Union internationale des télécommunications

UIT-T Rapport technique

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS DE L'UIT

(21 novembre 2014)

Contrefaçon d'équipements TIC

Résumé

Chacun s'accorde à reconnaître aujourd'hui que la contrefaçon est un problème socio-économique qui prend de plus en plus d'ampleur. On trouvera dans le présent rapport technique des renseignements à caractère général sur la nature des problèmes que pose la contrefaçon d'équipements utilisant les technologies de l'information et de la communication (TIC), une analyse des conventions internationales se rapportant à ce type d'atteinte aux droits de propriété intellectuelle et des activités menées par certaines organisations pour faire respecter ces droits, ainsi qu'une description des différents moyens permettant de lutter contre le commerce des produits de contrefaçon. En outre, on trouvera dans l'Annexe A un aperçu de plusieurs initiatives prises aux niveaux national et régional pour enrayer le phénomène de la contrefaçon de dispositifs mobiles.

Mots clés

Contrefaçon, de qualité inférieure aux normes exigées.

Numéro de la référence

QSTR-COUNTERFEIT.

Journal de consignation de changement

Le présent rapport constitue la version du rapport technique de l'UIT-T intitulé "*Contrefaçon d'équipements TIC*" approuvé lors de la réunion du groupe de travail 3 (GT 3) de la Commission d'études 11 de l'UIT-T tenue à Genève le 21 novembre 2014.

Editeur: Keith Mainwaring
UNIS
Tél.: +46 76 107 6877
Courriel: keith.mainwaring@ukrainesystems.com

TABLE DES MATIÈRES

LISTE DES FIGURES

Page

Rapport technique de l'UIT-T

Contrefaçon d'équipements TIC

Résumé

Chacun s'accorde à reconnaître aujourd'hui que la contrefaçon est un problème socio-économique qui prend de plus en plus d'ampleur. On trouvera dans le présent rapport technique des renseignements à caractère général sur la nature des problèmes que pose la contrefaçon d'équipements utilisant les technologies de l'information et de la communication (TIC), une analyse des conventions internationales se rapportant à ce type d'atteinte aux droits de propriété intellectuelle et des activités menées par certaines organisations pour faire respecter ces droits, ainsi qu'une description des différents moyens permettant de lutter contre le commerce des produits de contrefaçon. En outre, on trouvera dans l'Annexe A un aperçu de plusieurs initiatives prises aux niveaux national et régional pour enrayer le phénomène de la contrefaçon de dispositifs mobiles.

1 Introduction: produits de contrefaçon: un problème toujours plus préoccupant

Bien que le phénomène soit très difficile à quantifier, tout porte à croire que la diffusion des produits de contrefaçon est un problème de plus en plus préoccupant, tant par son ampleur que par la gamme des produits concernés. En 2008, l'OCDE [1] a publié un rapport selon lequel, sur la base des données de saisies douanières, le commerce international des biens matériels contrefaits et piratés (à l'exclusion des produits numériques ou des produits fabriqués et consommés au niveau national) aurait été supérieur à 200 milliards USD en 2005. D'après des estimations actualisées en fonction de la croissance et de la variation de la composition du commerce international, le commerce des produits de contrefaçon serait passé d'un peu plus de 100 milliards USD en 2000 à 250 milliards USD en 2007, ce qui représente 1,95% du commerce mondial [2]. Selon certaines estimations, ces chiffres seraient encore plus élevés, puisque pour le Bureau d'enquêtes sur la contrefaçon de la Chambre de commerce internationale (ICC), la contrefaçon représenterait 5% à 7% du commerce mondial et pèserait 600 milliards USD par an [3].

Le Groupe de l'ICC chargé de lancer un plan d'action des entreprises pour mettre un terme à la contrefaçon et au piratage (BASCAP) a commandité une étude [4] visant à compléter l'état des lieux dressé par l'OCDE sur les conséquences économiques et sociales de la contrefaçon et du piratage. D'après les estimations figurant dans ce rapport, la valeur économique mondiale des produits de contrefaçon et de piratage s'établirait à 650 milliards USD par an: le commerce international de ces produits représente la moitié de ce total (de 285 à 360 milliards USD), la part de la production et de la consommation nationales se situe entre 140 et 215 milliards USD, tandis que la part des contenus numériques (musique, films et logiciels) est comprise entre 30 et 75 milliards USD. En outre, on estime que la contrefaçon et le piratage coûtent aux pays du G20 et aux consommateurs plus de 125 milliards USD par an (pertes de recettes fiscales et accroissement des dépenses visant à faire appliquer les mesures de rétorsion ainsi que des dépenses consacrées aux soins de santé) et font perdre environ 2,5 millions d'emplois.

Les autorités douanières nationales de l'Union européenne (UE) ont constaté que le nombre de produits de contrefaçon entrant dans l'UE avait triplé entre 2005 et 2010. Les statistiques publiées par la Commission européenne en juillet 2011 font apparaître une forte tendance à la hausse du nombre d'envois que l'on soupçonne d'être en violation des droits de propriété intellectuelle (DPI). En 2010, les douanes ont enregistré environ 80 000 cas, chiffre qui a pratiquement doublé depuis 2009. Plus de 103 millions de produits contrefaits ont été retenus à la frontière extérieure de l'UE. http://trade.ec.europa.eu/doclib/docs/2012/january/tradoc_149003.pdf.

La contrefaçon touche une gamme de produits toujours plus diversifiée: denrées alimentaires et boissons, produits pharmaceutiques, composants électriques et automobiles, produits grand public de toutes sortes et même un magasin de gros. Les composants informatiques (écrans, boîtiers, disques durs), le matériel informatique, les routeurs, les caméras web, les télécommandes, les téléphones mobiles, les téléviseurs, les disques compacts (CD) et les lecteurs de disques numériques polyvalents (DVD), les haut-parleurs, les caméras, les écouteurs, les adaptateurs USB (bus série universel), les logiciels, les certificats, les marques et les données de certification (par exemple les données biométriques) sont autant de produits faisant l'objet d'une contrefaçon.

En outre, l'Internet est de plus en plus utilisé pour la piraterie numérique et est devenu un marché pour la contrefaçon de produits. Tous ces facteurs qui font de l'Internet une ressource extrêmement attrayante pour les revendeurs, en particulier ceux qui ciblent les marchés "étroits" (présence sur le marché mondial, facilité de création, de déplacement et de fermeture de sites web pour les rendre plus attrayants et modicité des coûts de l'envoi de courriers électroniques), conjugués à l'anonymat que permet la communication sur l'Internet, expliquent l'intérêt porté à la revente de produits de contrefaçon. Sans oublier qu'en raison du nombre considérable de sites Internet, il est très difficile pour les détenteurs de droits de propriété intellectuelle et pour les organismes chargés de faire respecter ces droits de repérer les opérations illégales. Les sollicitations par courrier électronique, les sites de vente en ligne et les sites d'enchères sont autant de tentatives utilisées pour vendre des produits de contrefaçon.

En ce qui concerne le secteur des TIC il ressort d'un rapport de KPMG et de l'AGMA que 8 à 10% de tous les produits issus du secteur des technologies de l'information (TI) qui sont vendus dans le monde sont des produits contrefaits, et que la contrefaçon a entraîné, en 2007, un manque à gagner de l'ordre de 100 milliards USD pour l'industrie informatique. Hewlett-Packard a mené entre 2005 et 2009 plus de 4 620 enquêtes dans 55 pays, qui ont permis la saisie de fournitures d'imprimerie de contrefaçon d'une valeur de plus de 795 millions USD [6]. La part de l'électronique grand public dans les saisies effectuées par les autorités douanières des Etats-Unis a été de 22% en 2011, la valeur des produits ayant augmenté de 16% en 2010. Un tiers environ des produits entrant dans cette catégorie étaient des téléphones mobiles [5].

En 2011, il existait d'après les estimations un marché mondial de 250,4 millions de téléphones mobiles contrefaits http://press.ihs.com/press-release/design-supply-chain/cellphone-gray-market-goes-legit-sales-continue-decline, soit environ 16% des 1 546 millions de combinés écoulés en 2011 [8]. Ces données estimatives du taux de pénétration des produits contrefaits sur le marché des téléphones mobiles correspondent à celles fournies dans l'étude sur l'internationalisation et la fragmentation des chaînes de valeur ainsi que la sécurité de l'offre effectuée en 2011 pour le compte de la Commission européenne. D'après cette étude, les téléphones mobiles contrefaits représentent 15 à 20% du marché mondial en termes d'unités vendues, et près de 9 milliards USD en termes de recettes.

Les composants électroniques de contrefaçon peuvent non seulement être utilisés pour produire des dispositifs contrefaits, mais également entrer dans les chaines d'approvisionnement de produits légitimes. L'utilisation de composants électroniques contrefaits dans les équipements militaires des Etats-Unis a fait la une de l'actualité à l'automne 2011, lors d'une audition devant la Commission des forces armées du Sénat américain sur l'électronique de contrefaçon au sein du Département de la chaîne d'approvisionnement de la Défense [9]. Une étude menée par le Bureau de l'industrie et de la sécurité du Département du Commerce [10] a révélé l'existence de 1 800 cas dans lesquels on avait constaté la présence de pièces électroniques de contrefaçon impliquant plus d'un million de parties suspectes. On a également constaté que le nombre d'incidents était passé de 3 868 en 2005 à 9 356 en 2008. Suite à cette audition, la Loi d'autorisation de la défense nationale (National Defence Authorisation Act – NDAA) promulguée en 2012 fournit des orientations sur la lutte contre la contrefaçon de composants et prévoit notamment la réalisation d'inspections

additionnelles sur les composants électroniques importés, tout en confiant aux entrepreneurs l'entière responsabilité de repérer les composants de contrefaçon et de remédier aux cas dans lesquels de tels composants se retrouvent dans certains produits [11].

Il ressort d'une étude effectuée par l'OCDE en 2008 que la plupart des produits de contrefaçon proviennent d'un pays asiatique (qui représente 69,7% des saisies de produits de contrefaçon).

On trouvera dans le présent Rapport technique des informations à caractère général sur le problème de la contrefaçon et sur les mesures prises pour endiguer ce phénomène, l'accent étant mis tout particulièrement sur la contrefaçon d'équipements TIC et sur les outils TIC susceptibles d'être utilisés pour remédier à ce problème.

A ces dispositifs de contrefaçon viennent s'ajouter une profusion d'équipements et d'accessoires TIC communément désignés sous le nom de produits "ne répondant pas aux normes" ou "non autorisés". Bien qu'il n'existe aucune définition universelle normalisée de ces termes, on peut dire que ces dispositifs utilisent fréquemment des composants de qualité inférieure et, le plus souvent, qu'ils ne satisfont pas aux dispositions juridiques nationales applicables en matière de certification, d'approbation, de distribution et de vente de dispositifs mobiles. Ces dispositifs ne s'accompagnent pas dans tous les cas d'atteintes aux droits de propriété intellectuelle des fabricants et ne correspondent dès lors pas à la définition communément admise de la "contrefaçon". En conséquence, ils ne seront pas traités dans le présent Rapport technique, qui sera axé sur les dispositifs de contrefaçon. Les dispositifs "ne répondant pas aux normes" posent un certain nombre de problèmes distincts et appellent des solutions qui doivent faire l'objet d'un examen séparé.

2 Qu'est-ce que la contrefaçon?

L'Accord de l'OMC sur les aspects des droits de propriété intellectuelle qui touchent au commerce (Accord sur les ADPIC) définit l'expression "marchandises de marque contrefaites" en ces termes: "toutes les marchandises, y compris leur emballage, portant sans autorisation une marque de fabrique ou de commerce qui est identique à la marque de fabrique ou de commerce valablement enregistrée pour lesdites marchandises, ou qui ne peut être distinguée dans ses aspects essentiels de cette marque de fabrique ou de commerce, et qui de ce fait porte atteinte aux droits du titulaire de la marque en question en vertu de la législation du pays d'importation"; (note 14 relative à l'Article 51). Le terme "contrefait" n'est donc employé dans l'Accord sur les ADPIC que dans le domaine des marques de fabrique ou de commerce. Il désigne des marchandises contrefaisantes qui sont définies avec davantage de précision que les atteintes classiques portées aux droits de marques, au motif que la marque de fabrique ou de commerce est identique ou pratiquement impossible à distinguer de l'original. Ce texte ne traite pas de la finalité de l'utilisation de marchandises de marque contrefaites, mais définit un produit de contrefaçon en fonction du lien étroit qui existe entre la marque utilisée et un produit enregistré et s'applique aux cas dans lesquels les produits sont les mêmes que ceux pour lesquels la marque de fabrique ou de commerce est enregistrée. Concrètement, ces produits contrefaits comprennent en général les cas dans lesquels une marque est copiée servilement, afin de donner à dessein l'impression de correspondre à un produit authentique. Ils s'accompagnent en général d'une intention de fraude, puisque la confusion entre le produit authentique et la copie est délibérée.

Dans cette même note de l'Accord sur les ADPIC, l'expression "marchandises pirates portant atteinte au droit d'auteur" s'entend de "toutes les copies faites sans le consentement du détenteur du droit ou d'une personne dûment autorisée par lui dans le pays de production et qui sont faites directement ou indirectement à partir d'un article dans les cas où la réalisation de ces copies aurait constitué une atteinte au droit d'auteur ou à un droit connexe en vertu de la législation du pays d'importation". Le terme "piratage" désigne donc une atteinte au droit d'auteur ou à un droit connexe au sens de l'Accord sur les ADPIC.

3 Conséquences de la contrefaçon d'équipements et de composants TIC

Les équipements TIC de contrefaçon ont pour la société des conséquences particulières, que n'ont pas nécessairement d'autres types de violations des droits de propriété intellectuelle. Ainsi, en général, les produits de contrefaçon n'auront pas été testés en bonne et due forme, ni homologués conformément aux prescriptions réglementaires susceptibles d'être applicables. L'utilisation des produits de contrefaçon peut être extrêmement dangereuse. On a par exemple signalé des cas de décès suite à l'explosion de batteries de contrefaçon, des cas d'électrocution et d'incendie dus à des chargeurs ainsi que des cas avérés dans lesquels ces dispositifs contenaient des substances dangereuses dans des concentrations importantes (plomb et cadmium par exemple).

Le rapport établi par l'OCDE en 2008 contenait une analyse des incidences socio-économiques de la contrefaçon sur les détenteurs de droits, les consommateurs et les gouvernements:

- Sous l'angle des incidences socio-économiques, la contrefaçon risque fort d'avoir des retombées négatives sur l'innovation, les niveaux d'investissement étranger direct, la croissance de l'économie et le taux d'emploi, et d'entraîner une réorientation des ressources vers les réseaux du crime organisé.
- La contrefaçon aura probablement des conséquences économiques sur les titulaires de droits, étant donné que les volumes des ventes et les redevances, les prix, l'image et la réputation de la marque, les coûts ainsi que le champ d'application des activités s'en trouveront affectés.
- Il se peut également que les consommateurs constatent que la qualité des produits de contrefaçon est inférieure à la norme et soient confrontés à des risques graves pour la santé et la sécurité.
- Les gouvernements seront privés d'une partie de leurs recettes fiscales et risquent d'être confrontés à des problèmes de corruption, qui les obligeront à mobiliser davantage de ressources pour contrer le phénomène de la contrefaçon.

3.1 Exemples d'équipements TIC de contrefaçon

On trouvera ci-après des exemples des principales conséquences de la contrefaçon d'équipements TIC.

