de formation portant sur la transmission d'informations, d'un savoir-faire et de connaissances:

- Collaborer avec des experts du domaine, notamment les Commissions d'études de l'UIT (Question 4/2 de l'UIT-D, CE 11 de l'UIT-T et contributeurs du Bureau des radiocommunications), les professionnels impliqués dans la réalisation de tests, les responsables de l'homologation et les experts commerciaux.
- Utiliser des matériels de formation basés sur les publications de l'UIT relatives au programme C&I, notamment les lignes directrices et les recommandations de l'UIT élaborées par l'UIT-R et l'UIT-T.
- S'appuyer sur les travaux des organisations internationales, régionales et nationales portant sur la transmission des connaissances.
- Faciliter l'accès à la formation dans le domaine de la conformité et de l'interopérabilité et garantir une approche avant-gardiste et professionnelle.
- Concevoir le cours de façon à ce qu'il soit accessible à tous, aussi bien aux débutants qu'aux spécialistes.
- Proposer une approche adaptable par modules qui permet d'apporter le niveau de connaissances correspondant à la tâche à accomplir et qui garantit que le contenu répond aux besoins du moment en matière de conformité et d'interopérabilité.

Annexes

Annex 1: Conformance and interoperability frameworks: country data

Understanding how countries organize themselves for guaranteeing proper conformance an interoperability levels for ICT networks and devices deployment can help C&I operators to establish efficient mechanisms for collaboration. This can be verified in effective technical collaboration agreements in some regions (e.g. Europe, APEC-MRA).

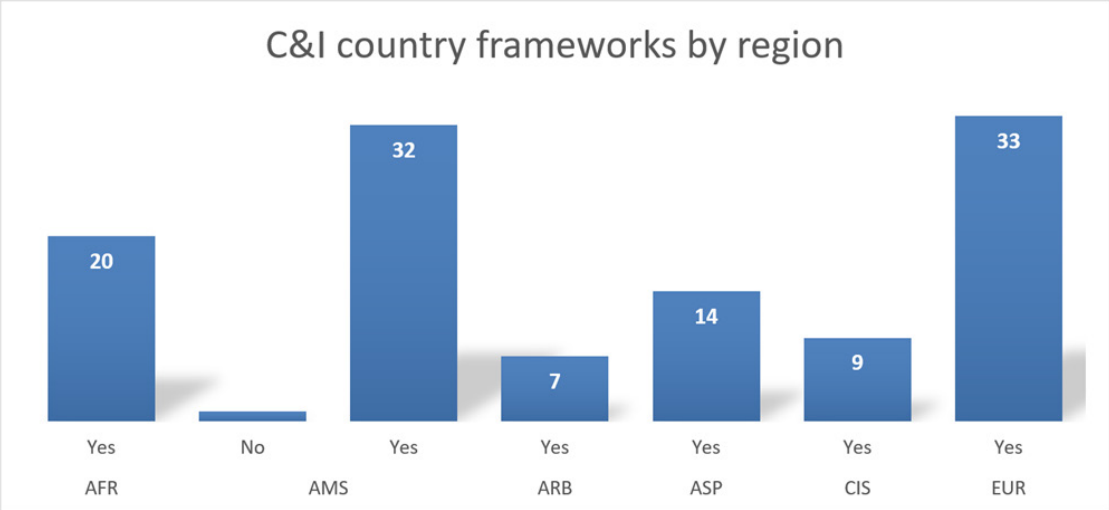
Data shows that most of the countries have in place a Conformance and Interoperability arrangement aiming to ascertain trust on a safe and interoperable use of ICT devices by networks and citizens. Noting that procedures and strictness levels of requirements (e.g., recognition of certification and use of proxies, self-declaration, local testing, etc.) can differ significantly.

Various events undertaken under the ITU C&I Programme Pillars 3 (capacity building) and 4 (assistance to developing countries)[51] allowed to gather related information from 116 countries[52].