3.1.1 Téléphones mobiles

Le phénomène de la contrefaçon des téléphones mobiles a de nombreuses conséquences négatives pour la société[1]:

- baisse de la qualité des services de télécommunication mobile, qui influe à son tour sur l'expérience-utilisateur et l'expérience-entreprise;
- risque de sécurité pour les consommateurs, en raison de l'utilisation de composants ou de matériaux défectueux ou inappropriés;
- menaces accrues sur la cybersécurité;
- risques pour la vie privée des consommateurs;
- dégradation de la sécurité des transactions numériques;
- non-paiement des taxes et des droits applicables, ce qui a des conséquences négatives sur les recettes fiscales;

---

[1] Le texte ci-après est fondé sur le document du Mobile Manufacturers Forum (MMF) "Téléphones portables contrefaits/de qualité inférieure – Guide de ressources à l'intention des gouvernements". http://www.mmfai.org/public/docs/eng/MMF%5FCounterfeitPhones%5FEN%2Epdf.

- les consommateurs les plus vulnérables sur le plan financier sont pénalisés, en ce sens qu'aucune garantie ne leur est offerte ou encore que les lois relatives à la protection des consommateurs ne sont pas respectées;
- risques pour l'environnement et la santé des consommateurs, en raison de l'utilisation de substances dangereuses dans la fabrication de ces dispositifs;
- la contrefaçon facilite le trafic de stupéfiants et favorise le terrorisme ainsi que d'autres activités criminelles au niveau local ou international;
- la distorsion du marché créée par les pratiques de concurrence déloyale et les pratiques frauduleuses entraînent un préjudice économique;
- la contrefaçon porte atteinte aux marques de commerce des entreprises qui fabriquent les produits d'origine.

Une étude menée par l'Instituto Nokia de Tecnologia (INdT), organisme indépendant de recherche-développement basé au Brésil, a confirmé la qualité médiocre des téléphones de contrefaçon et les incidences négatives qu'ils pouvaient avoir sur les consommateurs, les exploitants de télécommunication et l'activité économique locale. Cette étude portait sur 44 téléphones mobiles contrefaits ou de qualité inférieure, qui ont été comparés avec des téléphones d'origine et homologués. L'étude a démontré que les téléphones contrefaits enregistraient des résultats largement inférieurs aux téléphones d'origine, avec 26% d'échecs de connexion et 24% d'interruptions d'appel. En outre, dans les lieux où un téléphone d'origine pouvait parfaitement fonctionner, les téléphones de contrefaçon n'étaient pas utilisables en raison de leur qualité de transmission inférieure par rapport aux téléphones d'origine. Des problèmes de transfert de cellules (transfert automatique de la communication lors du passage d'une cellule à l'autre) ont également été signalés, le délai de transfert étant supérieur de 41% à celui des téléphones d'origine, avec un taux d'échec de transfert des appels de 34%. Voir les Figures reproduites dans l'Annexe 1 du document du Mobile Manufacturers Forum (MMF) "Téléphones portables contrefaits/de qualité inférieure – Guide de ressources à l'intention des gouvernements". http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf.

De plus, les téléphones mobiles de contrefaçon présentent des risques importants pour la santé et la sécurité. Ces dispositifs peuvent en effet contenir des substances chimiques dans des concentrations supérieures aux normes de sécurité établies et sont plus difficiles à collecter dans le cadre des programmes de gestion des déchets d'équipements électriques et électroniques. Ces difficultés se font particulièrement sentir dans les pays en développement, qui ne disposent que de capacités de recyclage écologiquement rationnelles limitées, voire inexistantes, et où il existe un volume considérable de dispositifs mobiles de contrefaçon. La désactivation de ces dispositifs pour lutter contre le problème de la contrefaçon vient encore compliquer ce problème pour les pays en développement.

Les produits de contrefaçon, dont le montage laisse souvent à désirer et qui utilisent des composants de mauvaise qualité, contiennent des substances dangereuses dont l'utilisation est interdite dans maints pays assujettis à la directive RoHS, qui restreint l'utilisation de certaines substances, ou à des législations nationales équivalentes.

Une autre étude menée récemment par l'Instituto Nokia de Tecnologia du Brésil (INdT) sur les substances dangereuses illustre les dangers potentiels des téléphones portables de contrefaçon. L'objectif de cette étude était plus précisément d'évaluer si les téléphones de contrefaçon étaient conformes à la directive européenne RoHS visant à limiter l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques. Cette directive restreint l'utilisation de six substances dangereuses dans différents types d'équipements électriques et électroniques.

Cette étude, qui utilisait la méthode d'essai CEI 62321 [75], a consisté à tester cinq téléphones de contrefaçon intégrés (CI) composés de 158 pièces (coques, écrans, circuits intégrés, claviers et autres composants montés en surface (CMS)). L'étude du INdT a révélé la présence de deux substances dangereuses (plomb et cadmium), tant dans les composants internes que dans les composants externes, dans des concentrations nettement supérieures aux valeurs maximales autorisées par la directive RoHS. La Figure A intitulée "Test: Substances dangereuses – Analyse chimique" reproduite dans le document du MMF "Téléphones portables contrefaits/de qualité inférieure – Guide de ressources à l'intention des gouvernements" http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf illustre les niveaux excessifs de plomb et de cadmium détectés dans les composants internes et externes des téléphones mobiles testés.

D'autres études menées dans différents pays ont confirmé la présence de substances dangereuses dans les téléphones mobiles de contrefaçon. L'une d'entre elles a été réalisée en Inde (Hyderabad) par le Centre for Materials for Electronics Technology (C-MET), afin de vérifier si les appareils mobiles mis sur le marché indien étaient conformes à la directive RoHS. Aux fins de cette étude, le C-MET a sélectionné 15 modèles de téléphones mobiles largement utilisés, en fonction de l'engouement qu'ils suscitent et de leur disponibilité sur le marché. Les tests ont également été réalisés selon les procédures CEI 62321 (2008).

Il ressort des résultats que des substances dangereuses, en particulier du plomb (Pb), étaient présentes dans tous les téléphones mobiles de contrefaçon, dans des concentrations extrêmement élevées. Dans certains cas, les valeurs étaient 35 à 40 fois supérieures aux limites autorisées au niveau mondial. De nombreux composants critiques tels que le logement pour la carte mémoire, celui pour la carte SIM, l'appareil photo, etc., qui impliquent un contact physique direct pour le consommateur, se sont avérés être ceux qui contenaient le plus de substances dangereuses, les risques étant bien plus importants que s'il s'agissait de composants se trouvant à l'intérieur des dispositifs. En revanche, les tests effectués sur des téléphones portables de marques internationales et autres marques reconnues ont démontré que ces dispositifs respectaient les limites acceptables de la directive RoHS et étaient par conséquent sans danger pour les consommateurs. La Figure B reproduite dans le document du MMF "Téléphones portables contrefaits/de qualité inférieure – Guide de ressources a l'intention des gouvernements" http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf donne un aperçu des résultats de cette étude, tandis que la Figure C reproduite dans ce même document indique les régions dans lesquelles des concentrations élevées de plomb ont été détectées.

En outre, l'utilisation de téléphones portant un numéro d'identité internationale d'équipements mobiles (IMEI) déjà existant, ou faux ou dépourvu d'un tel numéro fait peser de graves menaces sur la sécurité nationale et la sécurité des personnes, dans la mesure où il est difficile d'en suivre la trace sur le réseau.

L'Autorité du Kenya chargée de la lutte contre la contrefaçon a indiqué que le marché de la contrefaçon de dispositifs mobiles avait fait perdre 38,5 millions USD au Kenya [39], ce qui illustre les pertes de recettes que peut engendrer le commerce de dispositifs mobiles de contrefaçon. L'installation en Ukraine du Système d'information automatisé pour l'enregistrement des terminaux mobiles (AISMTRU) en 2009 a permis de dégager 500 millions USD de recettes supplémentaires entre 2000 et 2012, grâce au paiement de droits de douane à l'importation sur les terminaux mobiles. Avant la mise en oeuvre de ce système en 2009, seuls 5 à 7% des dispositifs mobiles en circulation en Ukraine étaient légalement importés, alors qu'à l'heure actuelle, ce pourcentage est compris entre 92 et 95% [40].

3.1.2 Accessoires et composants des produits TIC

La contrefaçon touche souvent les accessoires des produits TIC qui sont vendus et notamment, dans le cas des téléphones mobiles et d'autres produits TIC, les batteries, les chargeurs et les écouteurs. Dans le cas des imprimantes, ce sont souvent les cartouches d'encre qui sont contrefaites. Pour ce qui est des appareils photo numériques, on trouve parmi les accessoires de contrefaçon, par exemple les câbles et les cartes mémoires, de faux objectifs parfaitement intégrés au boîtier de l'appareil, et il existe même de faux composants au niveau de la puce électronique. Le remplacement accidentel ou délibéré de composants par des composants électroniques de contrefaçon peut causer des préjudices graves aux utilisateurs, lorsque ces composants sont utilisés dans du matériel médical ou dans d'autres produits TIC essentiels pour la sécurité. En 2013, des clones de cartes sans contact MIFARE ont été saisis au salon organisé à Paris. http://www.react.org/news-a-events/item/567-mifare.

Les batteries de contrefaçon sont largement répandues dans le monde entier et ce phénomène est particulièrement préoccupant. Les batteries ont notamment provoqué un certain nombre d'incendies. Parmi les types de batteries de contrefaçon, on citera les batteries alcalines de type AA et les batteries rechargeables au lithium-ion, que l'on trouve dans de nombreux types différents de produits, et plus particulièrement dans les téléphones mobiles.

Des cas de décès consécutifs à l'utilisation de batteries de contrefaçon ont également été signalés http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aLWvmmrHx9F0. A cet égard, il convient de noter que les batteries de contrefaçon sont très utilisées dans les zones défavorisées, car le taux d'utilisation des portables y est plus élevé, d'où la nécessité de remplacer plus fréquemment les batteries.

Des incidents analogues ont été signalés dans divers pays. Les incidents liés à l'utilisation de batteries de contrefaçon à bord d'aéronefs qui ont été rapportés constituent une source de préoccupation croissante. En février 2014, Geoff Leach, de l'Autorité de l'aviation civile du Royaume-Uni, s'est déclaré particulièrement préoccupé par l'existence de "copies de batteries bon marché, provenant de sources douteuses en ligne, qui risquaient d'être à l'origine de défaillances aux conséquences dramatiques". http://www.bbc.co.uk/news/business-25733346.

En 2004, alors qu'il témoignait devant la Commission des affaires judiciaires du Sénat des Etats-Unis, un représentant de Gillette a expliqué qu'en une semaine, cette entreprise avait saisi un million de fausses piles Duracell, entre autres nombreux produits de contrefaçon. http://www.judiciary.senate.gov/hearings/testimony.cfm?renderforprint=1&id=4f1e0899533f7680e78d03281ff674b8&wit_id=4f1e0899533f7680e78d03281ff674b8-2-2.

Le cas des écouteurs est particulièrement préoccupant, en ce sens que des écouteurs de contrefaçon de mauvaise qualité peuvent non seulement altérer l'ouïe, mais aussi présenter un risque potentiel d'incendie. En 2013, selon certaines informations, des responsables auraient saisi des écouteurs de contrefaçon d'une valeur de 15 millions GBP. http://www.express.co.uk/news/uk/387869/Designer-headphones-top-16m-deluge-of-fake-goods.

3.1.3 Emetteurs-récepteurs radiophoniques

Motorola Solutions Inc. a mis en garde ses clients contre l'achat d'émetteurs-récepteurs radiophoniques de contrefaçon qui ont été trouvés au Vietnam en 2013. Ces dispositifs peuvent présenter des dangers pour les utilisateurs: ils constituent non seulement des copies de modèles d'émetteurs-récepteurs radiophoniques de Motorola, mais portent aussi le logo et les numéros de modèle de cette entreprise, d'où la difficulté pour les consommateurs de les distinguer des produits d'origine.
http://nz.finance.yahoo.com/news/motorola-solutions-counterfeit-two-way-030000020.html.

3.1.4 Appareils photo numériques

Les appareils photo numériques font partie de la longue liste des produits TIC faisant l'objet de contrefaçon. Comme pour d'autres produits, ils sont très difficiles à identifier et les fournisseurs, les détaillants et les utilisateurs fournissent parfois des indications destinées à aider les consommateurs à identifier les faux produits.
http://www.ebay.co.uk/gds/How-to-Identify-a-Fake-Nikon-Camera-/10000000177984982/g.html.

Il arrive que des dispositifs de contrefaçon tels que les caméras web présentent des risques élevés pour la sécurité et la vie privée des utilisateurs. Non seulement les logiciels dont ces produits sont équipés au départ de qualité médiocre ou défectueuse, mais l'utilisateur ne bénéficiera d'aucune mise à jour de sécurité ni d'aucune assistance par la suite, de sorte qu'il sera encore plus exposé aux cybermenaces.

3.1.5 Ordinateurs personnels et tablettes

L'engouement suscité par certains types d'ordinateurs et de tablettes a entraîné une généralisation de la contrefaçon. Dans certains cas, ces produits sont en fait des "leurres" et ne contiennent même pas de circuit imprimé. http://www.cnn.com/2013/03/22/tech/mobile/fake-ipads-walmart/. Les produits dotés de composants électroniques sont parfois préinstallés et un logiciel malveillant est intégré dans des versions contrefaites des systèmes d'exploitation.
http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware.

3.1.6 Jouets électroniques

La plupart des jouets contiennent aujourd'hui des composants électroniques. Qu'il s'agisse de fausses consoles de jeux ou des jeux portatifs, en passant par les jouets pour bébés, tous ces objets peuvent causer des dommages corporels à l'enfant. Comme exemples de risques pour la sécurité, on citera les prises électriques sans mise à la terre, qui peuvent provoquer une électrocution.
http://www.theguardian.com/money/2011/dec/07/christmas-shopping-counterfeit-toys.

4 Conventions sur les droits de propriété intellectuelle (DPI)

Un certain nombre d'accords internationaux et de conventions internationales énoncent des normes de fond relatives à la protection des DPI conformément aux législations nationales, ainsi que des exceptions et des limites autorisées, et définissent les procédures que les gouvernements nationaux s'engagent à prévoir pour permettre aux titulaires de droits de prendre des mesures effectives pour se prémunir contre des actes délictueux.

4.1 Convention de Paris pour la protection de la propriété industrielle et Convention de Berne pour la protection des oeuvres littéraires et artistiques

L'Organisation mondiale de la propriété intellectuelle (OMPI) administre les traités multilatéraux concernant la propriété intellectuelle. Les principaux traités sont la Convention de Paris pour la protection de la propriété industrielle et la Convention de Berne pour la protection des oeuvres littéraires et artistiques.

La Convention de Paris a été signée en 1883 et a par la suite été révisée à plusieurs reprises. La protection de la propriété industrielle a pour objet "les brevets d'invention, les modèles d'utilité, les dessins ou modèles industriels, les marques de fabrique ou de commerce, les marques de service, le nom commercial et les indications de provenance ou appellations d'origine, ainsi que la répression

de la concurrence déloyale" [18]. En ce qui concerne la contrefaçon, cette Convention fait obligation aux Etats Contractants de prendre des mesures "en cas d'utilisation directe ou indirecte d'une indication fausse concernant la provenance du produit ou l'identité du producteur, fabricant ou commerçant".

4.2 Organisation mondiale du commerce (OMC) – Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC)

L'Organisation mondiale du commerce (OMC) administre l'Accord sur les ADPIC, qui fixe les normes minimales que doivent appliquer tous les Membres de l'OMC, tant en ce qui concerne la protection sur le fond que pour ce qui est des procédures destinées à faire respecter les DPI. L'Accord sur les ADPIC introduit pour la première fois un ensemble complet de dispositions destinées à faire respecter les DPI dans un accord multilatéral. Les différents qui peuvent survenir entre les Membres de l'OMC à cet égard doivent être réglés dans le cadre de l'Accord de l'OMC sur le règlement des différends.

Les dispositions de l'Accord sur les ADPIC relatives aux moyens de faire respecter les DPI ont deux objectifs fondamentaux: premièrement, faire en sorte que des moyens efficaces de faire respecter les DPI soient mis à la disposition des détenteurs de droits et, deuxièmement, veiller à ce que ces procédures soient appliquées de manière équilibrée et proportionnée et ne fassent pas obstacle au commerce légitime. Ces dispositions sont subdivisées en cinq sections. La première énonce les obligations générales auxquelles toutes les procédures destinées à faire respecter les DPI doivent satisfaire afin, notamment, que leur efficacité soit garantie et que certains principes fondamentaux nécessaires à une procédure régulière soient respectés. Les sections suivantes traitent des procédures et mesures correctives civiles et administratives, des mesures provisoires, des prescriptions spéciales concernant les mesures à la frontière et des procédures pénales.

L'Accord établit une distinction entre les activités qui portent atteinte aux DPI en général, pour lesquelles des procédures et des mesures correctives civiles ou administratives doivent être prévues, et la contrefaçon et le piratage – formes les plus flagrantes d'atteinte aux droits – pour lesquels des procédures et des mesures correctives supplémentaires doivent aussi être prévues, en l'occurrence des mesures à la frontière et des procédures pénales. A cette fin, les marchandises contrefaites sont définies par essence comme des marchandises impliquant une copie servile de la marque, et les marchandises pirates comme des marchandises qui violent un droit de reproduction découlant du droit d'auteur ou d'un droit connexe.

Les obligations détaillées incombant aux Membres de l'OMC sont décrites ci-après:

a) Procédures civiles et administratives: Le détenteur d'un droit doit avoir la possibilité d'engager une procédure civile, judiciaire ou, à titre facultatif, administrative à l'égard d'un contrevenant en ce qui concerne les DPI couverts par l'Accord. Ces procédures civiles et administratives doivent être loyales et équitables Certaines règles concernant les éléments de preuve sont établies. En outre, les Membres sont tenus d'habiliter les autorités judiciaires à prendre trois types de mesures correctives: injonctions, dommages-intérêts et autres mesures correctives. Dans le cadre des sauvegardes contre l'usage abusif des procédures destinées à faire respecter les DPI, les obligations s'étendent également à l'indemnisation du défendeur lorsque le détenteur d'un droit a utilisé abusivement des procédures destinées à faire respecter les droits.

b) Mesures provisoires: Les injonctions temporaires sont un outil important dans l'attente du règlement d'un différend au niveau judiciaire. En conséquence, les autorités judiciaires seront habilitées à ordonner l'adoption de mesures provisoires rapides et efficaces pour faire cesser immédiatement toute atteinte alléguée. Ces mesures visent à empêcher qu'un acte portant atteinte à un DPI ne soit commis et à sauvegarder les éléments de preuve pertinents

relatifs à cette atteinte alléguée. Comme les autres sections sur les moyens de faire respecter les DPI, les dispositions de cette section prévoient également certaines procédures requises et certaines sauvegardes pour éviter l'usage abusif des mesures provisoires.

c) Mesures à la frontière: Ces mesures permettent aux détenteurs de droits d'obtenir la coopération des autorités douanières pour intercepter à la frontière les marchandises portant atteinte à des DPI et empêcher leur mise en circulation. Elles sont obligatoires pour les marchandises de marque contrefaites et les marchandises pirates portant atteinte aux droits d'auteur, mais les Membres peuvent prévoir des mesures à la frontière pour les marchandises qui impliquent des atteintes à d'autres DPI, les marchandises portant atteinte à des DPI destinées à être exportées, les marchandises en transit, les importations de *minimis* et les importations parallèles. De même que les autres procédures relatives aux mesures provisoires, les mesures à la frontière sont soumises à certaines règles de procédure et à des sauvegardes contre les usages abusifs. En ce qui concerne les mesures correctives, les autorités compétentes doivent être habilitées à ordonner la destruction ou la mise hors circuits commerciaux de marchandises portant atteinte à un droit.

d) Procédures pénales: Des procédures pénales devront être mises en place pour les actes délibérés de contrefaçon de marque de fabrique ou de commerce ou de piratage portant atteinte à un droit d'auteur, commis à une échelle commerciale. L'application de ces procédures aux autres actes portant atteinte à des DPI est facultative. En ce qui concerne les mesures correctives, l'Accord stipule que les sanctions pénales doivent inclure l'emprisonnement et/ou des amendes suffisantes et, dans les cas appropriés, la saisie, la confiscation et la destruction des marchandises en cause et de tous matériaux et instruments ayant servi à les produire.

A l'heure actuelle, les pays les moins avancés Membres de l'OMC bénéficient de dispositions transitoires en vertu desquelles ils ne sont pas tenus d'appliquer les normes de protection et les normes destinées à faire respecter les droits énoncées dans l'Accord sur les ADPIC, généralement pendant un délai allant jusqu'à juillet 2021, ni de respecter les dispositions relatives à la protection et l'application des brevets et des renseignements non divulgués pour les produits pharmaceutiques, pendant un délai allant jusqu'à janvier 2016. L'objectif est notamment de leur permettre de se doter d'une base technologique viable.

5 Mise en oeuvre des DPI

Bien qu'il existe des traités internationaux concernant la protection des droits de propriété intellectuelle depuis plus d'un siècle, ce n'est que récemment que la question de la protection de ces droits a été examinée sur la scène internationale. Cela tient au fait que l'Accord sur les ADPIC fournit les bases nécessaires dans ce domaine et s'explique aussi par les conséquences de plus en plus importantes, sur le plan socio-économique, des atteintes aux DPI. La question de la mise en oeuvre des DPI figure aujourd'hui parmi les priorités d'un grand nombre d'organisations internationales, notamment l'OMPI, l'Organisation mondiale des douanes (OMD) et Interpol, au sein de l'Union européenne ainsi que dans de nombreux pays.

5.1 Organisation mondiale de la propriété intellectuelle (OMPI)

L'Organisation mondiale de la propriété intellectuelle (OMPI) a créé en 2002 un Comité consultatif sur l'application des droits (ACE), en vue de mener des activités de coordination avec d'autres organisations internationales et le secteur privé pour lutter contre la contrefaçon et le piratage. L'ACE coordonne l'organisation de programmes de formation et offre une assistance technique.

L'OMPI collabore en outre avec le Programme des Nations Unies pour l'environnement (PNUE) et d'autres organisations telles que la Commission économique et sociale des Nations Unies pour l'Asie et le Pacifique (CESAP), afin de sensibiliser l'opinion au problème du recyclage et de l'élimination des produits de contrefaçon, dont le volume ne cesse de croître.
http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html.
http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx.
http://www.unescap.org/events/wipoescapunep-workshop-environmentally-safe-disposal-ip-infringing-goods.

5.2 Organisation mondiale du commerce – Conseil des ADPIC

Le Conseil des ADPIC est l'un des trois Conseils relevant du Conseil général de l'OMC. Il est chargé d'administrer l'Accord sur les ADPIC et, en particulier, de suivre le fonctionnement de l'Accord et de contrôler si les Membres s'acquittent de leurs obligations au titre dudit Accord. Le Conseil tient des réunions formelles à Genève trois fois par an et, le cas échéant, des réunions informelles. Ces réunions offrent un cadre de discussion et de consultation sur les questions relatives à l'Accord sur les ADPIC et permettent aussi de clarifier ou d'interpréter des dispositions de l'Accord. La mise en oeuvre des DPI a été examinée sur une base ponctuelle par le Conseil des ADPIC à plusieurs occasions, dont la dernière remonte à 2012.

5.3 Office des Nations Unies contre la drogue et le crime (ONUDC)

L'ONUDC est le dépositaire de la Convention des Nations Unies contre la criminalité transnationale organisée, plate-forme mondiale de coopération qui vise à lutter contre le crime organisé sous toutes ses formes. A ce jour, 167 pays sont parties à la Convention et se sont engagés à coopérer pour lutter contre la criminalité transnationale organisée et à s'assurer que leurs lois nationales soient compatibles.

L'ONUDC tient des réunions biannuelles des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée, au cours desquelles des représentants de gouvernements du monde entier encouragent et examinent la mise en oeuvre de la Convention, afin d'améliorer les méthodes de lutte contre ce phénomène. La dernière réunion de l'ONUDC a eu lieu en octobre 2012.

L'Office des Nations Unies contre la drogue et le crime s'est plus particulièrement penché sur le lien entre la contrefaçon et la criminalité transnationale organisée http://www.unodc.org/counterfeit/. L'ONUDC a lancé en janvier 2014 une campagne intitulée "Contrefaçon: Ne soutenez pas le crime organisé", afin de sensibiliser les consommateurs au fait que le trafic illicite de biens contrefaits pèse plus de 250 milliards USD par an. Cette campagne fait prendre conscience aux consommateurs que l'achat de biens contrefaits peut être une source de financement des groupes criminels organisés, met la santé et la sécurité des consommateurs en péril et suscite d'autres préoccupations d'ordre éthique et environnemental.

Par le biais de ses programmes d'assistance technique, l'ONUDC s'emploie également à endiguer les flux de produits illégaux tels que les contrefaçons ou les drogues. L'ONUDC et l'Organisation mondiale des douanes ont ainsi lancé le Programme de contrôle des conteneurs (CCP) en 2006. Ce programme a permis d'obtenir des résultats remarquables, puisque 487 conteneurs de produits contrefaits et de contrebande ainsi que 195 conteneurs de drogues ont été saisis.

https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html.

https://www.unodc.org/unodc/en/frontpage/2012/July/criminals-rake-in-250-billion-per-year-in-counterfeit-goods-that-pose-health-security-risks-to-unsuspecting-public.html.

5.4 Organisation mondiale des douanes (OMD)

L'OMD est un organisme intergouvernemental composé de 179 administrations douanières, dont la mission est d'orienter l'action de ses Membres et de leur fournir des directives ainsi qu'un appui aux fins de la facilitation du commerce et de la sécurisation des échanges licites, du recouvrement des recettes fiscales, de la protection de la société et du renforcement des capacités. Etant donné que les administrations douanières sont chargées de la protection des frontières nationales contre les flux illicites de produits de contrefaçon et de piratage, l'OMD dirige les discussions sur l'action mondiale entreprise pour lutter contre ces délits. Cette action consiste à encourager les initiatives destinées à lutter contre la contrefaçon et le piratage, en améliorant les méthodes de mise en oeuvre et en encourageant l'échange d'informations entre les douanes elles-mêmes ainsi qu'entre les douanes et le secteur privé.

Les principaux objectifs du Programme sur les DPI, la santé et la sûreté de l'OMD sont d'attirer l'attention des agents des douanes et des entreprises du monde entier sur la nécessité de faire preuve de vigilance à l'égard des produits de contrefaçon. L'OMD a fait de la protection de la santé et de la sûreté du consommateur sa grande priorité et s'emploie activement à prendre des mesures de renforcement des capacités, tout en élaborant divers instruments d'application des réglementations.

Consciente de l'importance de la collaboration avec le secteur privé, l'OMD travaille en étroite liaison avec des représentants du secteur privé et d'associations professionnelles, afin d'évaluer leurs besoins ainsi que les problèmes qu'ils rencontrent lorsqu'ils sont confrontés à ce phénomène. L'OMD invite à intervalles réguliers les détenteurs de droits à participer à ses diverses activités de lutte contre la contrefaçon, par exemple aux opérations sur le terrain et à des séminaires régionaux ou nationaux, et a mis au point un outil en ligne, à savoir l'interface public membres (IPM), pour permettre aux agents des douanes de détecter les produits de contrefaçon et de piratage et de communiquer en temps réel avec les acteurs économiques.

Les opérations à grande échelle constituent un volet essentiel des initiatives prises par l'OMD en matière de lutte contre la contrefaçon, dans le cadre desquelles de nombreuses administrations douanières renforcent simultanément leur niveau de contrôle de l'application des réglementations concernant les produits de contrefaçon, afin de quantifier et de qualifier les incidences des activités de contrefaçon à l'échelle mondiale. Rien qu'en 2013, plus de 1,1 milliard de produits de contrefaçon ont été interceptés par les administrations douanières lors de deux opérations à grande échelle organisées l'une dans la région Afrique, et l'autre dans la région Amérique latine.

L'OMD a également conçu un outil mondial de détection en ligne (IPM), pour aider les agents des douanes de première ligne à distinguer les marchandises contrefaites des marchandises authentiques ainsi que leurs reproductions. Depuis son lancement en 2010, l'outil anti-contrefaçon en ligne IPM de l'OMD est devenu une véritable plate-forme de communication centrale entre les agents des douanes sur le terrain et le secteur privé, qui leur permet d'échanger des informations cruciales en temps réel afin d'intercepter les marchandises contrefaites.

L'application IPM mobile lancée récemment permet aux agents des douanes sur le terrain d'accéder à IPM via leurs dispositifs mobiles et de rechercher toutes les informations pertinentes contenues dans la base de données. Cette nouvelle version permet également d'utiliser les dispositifs mobiles pour scanner les codes-barres GS1 qui se trouvent sur des millions de produits, offrant ainsi aux agents des douanes la possibilité de parcourir la base de données de produits rapidement. En outre, le balayage des codes-barres assure une connexion automatique à tous les services d'authentification liés au produit contrôlé. Ce nouveau dispositif, baptisé "IPM Connecté", est un réseau mondial de fournisseurs de fonctionnalités de sécurité (Security Features Providers, ou SFP) connecté à l'IPM.

Avec ce réseau de plus en plus vaste de fournisseurs SFP, le nombre de titulaires de droits qui rejoignent l'IPM est en augmentation, puisque plus de 700 marques figurent actuellement dans le système et couvrent un large éventail de secteurs d'activité, allant des produits pharmaceutiques, des produits alimentaires aux articles de luxe, en passant par les pesticides et les marchandises à rotation rapide [16].

5.5 Union européenne

L'Union européenne s'est attaquée au problème de la contrefaçon en prenant un certain nombre d'initiatives, qui ont notamment consisté à établir des dispositions réglementaires applicables aux activités des autorités douanières et à élaborer une directive sur le respect des droits de propriété intellectuelle. La Commission a également lancé une consultation générale sur ce thème en publiant en octobre 1998 un Livre vert.

L'intervention des autorités douanières était définie précédemment dans le Règlement (CE) N° 3295/94 du Conseil "fixant des mesures en vue d'interdire la mise en libre pratique, l'exportation, la réexportation et le placement sous un régime suspensif des marchandises de contrefaçon et des marchandises pirates". Toutefois, ce texte a été abrogé et remplacé par le Règlement du Conseil N° 1383/2003 du 22 juillet 2003, concernant l'intervention des autorités douanières à l'égard de marchandises soupçonnées de porter atteinte à certains droits de propriété intellectuelle ainsi que les mesures à prendre à l'égard de marchandises portant atteinte à certains droits de propriété intellectuelle.

La directive 2004/48/CE relative au respect des droits de propriété intellectuelle (plus connue sous le nom de "directive IPRED") a pour objet d'harmoniser les moyens de faire respecter les droits de propriété intellectuelle dans les Etats Membres de l'UE. Cette directive s'applique à tous les types de propriété intellectuelle, tant dans les environnements physiques que dans les environnements numériques. La directive IPRED a fait l'objet de nombreuses controverses, étant donné que la proposition initiale contenait des dispositions relatives aux sanctions pénales, dispositions qui ont par la suite été supprimées, et qu'elle exigeait que des modifications soient apportées aux législations nationales pour permettre aux juridictions d'ordonner à un fournisseur de services Internet de révéler aux détenteurs d'un droit l'identité d'un client (sur la base de l'adresse du protocole Internet utilisée).

Le Conseil de l'Union européenne a adopté une Résolution sur un plan européen global de lutte contre la contrefaçon et le piratage (25 septembre 2008), qui a abouti à la création d'un Observatoire européen de la contrefaçon et du piratage. Cet Observatoire a pour mission de recueillir des données plus nombreuses sur la contrefaçon et le piratage, d'encourager une plus grande collaboration et d'échanger des renseignements sur les bonnes pratiques en matière d'application des procédures. https://oami.europa.eu/ohimportal/en/web/observatory/home.