Data research and organization of essential information considered different C&I infrastructure variables, such as:

1. Conformance and Interoperability Frameworks
2. ICT Standards and Technical Requirements
3. Conformance Assessment and Bodies
4. Testing Laboratories
5. Quality and metrology

Figure 1A: Legal C&I Frameworks from 114 countries that provided information



[51] The source material used for the data research is currently available on the ITU website, from: C&I events; Assessment studies; ITU-D Study Group Question 4/2 inputs as national and regional case studies.

[52] Reference contribution to Q4/2: SG2RGQ/274

The figure above displays the number of C&I country framework per region from 116 countries: 115 countries informed the existence of legal document and a level of procedure for accepting ICT products in their markets (importation fees and taxes not included); only one country in the Americas informed about the absence of any legal procedures for ICT products.

The complete dataset display is a work in progress and complete analysis will be provided through the ITU-C&I development portal (https://itu.int/go/ci_development)

Annex 2: Counterfeiting – a survey of national frameworks and practices

Data from the annual ITU World Telecommunication/ICT Regulatory Survey (edition 2019) on regulatory practices related to the distribution and use of counterfeit ICTs.

The data series featured are as follows:

1) Responsibilities of telecom/ICT regulators related to ICT counterfeiting,
2) Types of counterfeit ICTs overseen by the telecom/ICT regulator,
3) Policy/legislation/regulation related to ICT counterfeiting adopted,
4) Areas covered in ICT counterfeiting regulations,
5) Plans to adopt a regulatory framework for ICT counterfeiting.[53]

Table 1A: Summary of ITU World Telecommunication/ICT Regulatory Survey (edition 2019) survey on regulatory practices related to the distribution and use of counterfeit ICTs

Summary								
Question	Answer	Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas	Total
Does the Telecom/ICT regulator (or the entity in charge of regulation in the sector) have responsibilities related to ICT counterfeiting (e.g., fake mobile phones, smartphones, computers, any network or other computing equipment components)?	Yes	23	12	10	0	9	11	**65**
	No	10	3	10	2	28	14	**67**
Has your country adopted any policy/legislation/regulation related to ICT counterfeiting?	Yes	23	11	7	2	14	14	**71**
	No	10	5	15	3	20	12	**65**
If no, are there plans to adopt a regulatory framework for ICT counterfeiting?	Yes	3	3	4	0	3	3	**16**
	No	4	0	8	4	11	5	**32**
Region size		**44**	**22**	**40**	**9**	**46**	**35**	**196**
* This question allows multiple answers per country/economy								
Year: 2019 or latest available data.								
Source: ITU World Telecommunication/ICT Regulatory Database								
ITU ICT-Eye: http://www.itu.int/icteye								