L'UE a conclu, ou négocie activement, des accords commerciaux bilatéraux avec un grand nombre de pays, par exemple le Partenariat transatlantique de commerce et d'investissement (TTIP) avec les Etats-Unis d'Amérique. http://ec.europa.eu/trade/policy/in-focus/ttip/.

La Commission européenne a publié une communication intitulée "Commerce, croissance et propriété intellectuelle – Stratégie pour la protection et le respect des droits de propriété intellectuelle dans les pays tiers" en juillet 2014 http://ec.europa.eu/transparency/regdoc/rep/1/2014/EN/1-2014-389-EN-F1-1.Pdf, ainsi qu'un plan d'action figurant dans le document COM (2014) 392/2.

5.6 Interpol

Interpol, organisation internationale de police comptant 190 pays membres, a constitué en 2002 le Groupe d'action d'Interpol sur la criminalité liée à la propriété intellectuelle. Ce Groupe apporte un appui aux opérations menées aux niveaux régional et mondial pour la saisie de produits de contrefaçon, organise des cours de formation dans le cadre du service de formation IIPCIC (International IP Crime Investigators College) et a créé une base de données sur la criminalité internationale liée à la propriété intellectuelle.

5.7 Commission économique pour l'Europe de l'ONU (CEE-ONU)

Le Groupe de travail des politiques de coopération en matière de réglementation et de normalisation de la CEE-ONU (GT.6) a constitué un Groupe consultatif de la surveillance des marchés (connu sous le nom de Groupe "MARS"), qui a pour mission d'encourager les Etats Membres à coordonner leurs efforts pour lutter contre le phénomène des produits de contrefaçon. Ce Groupe a établi la Recommandation M. intitulée "Utilisation de la surveillance des marchés comme moyen complémentaire de protéger les consommateurs des marchandises de contrefaçon" [18].

5.8 Initiatives nationales (exemples)

5.8.1 France

Le CNAC (Comité National Anti-Contrefaçon) est le Comité national français de lutte contre la contrefaçon http://www.industrie.gouv.fr/enjeux/pi/cnac.php, tandis que l'INPI (Institut national pour la propriété industrielle) est l'institut national pour la propriété industrielle. http://www.inpi.fr/fr/connaitre-la-pi/lutte-anti-contrefacon.html. Le Ministère des finances (Ministère de l'économie et des finances) participe également à des activités de lutte contre la contrefaçon. http://www.economie.gouv.fr/signature-deux-nouvelles-chartes-lutte-contre-contrefacon-sur-internet.

5.8.2 Office de la propriété intellectuelle du Royaume-Uni

L'Office de la propriété intellectuelle du Royaume-Uni a créé en 2004 un Groupe chargé de la lutte contre la criminalité liée à la propriété intellectuelle (IP). Ce Groupe établit un rapport annuel sur la criminalité liée à la propriété intellectuelle et a également publié un outil en ligne sur la chaîne d'approvisionnement [19]. Il existe également au Royaume-Uni un Ministère de la propriété intellectuelle.

5.8.3 Agence de lutte contre la contrefaçon du Kenya

Le Parlement du Kenya a adopté en 2008 la Loi sur la lutte contre la contrefaçon (N° 13), qui interdit le commerce des produits de contrefaçon. Cette Loi a également porté création de l'Agence de lutte contre la contrefaçon [20].

5.8.4 Commission mixte Etats-Unis – Chine pour les questions économiques et commerciales

Les Etats-Unis et la Chine ont institué une Commission mixte pour les questions économiques et commerciales. Lors de sa 24ème réunion tenue en décembre 2013, le Groupe national de direction de la Chine chargé de la lutte contre les atteintes aux DPI et la fabrication et la vente de produits de contrefaçon et de produits de qualité inférieure s'est engagé à adopter un plan d'action en 2014, prévoyant une campagne de sensibilisation du public, l'élaboration de critères en matière de respect de toutes les législations et réglementations concernant la protection des DPI et des actions de répression www.commerce.gov/news/fact-sheets/2013/12/20/fact-sheet-24th-us-china-joint-commission-commerce-and-trade-fact-sheet.

6 Forums du secteur privé sur la lutte contre la contrefaçon

Les entreprises ont réagi au problème de la contrefaçon en mettant en place des forums visant à représenter leurs intérêts. Ces forums sont l'occasion de présenter des renseignements sur l'étendue du problème, de suggérer des méthodes permettant de limiter les effets de la contrefaçon et de faire pression auprès des pouvoirs publics et des organisations internationales pour qu'ils agissent afin de lutter contre la contrefaçon.

6.1 Chambre de commerce internationale (ICC)

La Chambre de commerce internationale (ICC) est l'organisation mondiale des entreprises. Elle compte parmi ses membres des milliers d'entreprises et d'associations présentes dans quelque 120 pays. Elle représente les entreprises auprès des gouvernements et des organisations intergouvernementales. La Chambre de commerce internationale a été créée en 1919. Sa Cour internationale d'arbitrage a été créée en 1923.

L'ICC a fondé en 1985 son Bureau d'enquêtes sur la contrefaçon et a lancé récemment un plan d'action des entreprises pour mettre un terme à la contrefaçon et au piratage (BASCAP).

Le Bureau d'enquêtes sur la contrefaçon de l'ICC tient à jour une base de données sur des études de cas et fournit également des services d'enquêtes.

Le BASCAP a poursuivi l'étude des conséquences économiques et sociales de la contrefaçon et du piratage entreprise par l'OCDE [4] et a créé un centre d'échange d'informations, qui fournit des renseignements par pays [21], par secteur [22] et par protection des marques [23] ainsi que des répertoires de points de contacts au niveau mondial [24].

L'ICC publie aussi une feuille de route sur la propriété intellectuelle [25].

6.2 Coalition internationale pour prévenir la contrefaçon (IACC)

L'IACC (Coalition internationale pour prévenir la contrefaçon) [26], créée en 1979, compte des membres provenant de tous les secteurs d'activité. Son objectif est de lutter contre la contrefaçon et le piratage en encourageant l'adoption de réglementations sur la lutte contre la contrefaçon.

6.3 Mobile Manufacturers Forum (MMF)

Le Mobile Manufacturers Forum tient à jour un site web (spotafakephone.com) qui donne des renseignements sur les téléphones mobiles et les batteries de contrefaçon.

6.4 Association of Service and Computer Dealers International and North American Association of Telecommunications Dealers (AscdiNatd)

L'AscdiNatd (Association des revendeurs d'ordinateurs et des prestataires de services du monde entier et association nord-américaine des revendeurs de télécommunications) a conçu un programme de lutte contre la contrefaçon qui prévoit l'adoption par les entreprises membres de mesures de lutte contre la contrefaçon et comprend des ressources d'information sur la contrefaçon, notamment des renseignements fournis par HP et Cisco [27].

6.5 Alliance for Gray Market and Counterfeit Abatement (AGMA)

L'AGMA (Alliance pour la lutte contre le marché gris et la contrefaçon), créée en 2001 par 3Com, Cisco Systems, Hewlett-Packard, Nortel et Xerox, a pour mission de lutter contre le commerce de produits de contrefaçon de haute technologie.

6.6 Groupe de travail sur la lutte contre la contrefaçon de la British Electrotechnical and Allied Manufacturers Association (BEAMA)

La BEAMA offre une base de compétences spécialisées et un forum destiné au secteur de l'électrotechnique du Royaume-Uni et de toute l'Europe. Cette Association représente plus de 300 entreprises manufacturières du secteur de l'électrotechnique et est très influente sur la scène internationale ainsi qu'au Royaume-Uni, dans le domaine des politiques générales, de la normalisation et des politiques commerciales.

Le Groupe de travail de la BEAMA chargé de la lutte contre la contrefaçon (ACWG) a été constitué en 2000. Il a pour mission de prendre des mesures contre les contrefacteurs qui fabriquent des produits pour installations électriques de contrefaçon et les négociants qui les distribuent sur de nombreux marchés internationaux, notamment en Europe, au Moyen-Orient et en Afrique. Outre les membres de la BEAMA, ce Groupe de travail comprend un grand nombre d'associations professionnelles de premier plan issues des secteurs de l'installation, de la distribution, des tests et de la certification et de l'application des lois. Son travail de pionnier lui vaut d'être reconnue au plan mondial et l'Association bénéficie à ce titre de la coopération d'associations professionnelles et d'organes chargés de l'application des lois du monde entier.

Il a été créé une base de données des contrefacteurs à l'usage du secteur de l'installation électrique, qui est transmise aux autorités du monde entier afin qu'elles puissent exercer un suivi sur les marchés locaux.

Les activités menées par le Groupe de travail sont rendues publiques dans des articles de revues spécialisées, à l'occasion de présentations et de la participation à des conférences ainsi que par le biais de guides et d'affiches destinées à sensibiliser l'opinion à ce phénomène de plus en plus préoccupant, qui risque de compromettre la sécurité des consommateurs et l'intégrité commerciale.

Ce Groupe de travail est chargé de gérer des projets de lutte contre la contrefaçon, de recueillir et de diffuser des renseignements sur les questions liées aux DPI et de répondre au nom de l'Association, aux demandes émanant des gouvernements, notamment. Il fournit également des avis et des informations aux entreprises ou associations qui rencontrent des problèmes en matière de DPI.

La BEAMA mène actuellement des projets en Chine, aux EAU, au Royaume-Uni, au Nigéria et en Irak et met également en place des programmes sur l'Internet ainsi que des programmes de surveillance portuaire de grande ampleur.

Au Royaume-Uni, la BEAMA collabore avec bon nombre des principaux organismes professionnels, pour sensibiliser l'opinion et lutter contre les produits de contrefaçon et les produits non conformes – le portail spécialisé www.counterfeit-kills.co.uk a été créé spécialement à cette fin.

6.7 UKEA (United Kingdom Electronics Alliance)

L'UKEA est un consortium d'associations professionnelles du Royaume-Uni représentant le secteur de l'électronique, qui a pour ambition de coordonner l'examen des problèmes que rencontre le secteur et de communiquer avec les pouvoirs publics. L'UKEA a mis sur pied un Forum sur la lutte contre la contrefaçon [28], qui publie des renseignements sur le problème des composants électroniques de contrefaçon, sur les fournisseurs de solutions possibles et sur les bonnes pratiques en la matière.

6.8 Anti-Counterfeiting Group (ACG)

L'ACG est une association professionnelle du Royaume-Uni créée en 1980, dont les membres proviennent essentiellement du secteur de l'automobile. Elle représente toutefois aujourd'hui la plupart des secteurs d'activité.

6.9 UNIFAB – *Union des Fabricants*

L'*Union des Fabricants* est une organisation française spécialisée dans la lutte contre la contrefaçon, qui s'efforce de sensibiliser l'opinion à ce problème (elle a par exemple ouvert un Musée de la contrefaçon, entre autres activités), en fournissant des informations aux entreprises et en menant des actions de persuasion. http://www.unifab.com/en/.

6.10 International Electronics Manufacturing Initiative (iNEMI)

L'iNEMI a défini un projet intitulé "Composants de contrefaçon – Méthodes d'évaluation et élaboration de valeurs de mesure". http://www.inemi.org/project-page/counterfeit-components-assessment-methodology-and-metric-development.

7 Mesures de lutte contre la contrefaçon d'équipements

7.1 Introduction

Il est possible de lutter contre la contrefaçon d'équipements en apposant des marques sur les produits, afin de pouvoir les authentifier en contrôlant rigoureusement leur cycle de vie.
Les étiquettes difficiles à falsifier peuvent être apposées sur les produits et des numéros de séries peuvent leur être assignés, afin de certifier que l'article est authentique (moyennant l'accès à une base de données par exemple).

Des identifiants uniques peuvent être attribués aux différents articles. Comme exemple de système utilisé pour lutter contre la contrefaçon, on peut citer l'application mPedigree, qui sert à lutter contre la contrefaçon de produits pharmaceutiques en Afrique. Ce système permet aux patients de vérifier l'authenticité des médicaments, ou de voir si ceux-ci sont contrefaits et potentiellement dangereux, en envoyant un SMS (gratuit) à un registre de produits pharmaceutiques.

Les chaînes d'approvisionnement, voire les cycles de vie complets des produits, doivent faire l'objet de contrôles rigoureux et, le cas échéant, de tests, d'évaluation et de certification, pour garantir la sécurité ainsi qu'une qualité satisfaisante du produit. De plus, il faut donner aux agents des douanes les outils nécessaires pour leur permettre d'identifier les produits de contrefaçon; à cet égard, il est possible d'avoir recours à des mécanismes de surveillance du marché.

Les identifiants peuvent être placés sur un objet en clair ou être codés sur une "étiquette d'identification" (ID), telle qu'un code-barres, une étiquette d'identification par radiofréquences (RFID), une carte à puce ou une étiquette infrarouge, afin de permettre leur lecture automatique. On distingue trois niveaux dans l'identification d'un objet. Il existe tout d'abord un niveau d'identification proprement dit, au cours duquel les objets sont identifiés de manière univoque, par exemple au moyen d'un code produit électronique (EPC). Le deuxième niveau est un niveau de codage, étant donné que les identifiants proprement dits peuvent être codés selon différents formats; enfin, il existe une réalisation physique, au cours de laquelle l'identité codée est écrite sur une étiquette RFID, par exemple.

Pour faire en sorte que les identifiants soient uniques au niveau mondial pour des applications déterminées, il faut les gérer de manière organisée, en prévoyant une procédure d'attribution. Ainsi, l'Association GSM (GSMA) gère les identités internationales d'équipements mobiles (IMEI) pour le système mondial de communications mobiles (GSM), le système de télécommunications mobiles universelles (UMTS) et les dispositifs LTE (évolution à long terme). L'Association des industries de télécommunication (TIA) gère les identifiants d'équipement mobile; (MEID) pour les dispositifs à accès multiple par répartition en code (AMRC) et GS1 gère les identificateurs de code-barres.
L'ISO gère plusieurs domaines d'identification et fait également office d'autorité de premier niveau chargée d'intégrer les systèmes d'identification d'autres organisations telles que GS1.

Autre exemple: celui du marquage des équipements pour indiquer que leur commercialisation dans un pays a été approuvée. Ainsi, Anatel exige que les chargeurs et les batteries de téléphones mobiles portent un label sécurisé défini conformément à la Résolution 481/2007[2]. Voir la Figure 1.

Figure 1 – Exemple de label sécurisé exigé par Anatel, défini conformément à la Résolution 481/2007

Cette méthode est depuis longtemps utilisée par les équipementiers de télécommunication et a été mise en oeuvre avec succès par certains pays ou certaines régions[3] (FCC[4], Anatel[5] et l'UE[6], par exemple).

Les agents des douanes doivent être à même d'identifier les produits de contrefaçon ainsi que les mécanismes de surveillance du marché et les autres mesures d'application des lois susceptibles d'être utilisés. En outre, les importateurs ayant la réputation de ne pas respecter les restrictions à l'importation peuvent être identifiés et inscrits sur une liste spéciale. Lorsque des envois d'équipements TIC sont importés par des importateurs peu scrupuleux, il est possible d'informer les autorités réglementaires, afin qu'une décision de procéder à des inspections puisse être prise et que des mesures d'application de la loi puissent être mises en oeuvre. Voir la Figure 2.

---

2 https://translate.google.com/translate?sl=pt&tl=en&js=y&prev=_t&hl=fr&ie=UTF-8&u=legislacao.anatel.gov.br%2Fresolu%C3%A7%C3%B5es%2F2007%2F192-resolu%C3%A7%C3%A3o-481&edit-text=

3 Dans le cadre d'un système d'évaluation de la conformité, qui nécessitera peut-être une certification, une déclaration de conformité ou le recours à des accords de reconnaissance mutuelle (MRA).

4 https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=30744&switch=P.