[53] Reference contribution to Q4/2: SG2RGQ/38 + Annex

Figure 2A: Regional distribution of responses from survey – Question 1

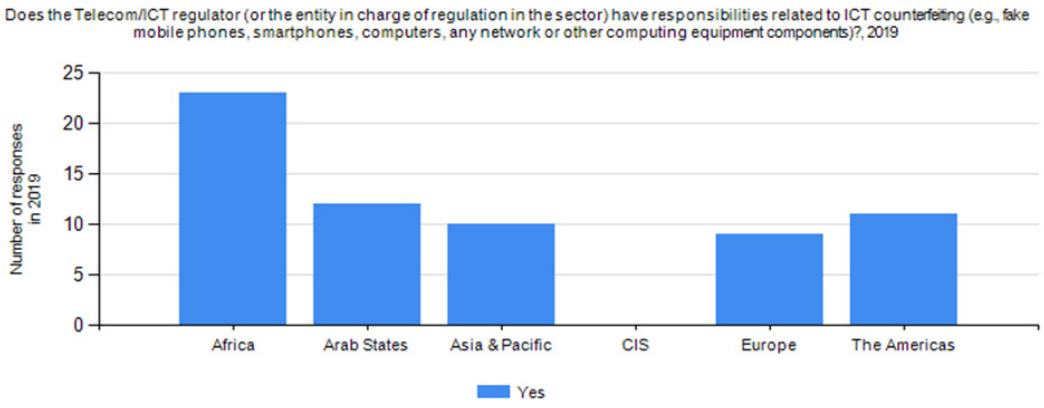


Figure 3A: Regional distribution of responses from survey – Question 2

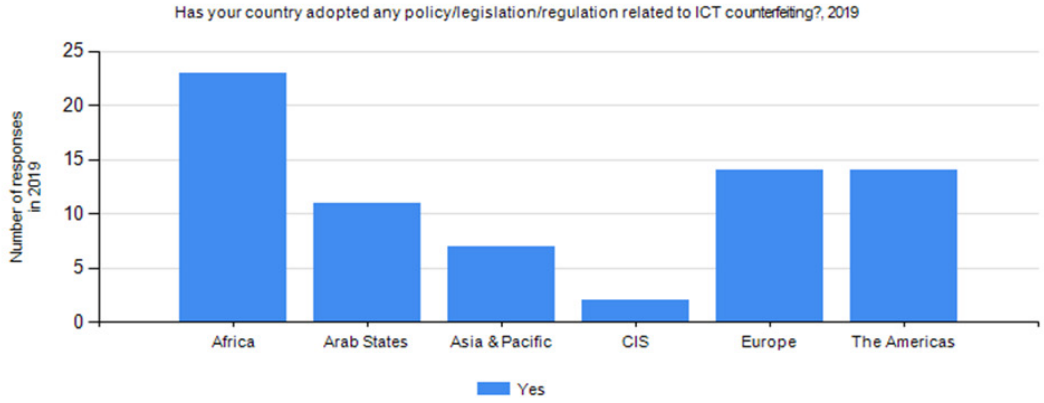
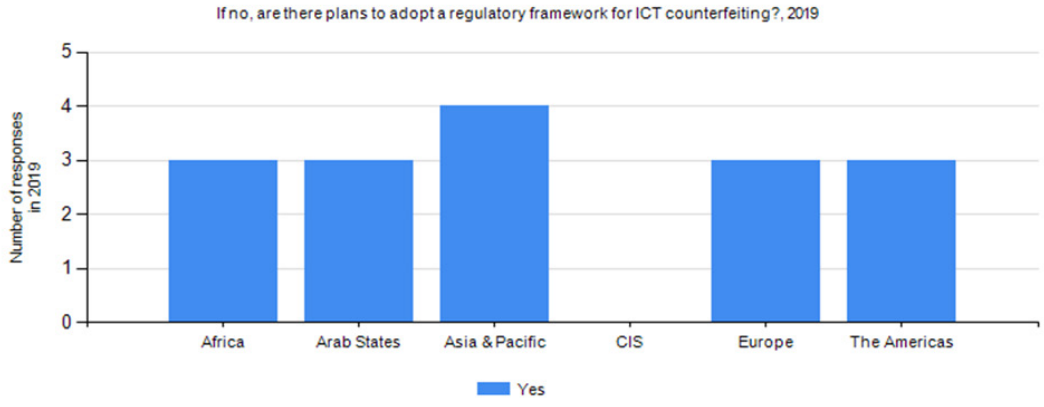


Figure 4A: Regional distribution of responses from survey – Question 3



Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi[54]

A3.1 Introduction

Counterfeiting of mobile phones has numerous negative effects on industry, society, governments and in particular consumers of ICT services. Primarily, it leads to a lower quality of service of mobile telecommunications and safety hazards associated with the use of defective second-hand terminals due to inferior quality or unsuitable technical characteristics.

A3.2 Impact of the proliferation and use of counterfeit mobile terminals

The use of counterfeit mobile terminals by consumers and rising dissatisfaction among mobile subscribers faced with the growing phenomenon of mobile terminal theft has undesirable consequences in the short and long term, including:

- Lowering the QoS of mobile telecommunication services, which in turn has an impact on the experience of consumers and businesses
- Compromising the security of digital transactions and that of mobile terminal users
- Increasing evasion from applicable taxes and duties, which has a negative effect on tax revenues
- Creating risks to the environment and consumer health due to the use of hazardous substances recovered from waste electrical and electronic equipment (WEEE)
- Facilitating the drugs trade, terrorism and other local, regional and international criminal activity
- Infringing on manufacturers' trademarks
- Significantly affecting the ICT market by proposing poor-quality, low-cost products that tend to have a greatly reduced lifetime, whence the accumulation of WEEE.