5 https://grandeseventos.anatel.gov.br/en/frequently-asked-questions.html#pergunta1.

6 http://exporthelp.europa.eu/thdapp/display.htm?page=rt%2frt_TechnicalRequirements.html&docType=main&languageId=en.

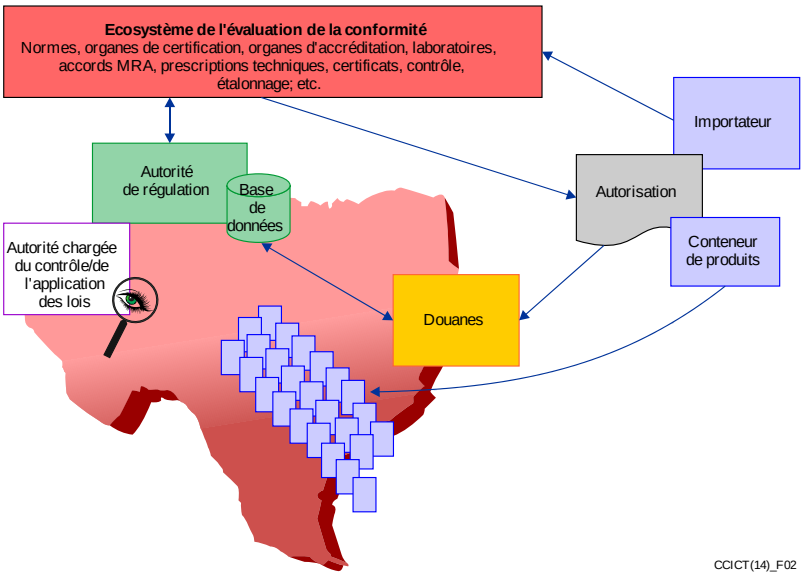


Figure 2 – Ecosystème de l'évaluation de la conformité

Il convient de noter qu'il arrive que des produits de contrefaçon soient en fait conformes à des prescriptions bien définies, soient capables d'interfonctionner avec des produits authentiques et satisfassent dès lors aux conditions des essais de conformité et d'interopérabilité. En pareils cas, il faudra peut-être que le titulaire de la marque procède à l'évaluation du produit, afin d'identifier avec précision les produits de contrefaçon et de pouvoir les distinguer des produits authentiques.

Le secteur des TIC est un secteur dynamique caractérisé par la présence d'un grand nombre de concurrents internationaux qui encouragent en permanence l'innovation. Cette situation est certes souhaitable, mais parallèlement, il peut y avoir sur le marché des fabricants ou des fournisseurs qui ne se sont pas toujours prêts à respecter les règles établies au niveau international, régional ou national.

Le problème de l'asymétrie de l'information est plus prononcé dans les pays en développement, où le développement des technologies est limité, voire inexistant, et où il existe très peu de procédures d'évaluation de la conformité, voire aucune. Les problèmes qui se posent généralement lors de la gestion d'un système d'évaluation de la conformité sont l'absence d'informations fiables et permettant une traçabilité, notamment dans les cas suivants: i) identification de l'origine des produits ou de la personne juridiquement responsable des produits; ii) emplacement des installations de production; iii) organismes de certification; et iv) laboratoires agréés disposant d'un certificat d'accréditation en bonne et due forme. Il arrive dans certains cas que des importateurs sans aucune connaissance ou capacité technique pour fournir une assistance représentent des entreprises étrangères ayant externalisé leurs unités techniques et de production à l'étranger (dans le cadre de plans d'externalisation, par exemple). Ces manières de procéder, même si elles débouchent parfois sur des économies au niveau des processus de production, nuisent cependant à la qualité et à la fiabilité de la production des équipements de télécommunication/TIC.

On peut même affirmer que les intérêts particuliers, l'appât du gain, la demande des consommateurs, l'absence de normes ou l'application peu rigoureuse des règles ont pour conséquence une qualité médiocre des équipements. Dans certains cas, pour une même marque ou un même modèle, étant donné qu'il n'existe aucun processus de conformité adapté sur un marché cible donné, le produit est assemblé et vendu avec des composants électroniques différents, certains de bonne qualité, d'autres dont la qualité laisse à désirer, puis est envoyé vers des destinations peu

regardantes sur la qualité. Le phénomène dit de "tropicalização" (mot portugais pour "tropicalisation") vient immédiatement à l'esprit quand on pense à l'altération volontaire d'équipements destinés à être vendus au sud de l'équateur. Voir la Figure 3.

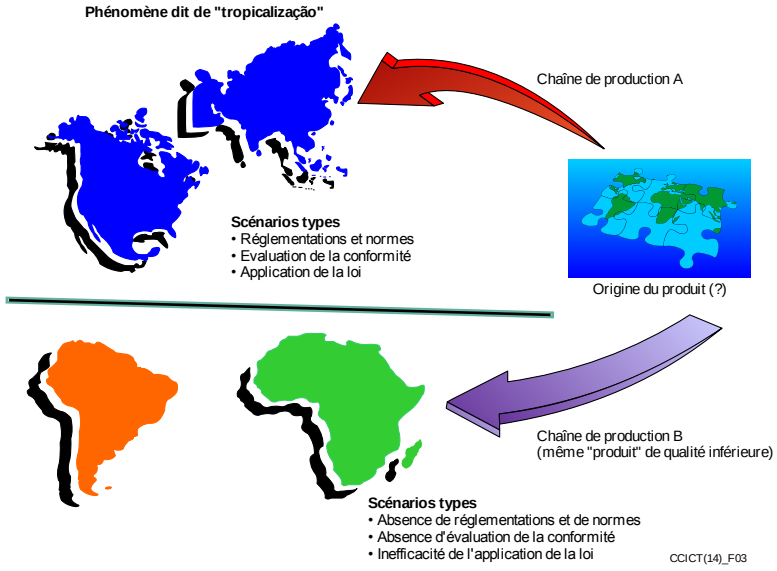


Figure 3 – Procédure dite de "tropicalização" (mot portugais pour "tropicalisation")

7.2 Utilisation abusive d'identifiants et de logos d'homologation

Tous les identifiants créés par des fabricants réels de produits peuvent faire l'objet d'une utilisation abusive par des contrefacteurs, qui cherchent à tromper les consommateurs et les autorités en leur faisant croire que leur produit est authentique. Ce problème, qui ne concerne pas seulement les TIC, se pose fréquemment dans de nombreux secteurs d'activité. Il faut garder à l'esprit que les mécanismes d'identification et les dispositifs de sécurité qui s'y rapportent deviendront une cible pour les contrefacteurs et les cyberdélinquants. Les logos d'homologation et les icônes ainsi que les identifiants électroniques sont souvent détournés à dessein, afin d'éviter les contrôles douaniers et les vérifications effectuées par les services de répression aux frontières. Cette situation est source de problèmes pratiques pour les fabricants, les consommateurs, les agents des douanes et les services chargés de l'application de la loi, qui éprouvent des difficultés à distinguer les fausses marques d'identification des marques authentiques, avant même d'avoir contrôlé le produit lui-même.

7.3 Identité internationale d'équipement mobile (IMEI)

Comme nous l'avons déjà indiqué, les téléphones mobiles constituent une cible de choix pour les contrefacteurs. En guise de riposte, le Mobile Manufacturers Forum (MMF) a créé un site web donnant des renseignements aux consommateurs sur la manière de reconnaître des téléphones et des batteries de contrefaçon. http://spotafakephone.com. Il y est indiqué que le consommateur devrait se familiariser avec les caractéristiques, les fonctionnalités, la disponibilité et le prix des articles authentiques et vérifier également le numéro d'identité internationale d'équipement mobile (IMEI). Le numéro IMEI est un identifiant unique pour chaque téléphone mobile. Bien souvent, les produits de contrefaçon ne portent pas de numéro IMEI ou ont un faux numéro. Pour les fabricants, les

opérateurs de réseaux et les autorités, le problème est que les contrefacteurs ont adapté leurs méthodes de fabrication et dérobent parfois des séries de numéros autorisées auprès des fabricants en place, dans le cadre de leur stratégie de contrefaçon. Cette méthode peut notamment être utilisée pour échapper aux systèmes de contrôle des numéros IMEI.

L'attribution des numéros IMEI est gérée par l'Association GSMA, afin de garantir que chaque numéro soit unique. Le système d'attribution est hiérarchique: la GSMA assigne des identifiants à deux chiffres à des Entités de notification, qui attribuent ensuite le numéro IMEI ainsi que le numéro de série de l'équipement. Les Entités de notification actuellement autorisées à attribuer des numéros IMEI sont les suivantes: CTIA – The Wireless Association, BABT (British Approvals Board for Telecommunications, Royaume-Uni), TAF (Telecommunications Terminal Testing and Approval Forum, Chine), et la MSAI (Mobile Standards Alliance, Inde).

Le format des numéros IMEI valables à compter du 1er janvier 2003 est indiqué sur la Figure 4 ci-après [37]:

Code d'attribution type (TAC)	Numéro de série	Somme de contrôle
NNXXXX YY	ZZZZZZ	A

TAC	Code d'attribution type, précédemment connu sous l'appellation "code d'homologation".
NN	Identifiant de l'Entité de notification.
XXXXYY	Identifiant du type d'équipement mobile (ME) défini par l'Entité de notification.
ZZZZZZ	Attribué par l'Entité de notification, mais assigné pour chaque équipement ME par le fabricant.
A	Somme de contrôle, définie en fonction de tous les autres chiffres IMEI.

Figure 4 – Format des numéros IMEI

La GSMA enregistre d'autres renseignements, par exemple le nom du fabricant et le numéro de modèle, ainsi que les capacités techniques, par exemple les bandes de fréquences prises en charge et la classe de puissance, pour chaque dispositif identifié par son numéro IMEI.

La GSMA tient à jour la base de données IMEI (Base de données IMEI) [38], plus connue auparavant sous l'appellation "CEIR" (Registre d'identification des équipements centraux). La base de données IMEI contient une "liste blanche" des équipements considérés comme pouvant être utilisés dans le monde entier, et une "liste noire" de numéros IMEI se rapportant aux dispositifs qui ne sont pas considérés comme pouvant être utilisés parce qu'ils ont été perdus ou volés ou parce qu'ils sont défectueux et mettent en péril l'intégrité du réseau. Il convient de noter que la liste blanche de la base de données IMEI est une liste de codes TAC plutôt qu'une liste complète de numéros IMEI et que les données sont mises gratuitement à la disposition des parties remplissant les conditions requises, notamment, les régulateurs nationaux, les organismes chargés de l'application de la loi et les services de douane. Outre la base de données des numéros IMEI, les différents opérateurs de réseaux peuvent mettre en oeuvre leurs propres registres d'identification des équipements (EIR), dans lesquels ils peuvent télécharger la "liste blanche" ce qui permet aux opérateurs de contrôler les dispositifs qui peuvent accéder à leurs réseaux. http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database/.

La base de données des numéros IMEI a principalement pour but de permettre aux opérateurs d'identifier les dispositifs, ainsi que leurs caractéristiques, qui sont utilisés sur leurs réseaux et de bloquer les combinés volés. Cette base de données peut également servir à détecter des dispositifs de contrefaçon, ce qui contribue à empêcher le blanchiment fondé sur ces dispositifs, à décourager la criminalité et à faciliter les poursuites.

Toutefois, la mise en oeuvre des numéros IMEI a posé un certain nombre de problèmes. On a par exemple signalé des cas dans lesquels des équipements étaient dépourvus de numéros IMEI ou comportaient un numéro IMEI exclusivement constitué de zéros, des numéros IMEI en double ou encore des numéros IMEI attribués par des organismes non autorisés. Certains de ces dispositifs comportant des numéros IMEI non valables ou non uniques sont des produits de contrefaçon, mais il peut aussi s'agir de produits authentiques, qui ne sont toutefois pas conformes à la procédure d'attribution des numéros IMEI de la GSMA, en raison de malentendus de la part des fabricants. On estime ainsi à 30 millions le nombre de combinés sans numéro IMEI en Inde, de sorte que la MSAI a été autorisée par la GSMA à proposer un programme d'amnistie temporaire prévoyant "l'implantation" de numéros IMEI authentiques (programme d'implantation de numéros IMEI authentiques (GII)), afin de permettre l'identification de manière univoque de chaque dispositif.

Pour illustrer le cas des numéros IMEI en double, on peut citer l'exemple de l'Australie, où l'on a constaté que 6 500 combinés portaient le numéro IMEI 135790246811220. Quant aux numéros IMEI non enregistrés, un opérateur de réseau de l'Ouganda a signalé que le nombre de codes TAC sur son réseau qui n'étaient pas enregistrés dans la base de données des numéros IMEI était supérieur à celui des numéros attribués par la GSMA et enregistrés dans la base de données IMEI.

Autant d'arguments qui militent en faveur de l'idée selon laquelle il faut rendre obligatoire l'utilisation des numéros IMEI et attribuer ces numéros conformément à la procédure établie par la GSMA. La base de données IMEI constitue un instrument permettant de détecter les dispositifs mobiles de contrefaçon. A cet égard, on peut citer l'exemple du Kenya, qui a interdit dès la fin septembre 2012 l'accès aux téléphones mobiles comportant des numéros IMEI non valables, le nombre d'abonnés utilisant de faux téléphones mobiles ayant été estimé à 2,3 millions. On trouvera dans l'Annexe A de plus amples renseignements sur ces exemples ainsi que sur les autres cas dans lesquels des numéros IMEI ont servi de base à l'identification de téléphones mobiles de contrefaçon. Etant donné que plusieurs initiatives prises au niveau national afin de lutter contre la contrefaçon des appareils mobiles reposent sur l'utilisation de numéros IMEI, il est indispensable que la procédure d'attribution de ces numéros et la base de données IMEI soient sécurisées et fiables et que les numéros IMEI soient codés en toute sécurité dans ces appareils.

On pourrait par exemple faire obligation aux opérateurs de bloquer les dispositifs comportant des numéros IMEI en double ou non valables, étant donné que ces dispositifs doivent être authentifiés sur un réseau afin de pouvoir fonctionner. Le blocage de ces dispositifs lors de la première connexion constitue probablement l'outil le plus efficace pour remédier pour l'heure à ce problème.

Le blocage des numéros IMEI est cependant assujetti à plusieurs contraintes. En premier lieu, la GSMA ne tient pas à jour une liste blanche complète des numéros IMEI, mais uniquement une liste blanche des codes TAC. Deuxièmement, les numéros IMEI provenant de dispositifs autorisés ont été clonés sur des dispositifs de contrefaçon ou de qualité inférieure aux normes, ce qui complique encore le processus de blocage. En définitive, toute solution de blocage doit empêcher ou interdire la copie d'autres numéros clonés dans les dispositifs en question.

Il existe cependant des solutions sur le marché, en dépit des problèmes que pose le blocage. Parallèlement, il est important d'éviter une multiplicité de solutions nationales uniques, qui ne feront que déplacer le problème au-delà des frontières nationales. Etant donné que les numéros IMEI sont attribués par la GSMA et que la base de données des numéros IMEI est tenue à jour par cette Association, il paraît logique d'associer la GSMA d'une manière ou d'une autre aux initiatives nationales, afin d'utiliser toutes les listes disponibles et les autres mesures techniques existantes.

Toutefois, étant donné que d'après les estimations, le nombre de dispositifs de contrefaçon est gigantesque, se contenter de bloquer des terminaux opérationnels aurait des conséquences aussi importantes qu'imprévues pour les réseaux et les utilisateurs finals, conséquences que l'on ne saurait ignorer.

A cet égard, il est important de tenir compte du fait que dans les pays en développement connaissant des conditions socio-économiques défavorables, les téléphones mobiles constituent la principale passerelle de communication et le principal moyen de participer à la société de l'information[7]. Malheureusement, les dispositifs utilisés à cette fin sont bien souvent des dispositifs de contrefaçon bon marché.