A3.3 National initiatives in the fight against mobile terminal theft and equipment counterfeiting

To combat the use of counterfeit terminals more effectively, the *Agence de régulation et de contrôle des télécommunications* (ARCT) (Telecommunication Regulatory and Control Agency of Burundi) has instituted the following measures:

1. Creation of certification procedures for telecommunication equipment
2. Registration of the characteristics of telecommunication equipment
3. Issuance of import certificates for vendors of telecommunication equipment
4. Enforcement of the requirement that telecommunication equipment vendors be licensed and display their vendor's licence on the establishment's walls, that terminals be certified by ARCT, and that equipment be guaranteed for at least six months
5. Regular inspections to verify compliance and respect of technical standards and regulations
6. Creation of a toll-free number (151) for members of the public to report telephone sales where there is a problem with the IMEI number of the phone and that on the package
7. Organization of public awareness campaigns on the dangers of using counterfeit mobile terminals

[54] ITU-D SG2 Document 2/390 from Burundi [in French]

8. Inspection of electronic communication terminal equipment in use by public and private organizations
9. Inspection of providers of value-added services who use numbering resources.

To combat the use of stolen mobile terminals more effectively, ARCT has initiated the following activities:

1. Registration of all mobile telecommunication service subscribers: ARCT regularly assesses compliance with the circular on the registration of subscribers by the telecommunication operators, in order to combat fraud.
2. Automation of the service for requisitioning expert testimony: A management application for processing and managing requisitions for expert testimony in cases of mobile communication terminal theft has been designed and implemented.
3. Combating theft and crimes committed using mobile telephones: ARCT invites members of the public to report the numbers used to send suspicious messages and to forward them to ARCT for systematic verification and deactivation if necessary.

A3.4 Conclusion

It is crucial to put into action all effective means for combating counterfeit terminals being sold or connected to the telecommunication network, so as to protect the consumers of ICT services. This will also enhance security for users, improve the quality of service of networks and stimulate digital economy and financial growth of the country.

Annex 4: Illustrations for chapters of the Output Report on Question 4/2

The following illustrations summarize concepts for Chapters 2, 3 and 5 of the Output Report.

Definitive, high-level resolution images of the illustrations are available at https://itu.int/go/CI_development.

Figure 5A: Illustration for Chapter 2 – What is conformance and interoperability (C&I)

Figure 6A: Illustration for Chapter 2 – C&I frameworks

Figure 7A: Illustration for Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices

Figure 8A: Illustration for Chapter 5 – The Internet of Things and C&I

Annex 5: Ideas for the future of the Question

Having regard to the role of C&I in a hyperconnected world where billions of people and objects connect with each other, the study group's work on C&I could focus on:

- **Efforts to manage the increasing number of devices sharing the same limited resources**
- **Measures to cover costs related to conformity procedures and controls of ICT products to allow only approved products to access markets**
- **Harmonization of procedures and collaboration**
    - Robust C&I frameworks: Making sure every country has or is part of a robust C&I framework at minimal cost (e.g. agreements on the shared use of national C&I infrastructure, such as testing facilities and certificates of conformity).
    - Collaboration: Are MRAs effective tools to pursue in the future? What aspects of MRAs need to be adapted to improve existing collaboration agreements or develop new ones? The group could focus on innovative collaboration structures to improve access to high-quality and safe ICT products.
- **Trends**
    - Future challenges for C&I, such as:
        - New technologies outpacing regulation/testing procedures
        - Regulatory aspects for open RAN and interoperability adoption related to 5G
        - Smart objects able to communicate through ICTs
        - Software tampering/hacking vulnerabilities
        - Effective harmonization of procedures and technical collaboration, etc.
    - Means of prioritizing device/type-approval models to achieve a good balance between trust and control.
    - C&I challenges and opportunities during the COVID-19 pandemic.
    - Ways in which new technologies (such as blockchain and artificial intelligence) can help to improve trust in the international C&I framework and trade in and use of ICT devices.

Annex 6: List of contributions and liaison statements received on Question 4/2

Contributions on Question 4/2

Web	Received	Source	Title
2/423	2021-03-18	Rapporteur for Question 4/2	Proposed liaison statement from ITU-D Study Group 2 Question 4/2 to ITU-T Study Group 11, ITU-R WP1A and WP6A, and ISO/CASCO
2/390	2021-02-03	Burundi	Initiatives de lutte contre les équipements de contrefaçon et le vol des terminaux mobiles au Burundi
RGQ2/277	2020-09-22	Algérie Télécom SPA (Algeria)	Revisions to Draft Chapter 3 for the Final Report of Question 4/2
RGQ2/274 +Ann.1	2020-09-22	BDT Focal Point for Question 4/2	C&I Database - updated summary
RGQ2/269	2020-09-22	Rapporteur for Question 4/2	Draft text for new chapter (Ideas for the Future of the Question) of the Output Report for Question 4/2
RGQ2/265	2020-09-22	Rapporteur for Question 4/2	Draft text for Chapter 1 Section 1.4 on COVID-19 impact to type approval procedures
RGQ2/264	2020-09-22	Kenya	Proposed draft text for Chapter 4 of the Output Report for Question 4/2
RGQ2/233	2020-08-20	Algérie Télécom SPA (Algeria)	Proposed text for Chapter 5: Internet of Things and C&I
2/345	2020-02-11	BDT Focal Point for Question 4/2	ITU Conformance and Interoperability Training Programme
2/337	2020-02-11	Algérie Télécom SPA (Algeria)	Revisions to draft Chapter 3 for the Final Report of Q4/2
2/332 +Ann.1	2020-02-11	Kenya	Device Management System - Kenyan Case
2/326	2020-02-10	Oman	Problem of increasing use of fake IMEI
2/323 (Rev.1)	2020-02-07	Ghana	Achieving quality C&I regimes - Challenges from basic Infrastructure to legislative and regulatory frameworks. The experience of Ghana
2/311	2020-01-28	International Telecommunication Academy (Russian Federation)	Regulation on the system to confirm the compliance of communication facilities and services with the ITU standard
2/290	2020-01-08	Mauritania	Mauritania (Islamic Republic of)
2/261	2019-12-24	Guinea	Conformance and interoperability (C&I)
2/257	2019-12-20	Mauritania	Proposed draft text for Chapter 2 of the Final Report for Question 4/2
2/250	2019-12-08	Comoros	Progress of activities for implementing conformance and interoperability programmes in the Union of the Comoros

(suite)

Web	Received	Source	Title
RGQ2/194 +Ann.1	2019-09-24	BDT Focal Point for Question 4/2	ITU Conformity and Interoperability Training Programme (CITP)
RGQ2/171	2019-09-18	Algérie Télécom SPA (Algeria)	Implementation of Plenipotentiary Conference (PP-18) Resolution 177 (Rev. Dubai, 2018)
RGQ2/170	2019-09-15	Mauritania)	Conformité et interopérabilité des équipements TIC dans les pays en développement : normes et procédures - cas de la Mauritanie
RGQ2/144	2019-08-20	Central African Republic	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment and theft of mobile devices
RGQ2/139	2019-08-06	Guinea	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment
2/TD/24	2019-03-29	Rapporteur for Question 4/2	Proposed outgoing liaison statements from Q4/2
2/TD/22 +Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/210	2019-03-12	BDT Focal Point for Question 4/2	C&I Programme - Pillars 3 & 4 implementation report
2/202 +Ann.1	2019-03-08	BDT Focal Point for Question 4/2	Summary on national C&I topics
2/177	2019-02-07	Rapporteur for Question 4/2	Draft Chapter 3 for Final Report on Question 4/2
2/166	2019-02-06	Mexico	Regulatory obligations to help combat the theft of mobile devices
2/149	2019-01-24	Guinea	Assistance to developing countries for implementing conformance and interoperability programmes, portability and combating counterfeit ICT equipment and theft of mobile devices
2/142	2019-01-16	Madagascar	Implementing conformance and interoperability programmes
2/133	2019-01-10	Comoros	Realization of a programme for assistance to developing countries for implementing conformance and interoperability programmes: case of Union of the Comoros
RGQ2/TD/8	2018-09-25	South Sudan	Challenges and proposals to deal with counterfeit ICT equipment and mobile device theft in South Sudan and region
RGQ2/TD/7	2018-10-01	Russian Federation	ITU-D SG1 and SG2 coordination: Mapping of ITU-D Study Group 1 and 2 Questions
RGQ2/86 +Ann.1	2018-09-18	BDT Focal Point for Question 4/2	ITU C&I programme: implementation update