C'est pourquoi la société tout entière doit être préparée à faire face à cette évolution. Il faut étudier, examiner et planifier les solutions les mieux adaptées. Il faut par exemple expliquer clairement aux consommateurs les raisons pour lesquelles les dispositifs de contrefaçon ne doivent pas être autorisés (risques pour la sécurité, qualité de service inférieure et augmentation en conséquence du nombre de réclamations, risques de brouillages et atteintes aux DPI, etc.).

Dans cette perspective, si les régulateurs et les gouvernements choisissent de mettre en place des mesures de blocage des terminaux, il est important d'adopter des politiques de transition, en ne bloquant par exemple dans un premier temps que les nouveaux terminaux et en autorisant les dispositifs en service sur le réseau à continuer de fonctionner, à charge pour les utilisateurs de passer à terme à l'utilisation de terminaux authentiques, la durée de vie d'un terminal mobile étant estimée à 18 mois[8].

7.4 Identifiants uniques

Les codes produit électroniques (EPC) ont été mis au point à l'origine par l'Auto-ID Centre du Massachusetts Institute of Technology créé en 1999 et sont aujourd'hui gérés par EPCglobal, filiale de GS1 qui a défini les spécifications applicables aux systèmes mondiaux de chaîne d'approvisionnement couramment utilisées de nos jours. L'Organisation internationale de normalisation (ISO) et l'Ubiquitous ID Centre (Japon) ont également défini des identifiants pour un certain nombre d'applications.

GS1 définit neuf "clés d'identification" pour l'identification des articles, des lieux, des unités d'expédition, des actifs, des services, des types de document, des envois et des expéditions, à savoir:

- GTIN – code article international
- GLN – code lieu-fonction international
- SSCC – code de colis de série
- GRAI – code d'identification des supports réutilisables

---

[7] Initiative de l'UIT sur le mobile au service du développement: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Pages/default.aspx.

[8] http://www.epa.gov/osw/education/pdfs/life-cell.pdf: "Les téléphones cellulaires ne sont en moyenne utilisés que pendant 18 mois avant d'être remplacés, alors qu'ils peuvent fonctionner pendant beaucoup plus longtemps".

- GIAI – code international d'identification des actifs
- GSRN – code international d'identification d'une relation de service
- GDTI – code international d'identification d'un type de document
- GSIN – code international d'identification d'une expédition
- GINC – code international d'identification d'un groupement d'unités logistiques

Le code GTIN sert à identifier des catégories d'objets, alors que les codes GLN, SSCC, GIAI et GSRN identifient des objets en tant que tels; les codes GRAI et GDTI peuvent être utilisés pour identifier soit des catégories d'objets, soit des articles en tant que tels, en fonction de l'absence ou de la présence d'un numéro de série. Les codes GINC et GSIN identifient des groupements logiques plutôt que des objets physiques. Ces clés d'identification sont destinées à la réalisation au moyen de codes à barres. Il existe une correspondance entre ces codes et les codes EPC définis par EPCglobal en vue de leur utilisation avec des étiquettes RFID. Il y a extension du code GTIN dans le système EPC moyennant l'adjonction d'un numéro de série, afin d'identifier un objet de manière univoque. Les autres clés utilisées pour identifier des objets en tant que tels ont un équivalent EPC direct. Les codes EPC suivants sont définis [41]:

- Identifiant général (GID)
  - urn:epc:id:gid:*ManagerNumber.ObjectClass.SerialNumber*
- Numéro international d'identification commerciale de série (SGTIN)
  - urn:epc:id:sgtin:*CompanyPrefix.ItemReference.SerialNumber*
- Code de colis de série (SSCC)
  - urn:epc:id:sscc:*CompanyPrefix.SerialReference*
- Numéro de série international de localisation avec ou sans extension (SGLN)
  - urn:epc:id:sgln:*CompanyPrefix.LocationReference.Extension*
- Code d'identification des supports réutilisables (GRAI)
  - urn:epc:id:grai:*CompanyPrefix.AssetType.SerialNumber*
- Code international d'identification des actifs (GIAI)
  - urn:epc:id:giai:*CompanyPrefix.IndividulAssetReference*
- Code international d'identification d'un type de document (GDTI)
  - urn:epc:id:gdti:*CompanyPrefix.DocumentType.SerialNumber*
- Code international d'identification d'une relation de service (GSRN)
  - urn:epc:id:gsrn:*CompanyPrefix.ServiceReference*
- Département de la Défense des Etats-Unis (DoD)
  - urn:epc:id:usdod:*CAGEOrDODAAC.SerialNumber*
- Code d'identification aérospatiale et défense (ADI)
  - urn:epc:id:adi:*CAGEOrDODAAC.OriginalPartNumber.Serial*

La norme ISO/IEC 15459 [42] définit des identifiants uniques pour la traçabilité de la chaîne d'approvisionnement, qui peuvent être représentés dans des supports d'identification et de captage de données automatiques (AIDC) tels que les codes à barres et les étiquettes RFID.

Les Parties 1, 4, 5, 6 et 8 de la norme ISO/IEC 15459 définissent la chaîne unique de caractères permettant d'identifier respectivement des unités de transport, des articles individuels, des unités de transport réutilisables, des groupements de produits et des unités de transport. Dans chaque cas, l'identifiant unique est structuré en classes, afin de faciliter la gestion efficace des identifiants pour cette classe d'objets.

La Partie 2 indique les règles de procédure régissant l'attribution d'identifiants uniques pour les applications de gestion d'articles et décrit les obligations incombant à l'organisme d'enregistrement et aux entités émettrices. Ces procédures ne s'appliquent pas aux articles pour lesquels l'ISO a déjà désigné des autorités de mise à jour et des organismes d'enregistrement pour la fourniture de systèmes d'identification. En conséquence, ces procédures ne s'appliquent pas:

- aux conteneurs pour le transport de marchandises, étant donné que leur codage unique est défini dans la norme ISO 6346 [43];
- aux véhicules routiers, étant donné que leur identification unique est définie dans la norme ISO 3779 [44];
- aux autoradios, étant donné que leur identification unique est définie dans la norme ISO 10486 [45]; et
- aux systèmes ISBN [46] et ISSN [47].

La Partie 3 décrit les règles communes applicables aux identifiants uniques pour la gestion des articles qui sont nécessaires pour garantir une parfaite compatibilité entre différentes classes d'identifiants uniques.

Le Comité technique 246 de l'ISO est chargé d'élaborer des normes sur les dispositifs anti-contrefaçon. A l'heure actuelle, ce Comité met au point une norme sur les critères de qualité de fonctionnement applicables aux solutions d'authentification permettant de lutter contre la production de produits de contrefaçon [48].

Outre l'ISO et EPCglobal, le Centre japonais Ubiquitous ID Centre a défini un identifiant générique appelé "ucode" [49], qui vise non seulement à identifier des objets physiques, mais peut aussi servir à identifier des lieux et des informations numériques (voir la Figure 5). Les "ucodes" de base ont une longueur de 128 bits (mais peuvent être étendus par multiples de 128 bits) et peuvent intégrer d'autres identifiants, tels que des numéros ISBN, des adresses fondées sur le protocole Internet (IP) ou des numéros de téléphone UIT-T E.164 [76]. L'ucode est en substance un numéro auquel il faut assigner une signification dans une base de données relationnelle. Tout individu ou toute organisation peut obtenir des ucodes auprès de l'Ubiquitous ID Centre, qui fait office d'organisme d'enregistrement pour ces numéros.

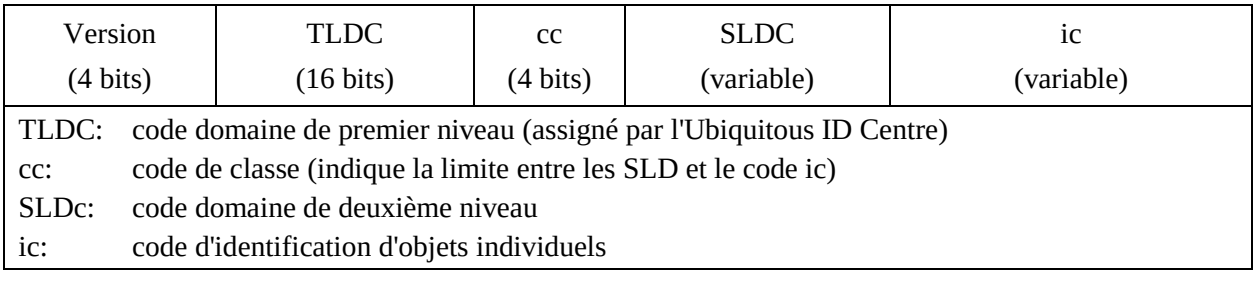


Figure 5 – Format de l'ucode

L'UIT-T mène actuellement des travaux sur les systèmes d'accès aux informations multimédias déclenchés par l'identification à base d'étiquettes. Dans le cadre de ces travaux, une description des différents systèmes d'identification susceptibles d'être utilisés pour une telle identification est en cours d'élaboration. L'Ubiquitous ID Centre a soumis son système ucode, selon lequel un identificateur d'objet (OID) enregistré sous la branche {joint-iso-itu-t(2) tag-based(27)} serait assigné à l'ucode, conformément à la Recommandation UIT-T X.668 [50]. On assigne au système d'identification unique de l'ISO/CEI décrit précédemment un identificateur d'objet sous la branche {iso(1)} de l'arborescence de l'identificateur d'objet. En conséquence, on assigne aux systèmes d'identification de l'ISO/CEI (y compris EPCglobal) et de l'Ubiquitous ID Centre des identificateurs d'objet soit sous la branche {**iso**} (ISO et EPCglobal), soit sous la branche {**joint-iso-itu-t**} (Ubiquitous ID Centre), ce qui permet la coexistence des divers systèmes d'identification ayant différents organismes d'enregistrement. En ce qui concerne les étiquettes RFID, l'identificateur d'objet (OID) et l'identifiant (ID) seraient codés comme indiqué dans la norme ISO/CEI 15962 [77].

NOTE – Le terme "objet", dans "identificateur d'objet", ne s'entend pas ici d'une "chose" en général, mais est plutôt utilisé au sens où il est défini dans la norme ISO/CEI 15961 [78] à savoir: "information, définition ou spécification bien définie, nécessitant un nom afin de l'identifier dans une instance de communication". Un identificateur d'objet identifie sans ambiguïté un tel objet. Les identificateurs d'objet sont organisés de manière hiérarchique avec les racines de l'arborescence ou les "arcs" sommitaux indiquant l'organisation qui est responsable de la définition de l'information. Les arcs sommitaux représentent l'UIT-T, l'ISO et Joint ISO – UIT-T. On leur attribue respectivement les valeurs numériques 0,1 et 2. On attribue la valeur numérique 27 à l'arc "basé sur des étiquettes" dans l'arborescence Joint ISO – UIT-T.

Les données associées à un objet peuvent être stockées sur une étiquette avec l'identifiant, si l'étiquette possède suffisamment de mémoire. Cependant, une autre façon possible de trouver les renseignements associés à un identifiant consiste à utiliser un mécanisme de résolution des identifiants.

Une très grande diversité de services et d'applications peuvent être envisagées pour les RFID, dès lors qu'il devient possible de fournir des informations associées à un identifiant d'étiquette sous différentes formes (texte, son ou image). Par exemple, dans un musée, un identifiant sur une étiquette jointe à un tableau pourrait servir à fournir des informations complémentaires sur le tableau en question et l'artiste. Dans une épicerie, un identifiant figurant sur l'emballage d'un produit alimentaire pourrait permettre de vérifier que l'aliment en question est propre à la consommation et qu'il ne fait pas partie d'un lot qui a été détecté comme étant contaminé d'une manière ou d'une autre. D'autres domaines dans lesquels il pourrait être utile de disposer d'un accès à des informations déclenché par un identifiant sont les médicaments et les produits pharmaceutiques, l'agriculture, les bibliothèques, le commerce de détail et la gestion de la chaîne d'approvisionnement. Ces mécanismes pourraient également être utilisés pour lutter contre la contrefaçon. Un certain nombre de services qui pourraient être fondés sur l'utilisation d'informations associées à des objets étiquetés ainsi que les spécifications de ces services sont présentés dans la Recommandation UIT-T F.771 [55].

Un modèle permettant d'accéder aux informations associées à un objet étiqueté est décrit dans la Recommandation UIT-T H.621 (52) (voir la Figure 6). Dans ce modèle, une fonction de découverte d'informations multimédias peut envoyer l'identifiant obtenu à partir d'un lecteur d'étiquette d'identification à une fonction de résolution d'identification, ce qui permet d'obtenir un pointeur (par exemple une adresse URL (localisateur uniforme de ressource)) vers le gestionnaire d'informations multimédias approprié. De ce fait, il devient possible d'accéder aux informations associées à l'étiquette d'identification. Etant donné qu'il devrait y avoir un très grand nombre d'identifiants, la fonction de résolution d'identification sera vraisemblablement répartie dans une structure arborescente.

Cette fonction de résolution d'identification pourrait reposer sur l'utilisation du système de noms de domaine (DNS) Internet utilisé pour fournir l'adresse IP correspondant à un localisateur uniforme de ressource (URL). Le service de nommage d'objets (ONS) décrit par EPCglobal utilise des mécanismes DNS pour trouver des renseignements associés à des codes produits électroniques.

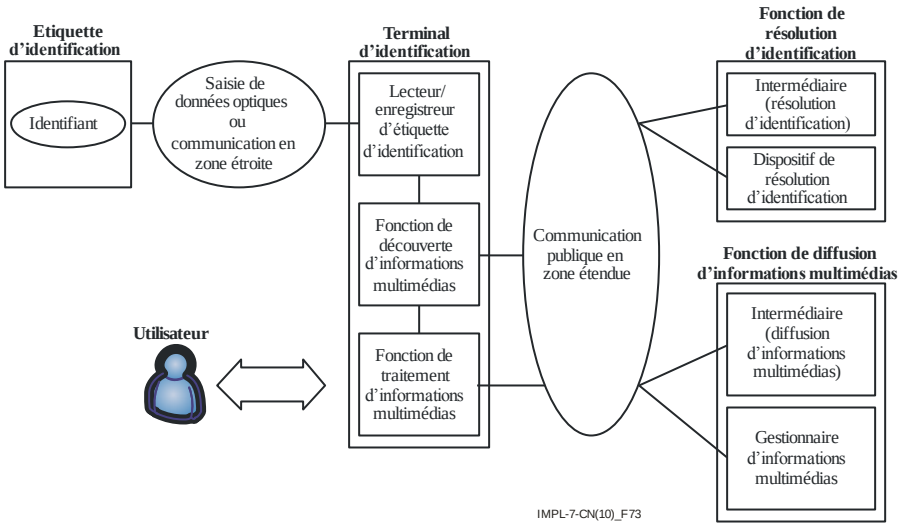


Figure 6 – Architecture fonctionnelle pour l'accès à des informations multimédias déclenché par une identification basée sur une étiquette (Recommandation UIT-T H.621)

En outre, la Recommandation UIT-T X.1255 [79] https://www.itu.int/rec/T-REC-X.1255-201309-I/en établit un cadre pour la découverte des informations relatives à la gestion d'identité qui est reconnu dans la Résolution de la Conférence de plénipotentiaires de l'UIT sur la lutte contre la contrefaçon de dispositifs de télécommunications fondés sur les technologies de l'information et de la communication.

7.5 Identification et captage de données automatiques (AIDC)

7.5.1 Codes-barres

Les codes-barres sont souvent utilisés pour identifier des produits. Ils peuvent prendre différentes formes, des codes produits universels (CUP), bien connus dans les supermarchés, aux codes-barres à matrice 2D. Ces codes sont faciles à falsifier et à copier pour les contrefacteurs.