(suite)

Web	Received	Source	Title
RGQ2/85	2018-09-18	Zimbabwe	Actions to combat counterfeit and theft of mobile devices in Zimbabwe
RGQ2/82	2018-09-18	Ghana	Ghana's Type Approval Regime - a sustainable approach to connecting and protecting users of telecommunications/ICTs and networks through conformance assessment
RGQ2/80	2018-09-18	GSM Association	GSMA's IMEI database and services
RGQ2/69	2018-09-17	Rwanda	Regional effort to fight illegal devices, improve the quality of services and minimize health hazard to consumers
RGQ2/66 (Rev.1)	2018-09-16	Senegal	Lutte contre la contrefaçon et le vol de téléphone
RGQ2/38 +Ann.1	2018-08-18	BDT Focal Point for Question 3/1	ITU data on regulatory practices related to counterfeit ICTs
RGQ2/9 (Rev.1)	2018-07-05	Guinea	Implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices
2/TD/10	2018-05-10	Rapporteur for Question 4/2	Draft reply liaison statements from ITU-D Study Group 2 Question 4/2
2/TD/8	2018-05-09	Rapporteur for Question 4/2	Draft work plan, Table of Contents (ToC) and responsibilities for ITU-D Question 4/2
2/97 (Rev.1)	2018-05-06	Chairman, ITU-D Study Group 2	List of proposed Rapporteurs and Vice-Rapporteurs of ITU-D Study Group 2 study Questions for the 2018-2021 period
2/92 +Ann.1	2018-04-24	BDT Focal Point for Question 4/2	ITU C&I Programme status - Pillars 3 and 4
2/90	2018-04-24	Mauritania	Draft work plan for ITU-D Study Group 2 Question 4/2
2/88 +Ann.1	2018-04-23	BDT	Implementation of ITU C&I Programme and ITU-T activities on combatting counterfeiting and stolen ICT devices
2/83	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	HAMTA: A system for combating counterfeit ICT equipment and theft of mobile devices
2/58	2018-03-22	Algérie Télécom SPA (Algeria)	Conformance and interoperability
2/45	2018-03-12	Madagascar	Monitoring counterfeit terminal devices, building a healthy network that brings in revenues for the State

Incoming liaison statements for Question 4/2

Web	Received	Source	Title
RGQ2/219	2020-08-06	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/205 +Ann.1-2	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/204 +Ann.1	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on contribution on conformance and interoperability
RGQ2/115 +Ann.1	2019-06-14	ITU-T Study Group 5	Liaison statement from ITU-T SG5 to ITU-D SG2 Q4/2 and Q7/2 on work being carried out under study in ITU-T Study Group 5 Question 3/5
RGQ2/113	2019-05-29	ITU-T Study Group 20	Liaison statement from ITU-T SG20 to ITU-D SG2 Q4/2 on SG20 activities on IoT and Smart Cities & Communities
RGQ2/111 +Ann.1-3	2019-04-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/22 +Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/TD/19 +Ann.1-3	2019-03-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/17 +Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates to the Technical Report on the Combat of Counterfeit Devices
2/TD/16 +Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on creation of new work item on "Reliability of IMEI identifier"
2/TD/15	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on impact of counterfeit mobile devices on Quality of Service
2/139	2019-01-16	ITU-T Study Group 20	Liaison statement from ITU-T SG20 on SG20 activities on IoT and Smart City & Community
RGQ2/16 +Ann.1-3	2018-08-02	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on progress and collaboration on the combat of counterfeit and mobile device theft
2/35	2017-12-01	ITU-T Study Group 11	Liaison Statement from ITU-T SG11 to ITU-D SG2 Question 4/2 on ongoing collaboration

Union internationale des télécommunications (UIT)
Bureau de développement des télécommunications (BDT)
Bureau du Directeur
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdirector@itu.int
Tél.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Adjoint au directeur et Chef du Département de l'administration et de la coordination des opérations (DDR)
Place des Nations
CH-1211 Genève 20
Suisse

Courriel: bdtdeputydir@itu.int
Tél.: +41 22 730 5131
Fax: +41 22 730 5484

Département des réseaux et de la société numériques (DNS)
Courriel:: bdt-dns@itu.int
Tél.: +41 22 730 5421
Fax: +41 22 730 5484

Département du pôle de connaissances numériques (DKH)
Courriel: bdt-dkh@itu.int
Tél.: +41 22 730 5900
Fax: +41 22 730 5484

Département des partenariats pour le développement numérique (PDD)
Courriel: bdt-pdd@itu.int
Tél.: +41 22 730 5447
Fax: +41 22 730 5484

Afrique

Ethiopie
International Telecommunication Union (ITU) Bureau régional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Addis Ababa
Ethiopie

Courriel: itu-ro-africa@itu.int
Tél.: +251 11 551 4977
Tél.: +251 11 551 4855
Tél.: +251 11 551 8328
Fax: +251 11 551 7299

Cameroun
Union internationale des télécommunications (UIT)
Bureau de zone
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Cameroun

Courriel: itu-yaounde@itu.int
Tél.: + 237 22 22 9292
Tél.: + 237 22 22 9291
Fax: + 237 22 22 9297

Sénégal
Union internationale des télécommunications (UIT)
Bureau de zone
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar - Yoff
Sénégal

Courriel: itu-dakar@itu.int
Tél.: +221 33 859 7010
Tél.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU) Bureau de zone
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe

Courriel: itu-harare@itu.int
Tél.: +263 4 77 5939
Tél.: +263 4 77 5941
Fax: +263 4 77 1257

Amériques

Brésil
União Internacional de Telecomunicações (UIT)
Bureau régional
SAUS Quadra 6 Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul (Anatel)
CEP 70070-940 Brasilia - DF
Brazil

Courriel: itubrasilia@itu.int
Tél.: +55 61 2312 2730-1
Tél.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

La Barbade
International Telecommunication Union (ITU) Bureau de zone
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados

Courriel: itubridgetown@itu.int
Tél.: +1 246 431 0343
Fax: +1 246 437 7403

Chili
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chili

Courriel: itusantiago@itu.int
Tél.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras

Courriel: ituteguciglapa@itu.int
Tél.: +504 2235 5470
Fax: +504 2235 5471

Etats arabes

Egypte
International Telecommunication Union (ITU) Bureau régional
Smart Village, Building B 147,
3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
Cairo
Egypte

Courriel: itu-ro-arabstates@itu.int
Tél.: +202 3537 1777
Fax: +202 3537 1888

Asie-Pacifique

Thaïlande
International Telecommunication Union (ITU) Bureau régional
Thailand Post Training Center
5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Thailande

Adresse postale:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Thailand

Courriel: ituasiapacificregion@itu.int
Tél.: +66 2 575 0055
Fax: +66 2 575 3507

Indonésie
International Telecommunication Union (ITU) Bureau de zone
Sapta Pesona Building
13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonésie

Adresse postale:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia

Courriel: ituasiapacificregion@itu.int
Tél.: +62 21 381 3572
Tél.: +62 21 380 2322/2324
Fax: +62 21 389 5521

Pays de la CEI

Fédération de Russie
International Telecommunication Union (ITU) Bureau régional
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Fédération de Russie

Courriel: itumoscow@itu.int
Tél.: +7 495 926 6070

Europe

Suisse
Union internationale des télécommunications (UIT)
Bureau pour l'Europe
Place des Nations
CH-1211 Genève 20
Suisse
Courriel: eurregion@itu.int
Tél.: +41 22 730 5467
Fax: +41 22 730 5484

Union internationale des télécommunications
Bureau de développement des télécommunications
Place des Nations
CH-1211 Genève 20
Suisse

ISBN: 978-92-61-34132-9

Publié en Suisse
Genève, 2021