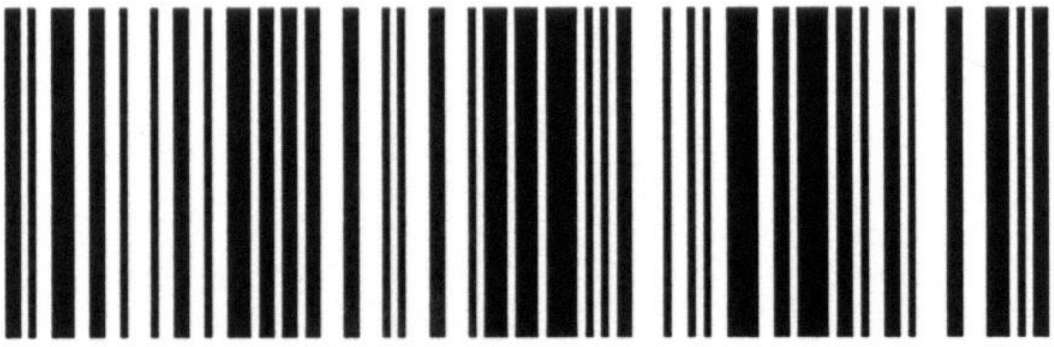


Figure 7 – Exemples de codes-barres linéaires

Pour des exemples de codes-barres linéaires, voir la Figure 7:

UPC ISO/CEI 15420 [80]

Code-barres 39 ISO/CEI 16388 [81]

Code-barres 128 ISO/CEI 15417 [82]

Figure 8 – Exemples de codes-barres matriciels (2D ou bi-dimensionnels)

Pour des exemples de codes-barres matriciels (2D ou bi-dimensionnels), voir la Figure 8:

Codablock F ISO/CEI 15417+

PDF 417 ISO/CEI 15438 [83]

Maxicode ISO/CEI 16023 [84]

Code QR ISO/CEI 18004 [85]

Matrice de données ISO/CEI 16022 [86]

Les codes-barres peuvent être utilisées pour coder un numéro de série. Par exemple, DIN 66401 [87] définit une marque d'identification unique (UIM) comprenant un symbole de matrice (ISO/CEI 16022 ou ISO/CEI 18004) et un identificateur de données unique (conformément à la norme ANSI MH10.8.2 [88] et "+" conformément à la norme ANSI/HIBC 2.3 [89]). Il s'agit d'une norme d'application pour le marquage d'articles de petite taille dans les domaines de l'électronique et des soins de santé par exemple. Ces codes-barres se prêtent bien au marquage direct utilisant le marquage par jet d'encre ou par laser et à l'impression d'étiquettes.

Les prescriptions applicables à l'étiquetage d'articles et au marquage direct de produits à l'aide de codes-barres linéaires et bi-dimensionnels sont définis dans la norme ISO 28219 [53]. Les prescriptions applicables à la conception d'étiquettes à codes-barres linéaires et 2D sont décrites dans la norme ISO 22742 [54], tandis que celles applicables aux étiquettes d'expédition, de transport et de réception sont présentées dans la norme ISO 15394 [55].

7.5.2 Dispositifs RFID

Les dispositifs RFID permettent d'étiqueter des objets et de lire les informations stockées sur ces étiquettes au moyen de technologies de communication sans fil à courte portée. Les spécifications applicables aux dispositifs RFID portent sur l'identification des objets, les caractéristiques de l'interface radioélectrique et les protocoles de communication de données.

La norme ISO/CEI 15963 [56] décrit la manière dont des identifiants uniques sont assignés à des étiquettes à radiofréquences (RF). Les étiquettes RF disposent d'un identifiant qui leur est attribué par le fabricant du circuit intégré – à savoir l'identifiant d'étiquette. L'identifiant d'étiquette (TID) peut être utilisé comme identifiant d'article unique (UII), lorsque l'étiquette est apposée sur un article. L'UII peut aussi être stocké dans une partie distincte de la mémoire de l'étiquette. En pareil cas, l'UII pourrait être un code EPC selon les spécifications d'EPCglobal.

La Figure 9 représente le format de l'identifiant d'étiquette ISO/CEI 15963.

Classe d'attribution (AC)	Numéro d'enregistrement de l'entité émettrice du TID	Numéro de série
8 bits	Taille définie par la valeur de la classe AC	Taille définie par la valeur de la classe AC et de l'entité émettrice du TID

Figure 9 – Format de l'identifiant d'étiquette ISO/CEI 15963.3

La classe d'attribution indique l'autorité qui assigne les numéros, à savoir l'entité émettrice du TID. Les fabricants de cartes à circuit imprimé peuvent s'enregistrer pour l'assignation d'identifiants uniques, conformément au système ISO/CEI 7816-6 [90] ou au système de l'American National Standards Institute INCITS (International Committee for Information Technology Standards), de même que les fabricants d'étiquettes destinées aux conteneurs pour le transport de marchandises, conformément aux procédures décrites dans la norme ISO 14816 [91].Les identifiants d'EPCglobal sont pris en compte dans le système ISO/CEI 15963 sous la forme "GS1 class".

Les cinq classes d'entités émettrices de TID sont présentées sur la Figure 10:

Valeur de la classe AC	**Classe**	**Taille de l'identificateur de l'entité émettrice du TID**	**Taille du numéro de série**	**Organisme d'enregistrement (du numéro d'enregistrement de l'entité émettrice du TID)**
000xxxxx	INCITS 256	Voir ANSI INCITS 256 [92] & 371.1 [93]	Voir ANSI INCITS 256 et 371.1	autoid.org
11100000	ISO/CEI 7816-6	8 bits	48 bits	APACS (UK Payments Administration)
11100001	ISO 14816	Voir NEN	Voir NEN	NEN (Institut de normalisation des Pays-Bas)
11100010	GS1	Voir la norme ISO/CEI 18000-6 Type C [94] & ISO/CEI 18000-3 Mode 3 [95]	Voir la norme ISO/CEI 18000-6 Type C & 18000-3 Mode 3	GS1
11100011	ISO/CEI 7816-6	8 bits	48 bits	APACS (y compris la taille de la mémoire et l'en-tête étendu de l'identifiant TID)
Toutes les autres valeurs	Réservé			Réservé

Figure 10 – Classes d'entités émettrices TID uniques

L'identification des animaux a été l'une des premières applications des étiquettes RFID. L'ISO a élaboré en 1994 une norme définissant la structure d'un code d'identification des animaux par radiofréquence (ID) (norme ISO 11784 [96]). La norme complémentaire ISO 11785 [97] décrit la manière de lire les informations figurant sur cette étiquette.

L'ISO a défini par la suite un ensemble complet de spécifications portant sur l'identification par radiofréquence pour la gestion des objets: les normes ISO/CEI 15961 à 15963 décrivent le protocole commun de données et les formats d'identification applicables aux normes ISO/CEI de la série 18000 [98], qui décrivent les interfaces radioélectriques à différentes fréquences. Des spécifications distinctes sont nécessaires pour les différentes bandes de fréquences, étant donné que la fréquence d'exploitation détermine les caractéristiques de la capacité de communication, par exemple la portée en exploitation ou la question de savoir si la présence d'eau a une incidence sur la transmission.

La norme ISO/CEI 29167-1 [57] définit l'architecture pour les services de sécurité et la gestion des fichiers dans le cadre des normes relatives à l'interface radioélectrique ISO/CEI de la série 18000. Des mécanismes de sécurité dépendant de l'application sont définis et une étiquette peut prendre en charge la totalité ou un sous-ensemble de ces derniers. Un dispositif d'interrogation d'une étiquette RFID peut accéder aux informations sur les mécanismes de sécurité pris en charge par une étiquette ainsi qu'à d'autres renseignements tels que l'algorithme de chiffrement et la longueur des clés employée.

On trouve dans la norme ISO/CEI TR 24729-4 [58] des directives de mise en oeuvre à l'intention des concepteurs de systèmes permettant d'évaluer les risques potentiels pour la sécurité des données sur l'étiquette et la communication entre l'étiquette et le lecteur, ainsi que des descriptions des mesures de rétorsion à prendre pour garantir la sécurité des données sur les étiquettes.

Les applications des étiquettes RFID à la chaîne d'approvisionnement (certaines parties de la norme s'appliquent aux conteneurs pour le transport de marchandises, aux éléments de transport restituables, aux unités de transport, à l'emballage des produits et à l'étiquetage des produits) sont définies dans les normes ISO 17363 à 17367 [99] à [103]; la norme ISO 18185 [104] décrit la manière dont les étiquettes RFID permettent de suivre les mouvements des conteneurs pour le transport de marchandises. L'ISO a également élaboré des spécifications relatives aux tests de qualité de fonctionnement et de conformité.

L'emblème RFID défini dans la norme ISO/CEI 29160 [105] peut être utilisé comme label sur les produits pour indiquer la présence d'une étiquette RFID. Voir la Figure 11.

Figure 11 – Exemple d'emblème RFID défini dans la norme ISO/CEI 29160

EPCglobal est la filiale de GS1 chargée d'élaborer des spécifications applicables à l'utilisation de codes produits électroniques avec des étiquettes RFID. EPCglobal a mis au point une série de normes comprenant des spécifications applicables au codage des données d'étiquettes, aux protocoles des interfaces radioélectriques, aux protocoles pour les lecteurs ainsi qu'aux services d'information et de nommage d'objets. La Figure 12 donne un aperçu de la série de normes mises au point par EPCglobal.

Les principaux éléments de la série de normes élaborées par EPCglobal sont les suivants:

- La norme de données d'étiquettes EPC (TDS) définit plusieurs systèmes d'identification et décrit comment ces données sont codées sur les étiquettes ainsi que la manière dont elles sont codées sous une forme adaptée, pour pouvoir être utilisées dans le réseau de systèmes EPC.
- Une version lisible en machine des formats de données EPC figure dans la norme relative à la traduction des données d'étiquettes EPC (TDT) standard. Elle peut être utilisée pour valider les identifiants EPC et les traduire entre différentes représentations des données.
- Les protocoles d'étiquettes sont des interfaces radioélectriques RFID. Sur l'interface "Gen 2", un lecteur envoie des informations à une étiquette en modulant un signal radioélectrique dans la gamme 860-960 MHz. Les étiquettes sont passives, en ce sens qu'elles reçoivent de l'énergie en provenance du signal émis par le lecteur. Ce protocole d'interface radioélectrique a été inclus dans les spécifications ISO/CEI de la série 18000 (Type C – Partie 6). Cette interface radioélectrique en ondes décamétriques fonctionne à 13,65 MHz. La spécification en question est compatible en amont avec la norme ISO/CEI 15693 [106].
- Le protocole LLRP (low level reader protocol) est utilisé par un client pour contrôler un lecteur au niveau de l'exploitation du protocole de l'interface radioélectrique et définit une interface entre les logiciels d'application et les lecteurs (protocole lecteur (RP)).
- Les lecteurs découvrent les clients en utilisant les procédures définies dans la norme DCI (Découverte, configuration et initialisation).
- La norme sur la gestion des lecteurs (RM) sert à suivre l'état de fonctionnement des lecteurs RFID. Elle repose sur l'utilisation du protocole simple de gestion de réseau (SNMP) défini par le Groupe d'étude sur l'ingénierie Internet (IETF).
- La norme relative aux événements reçus au niveau de la couche application (ALE) permet aux clients d'obtenir des données EPC filtrées. Cette interface assure l'indépendance entre les composants de l'infrastructure qui acquièrent l'information EPC "brute", les composants de l'architecture qui traitent ces données et les applications qui les utilisent.
- La norme relative aux services d'informations sur les EPC (EPCIS) permet d'échanger des données EPC dans et entre les entreprises.
- Le vocabulaire normalisé (core business vocabulary – CBV) vise à faire en sorte que toutes les parties échangeant des données aient une compréhension commune de la signification de ces données.
- La norme relative au service de nommage d'objets (ONS) décrit comment le système des noms de domaine (DNS) peut être utilisé pour obtenir des informations associées à un code EPC déterminé.
- La norme relative au profil de certificat d'EPCglobal décrit la manière d'authentifier les entités faisant partie du réseau mondial EPC. Le cadre d'authentification de la Recommandation UIT-T X.509 [60] et les profils de l'infrastructure de clé publique Internet définis dans les normes IETF RFC 3280 [61] et IETF RFC 3279 [62] sont utilisés.

- La norme "Pedigree" traite de la manière de gérer des documents sur un "pedigree" électronique pour les produits pharmaceutiques dans les applications liées à la chaîne d'approvisionnement en produits pharmaceutiques.

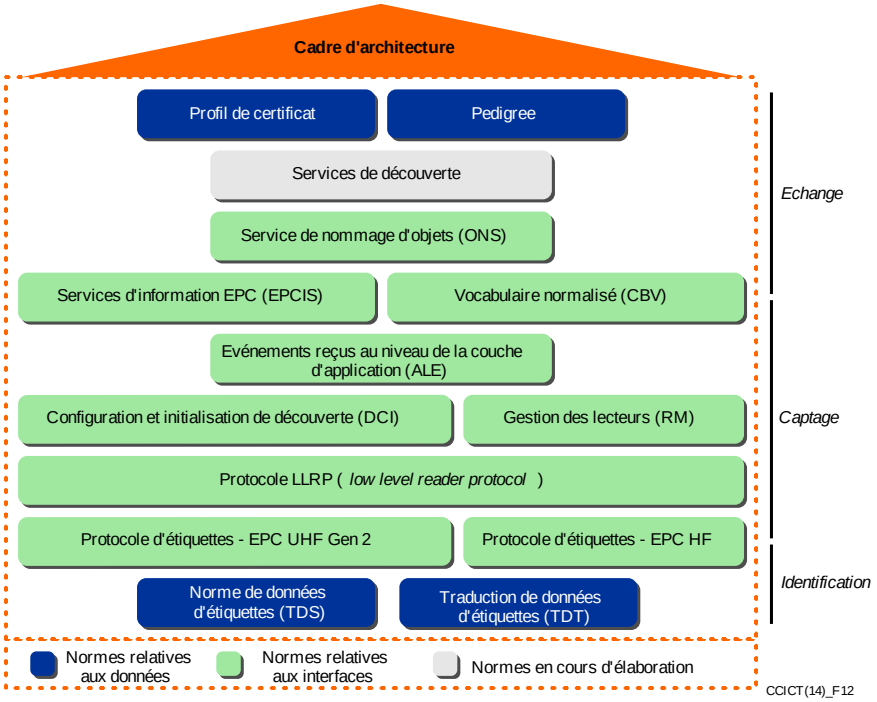


Figure 12 – Aperçu des normes EPCglobal [59]

7.6 Sécurisation des étiquettes d'impression et des étiquettes holographiques

Il est possible de faire appel à des techniques d'impression sécurisées pour créer des étiquettes de garantie d'inviolabilité, étiquettes qui peuvent être complétées par des hologrammes difficiles à falsifier. A noter toutefois que l'utilisation abusive et la reproduction de tels mécanismes sont largement répandues parmi les contrefacteurs.

7.7 Gestion de la chaîne logistique

Il est très important d'assurer la sécurité des chaînes logistiques pour lutter contre les activités de contrefaçon. Les normes ISO de la série 28000 publiées en tant que normes internationales définissent les exigences permettant de garantir la sûreté de la chaîne logistique. Ces normes sont applicables aux organismes de toute taille, opérant dans les secteurs de la production, des services, de l'entreposage et du transport aérien, ferroviaire, routier et maritime, à tous les stades du processus de production ou d'approvisionnement. Les normes suivantes ont été publiées:

- ISO 28000:2007, *Spécifications pour les systèmes de gestion de la sûreté pour la chaîne d'approvisionnement*. [107]
- ISO 28001:2007, *Systèmes de gestion de la sécurité pour la chaîne d'approvisionnement – Meilleures pratiques pour la mise en application de la sécurité de la chaîne d'approvisionnement – Evaluations et plans – Exigences et orientations*. [108]
- ISO 28003:2007, *Systèmes de gestion de la sécurité pour la chaîne d'approvisionnement – Exigences pour les organismes effectuant l'audit et la certification des systèmes de gestion de la sécurité pour la chaîne d'approvisionnement*. [109]

- ISO 28004:2007, *Systèmes de gestion de la sécurité pour la chaîne d'approvisionnement – Lignes directrices pour la mise en application de la norme ISO 28000 – Partie 1: Principes généraux*. [110]
- ISO 28005-2:2011, *Systèmes de gestion de la sécurité pour la chaîne logistique – Opérations portuaires assistées par systèmes électroniques (EPC) – Partie 2: Eléments de données principaux*. [111]

Conformément aux normes ISO de la série 28000, les organisations doivent évaluer les conditions de sécurité dans lesquelles elles fonctionnent et déterminer si des mesures de sécurité suffisantes ont été prises. On trouvera à la Figure 13 les éléments d'un système de gestion de la sécurité.

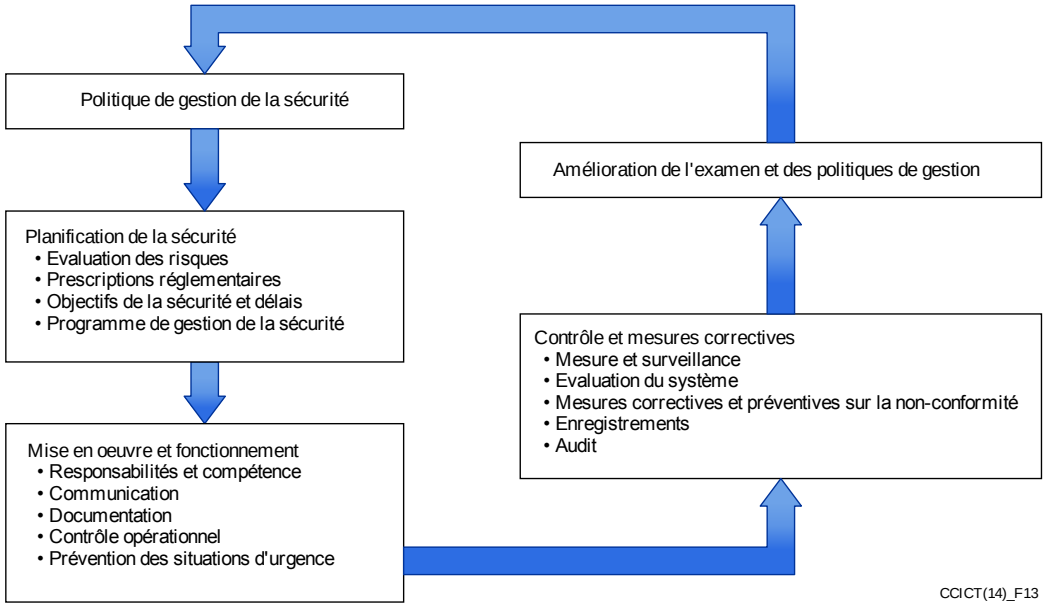


Figure 13 – Eléments du système de gestion de la sécurité ISO 28000

Le Cadre de normes SAFE de l'Organisation mondiale des douanes (OMD) [63] vise à garantir la sécurité de la chaîne logistique internationale et comprend un manuel décrivant les facteurs qui permettent d'identifier les envois risquant de contenir des produits de contrefaçon. Le Cadre SAFE repose sur des accords du réseau douane-douane et des partenariats douane-entreprises, la douane offrant des avantages aux entreprises qui respectent les normes minimales en matière de sécurité de la chaîne logistique.

Le Comité technique 107 de la CEI (CEI TC 107), chargé de l'étude de la gestion des processus pour l'avionique, a élaboré des spécifications sur les moyens d'éviter l'utilisation de composants électroniques de contrefaçon, frauduleux et recyclés [64]. Ce Comité s'emploie actuellement à établir une spécification relative à la gestion des composants électroniques provenant de sources non franchisées pour empêcher l'introduction de composants contrefaits dans la chaîne logistique [65].

SAE International (ancienne Society for Automotive Engineers) a conçu un certain nombre de spécifications visant expressément à éviter l'introduction de composants électroniques de contrefaçon dans les chaînes logistiques des secteurs de l'aérospatiale et de l'automobile, qui sont largement utilisées dans le secteur de l'électronique. La SAE a établi deux documents à l'usage des responsables des décisions en matière d'achats, à savoir:

SAE AS5553 [112]: "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation"; et

SAE ARP6178 [113]: "Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors"; ainsi qu'une spécification à l'usage des distributeurs: SAE AS6081 [114]: "Counterfeit Electronic Parts; Avoidance Protocol, Distributors". La SAE a aussi élaboré une spécification relative aux essais: SAE AS6171 [115]: "Test Methods Standard; Counterfeit Electronic Parts".

Le Comité technique 107 de la CEI travaille en étroite collaboration avec SAE International concernant la norme SAE AS5553 dans le cadre d'un mécanisme de liaison.

La plupart des instances susmentionnées chargées de lutter contre les produits de contrefaçon fournissent des avis et des directives sur la gestion de la chaîne logistique. En général, des prescriptions (l'évaluation de la conformité est effectuée par une première, une deuxième ou une tierce partie) sont imposées en ce qui concerne la traçabilité, l'inspection et les tests. En 2011, l'IP Crime Group du Royaume-Uni a conçu un kit d'aide en ligne sur la chaîne logistique.

7.8 Tests

La Commission électrotechnique internationale (CEI) dirige les systèmes ci-après d'évaluation de la conformité http://www.CEI.ch/about/activities/conformity.htm:

- IECEE – Système CEI d'évaluation de la conformité des équipements et des composants électrotechniques;
- IECEx – Système CEI de certification de conformité aux normes des matériels électriques destinés à être utilisés en atmosphères explosives;
- IECQ – Système CEI d'évaluation de la conformité des composants électroniques.

Ces systèmes d'évaluation de la conformité de la CEI sont fondés sur l'évaluation de la conformité par un organisme tiers et utilisent des systèmes en ligne pour donner des renseignements sur les certificats pouvant être employés pour identifier des produits de contrefaçon.

La CEI administre le système des organismes de certification (CB), qui repose sur le principe de la reconnaissance mutuelle (acceptation réciproque), par ses membres, des résultats d'essais, dans le but d'obtenir une certification ou une homologation de produits à l'échelon national. Le Bulletin du système CB est une base de données destinée aux utilisateurs du http://members.CEIee.org/CEIee/CEIeemembers.nsf/cb_bulletin?OpenForm système CB, qui donne des renseignements sur:

- les normes dont l'utilisation est acceptée dans le système;
- les organismes de certification nationaux participants, y compris les catégories de produits et les normes pour lesquelles ils ont été reconnus; et
- les différences nationales entre chaque pays membres pour chaque norme.

Le système CBTC Online de l'IECEE est un système d'enregistrement de certificats de test en ligne destiné aux organismes nationaux de certification, qui permet également l'accès du public.

L'IECEE a créé un Groupe d'action chargé d'étudier des mesures de lutte contre la contrefaçon (CMC-WG 23 "Contrefaçon").

Le système de certification international IECEx comprend les systèmes suivants:

– Système Equipement certifié IECEx.
– Système Installations de services certifiées IECEx.
– Système Licence pour les marques de conformité IECEx.
– Certification de compétence de personnes IECEx.

Le Certificat CoC IECEx (Certificat de conformité) en ligne donne des renseignements sur les certificats et les licences délivrés conformément à ces systèmes.

L'IECQ gère le Plan IECQ de gestion des composants électroniques (ECMP) pour l'avionique et le système IECQ de gestion des processus pour les substances dangereuses (HSPM). Des certificats sont accessibles en ligne.

7.9 Bases de données

Des bases de données de produits de contrefaçon connus sont mises à la disposition des organismes chargés de l'application de la loi, par exemple celles gérées par l'OMD et Interpol, ainsi que des consommateurs. Le Bureau d'enquêtes sur la contrefaçon ICC tient à jour une base de données d'études de cas.

7.10 Surveillance du marché

On entend par surveillance du marché "les opérations effectuées et les mesures prises par des autorités désignées pour garantir que les produits ne portent pas atteinte à la santé et à la sécurité ou à tout autre aspect de la protection de l'intérêt public et, dans le cas des produits entrant dans le champ d'application de la législation pertinente, qu'ils sont conformes aux exigences définies dans cette législation" [66].

Les produits de contrefaçon peuvent être identifiés lors des opérations de surveillance du marché et les autorités chargées d'une telle surveillance peuvent être associées aux mesures de lutte contre le commerce des produits de contrefaçon. La Commission économique pour l'Europe de l'Organisation des Nations Unies (CEE-ONU) recommande que les autorités nationales de surveillance du marché et les autorités douanières collaborent et que les détenteurs de droits aient la possibilité de rendre compte aux autorités de surveillance du marché des marchandises de contrefaçon [67].

Dans certains pays, les produits doivent être enregistrés pour pouvoir être commercialisés. Ainsi, l'Organisation de normalisation du Nigéria a récemment mis en place un système d'enregistrement en ligne des produits destiné à limiter la vente de produits de contrefaçon.

8 Organisations de normalisation

Les principales organisations internationales de normalisation chargées d'étudier les questions ayant trait à la lutte contre contrefaçon sont l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI).

L'ISO a créé en 2009 un Comité technique chargé d'établir des spécifications sur les dispositifs techniques anti-contrefaçon (ISO TC 246). Ce Comité a défini des critères de performance des solutions d'authentification utilisées pour lutter contre la contrefaçon de biens matériels (ISO 12931) [48]. Cette spécification vise à étayer le capital de confiance des consommateurs, à responsabiliser et à sécuriser les circuits de distribution et à aider les autorités publiques à déployer des mesures préventives et répressives. Le Comité technique ISO TC 246 n'existe plus, mais ses travaux dans ce domaine se poursuivront dans le cadre du Comité technique ISO TC 247.

Le Comité technique ISO/TC 247, chargé des mesures de prévention et de lutte contre la fraude, s'occupe de la normalisation dans le domaine de la détection, de la prévention et du contrôle de la fraude liée à l'identité, de la fraude financière, de la fraude relative aux produits et d'autres formes de fraude sociale et économique. Ce Comité a élaboré une norme d'orientation de l'ISO sur l'interopérabilité des identificateurs d'objet pour la lutte contre la contrefaçon (ISO 16678 [116]: "Lignes directrices relatives à des systèmes interopérables d'identification d'objets et d'authentification associés destinés à décourager la contrefaçon et le commerce illicite"). Ce nouveau projet concerne l'utilisation de la sérialisation de masse pour identifier des produits à partir d'une base de données destinée à vérifier un certain niveau d'authenticité. Cette Norme

internationale doit permettre une identification fiable et sûre des objets, afin de décourager l'introduction d'objets illégaux sur le marché. Il est possible d'authentifier les produits portant des numéros de série tout au long de la chaîne de production et de distribution, y compris au niveau du consommateur.

L'ISO a reconnu que la contrefaçon et le piratage touchaient une très large gamme de produits de consommation: habillement et chaussures, médicaments, automobiles et pièces détachées pour l'automobile, produits alimentaires et boissons, cosmétiques, films et musique, produits électriques, dispositifs de sécurité et pièces détachées pour l'aviation. Pour les consommateurs, les risques concernent plus particulièrement la sécurité et la santé, les aspects liés à la qualité de fonctionnement, la possibilité d'utilisation l'adéquation à un usage, l'accessibilité, la protection des données, la perte d'emplois, le préjudice économique et les liens avec le crime organisé. http://www.iso.org/iso/copolco_priority-programme_annual-report_2012.pdf.

Le Comité technique mixte ISO/CEI JTC 1/SC 31 mène actuellement des travaux sur les techniques automatiques d'identification et de saisie de données (AIDC). Ce Comité est composé de sept Groupes de travail chargés d'étudier les questions suivantes:

- GT 1 Dispositif de transport des données;
- GT 2 Structure des données;
- GT 4 Identification par radiofréquences (RFID) pour la gestion d'objets;
- GT 5 Systèmes de géolocalisation en temps réel;
- GT 6 Gestion et identification d'élément mobile (MIIM);
- GT 7 Sécurité pour la gestion d'objets.

Le Comité européen de normalisation (CEN) effectue également des travaux sur les techniques AIDC au sein du Comité technique TC 225.

Un grand nombre d'organisations nationales de normalisation ont institué des comités équivalents à ceux de l'ISO/CEI. Pour ne prendre qu'un exemple, l'Institut allemand de normalisation (DIN) a créé le Comité DIN NA 043-01-31, qui est chargé de l'étude des techniques automatiques d'identification et de saisie de données [68] et le Comité DIN NA 043-01-31-04 UA, qui étudie l'identification par radiofréquences pour la gestion d'objets.

Le Comité technique CEI TC 107 sur la gestion des processus pour l'avionique mène des travaux sur les mesures de prévention de la contrefaçon.

En outre, SAE International élabore actuellement des spécifications visant à éviter l'utilisation de composants électroniques de contrefaçon dans les secteurs de haute technologie; pour sa part, GS1 a mis au point une série de spécifications sur l'identification d'objets et la gestion de la chaîne logistique.

9 Lignes directrices sur la lutte contre la contrefaçon

Un certain nombre d'organismes venus d'horizons divers, qu'il s'agisse d'équipementiers et de distributeurs, d'organismes publics et d'instances chargées de faire respecter la loi ainsi que de consommateurs, ont présenté des lignes directrices relatives à la lutte contre la contrefaçon.

L'Anti-Counterfeiting Forum propose un certain nombre de bonnes pratiques à l'intention des constructeurs d'équipements d'origine (OEM – Original Equipment Manufacturers), des distributeurs et des fabricants de composants [69]. Ces lignes directrices visent à:

- favoriser l'approvisionnement direct auprès du constructeur ou d'un distributeur agréé ou, si cela n'est pas possible, auprès d'une source du marché gris établie au niveau local;

- insister pour obtenir des justificatifs attestant l'authenticité, si des sources du marché gris sont utilisées;
- favoriser une plus grande coordination de la gestion des composants et des produits pendant leur cycle de vie;
- faire en sorte que les déchets et les produits défectueux soient éliminés et mis au rebut;
- améliorer la traçabilité des produits en utilisant des identificateurs uniques et en contrôlant la documentation.

Le Components Technology Institute Inc. (CTI) a élaboré le Programme CCAP-101 (Counterfeit Components Avoidance Program – Programme de lutte contre les composants de contrefaçon) [70] relatif à la certification de distributeurs indépendants de composants électroniques. Les distributeurs sont tenus de respecter des règles afin de repérer et d'éviter la fourniture de composants de contrefaçon à leurs clients. Des tests électriques peuvent être effectués. Ce programme de certification vise à satisfaire aux objectifs de la spécification SAE AS5553.

De même, l'Independent Distributors of Electronics Association (IDEA) a élaboré une spécification relative à l'atténuation des effets de la contrefaçon et aux inspections en la matière (IDEA-STD-1010A) [117] ainsi qu'une spécification relative à la gestion de la qualité (IDEA-QMS-9090) [118].

La feuille de route de la Chambre de commerce internationale (ICC) sur la propriété intellectuelle (ICC IP Roadmap) comprend des recommandations à l'intention des entreprises et des pouvoirs publics touchant tous les aspects de la protection de la propriété intellectuelle, y compris la lutte contre la contrefaçon et le piratage. L'ICC exhorte en particulier les gouvernements à intensifier leurs efforts pour faire appliquer la réglementation relative aux DPI, étant donné que "les ressources allouées par les pouvoirs publics en faveur de la lutte contre le piratage et la contrefaçon sont souvent très insuffisantes au regard de la gravité du problème".

L'OCDE a fait observer que l'on pouvait subdiviser le marché des produits de contrefaçon et des produits piratés en un "marché primaire", sur lequel les consommateurs croient qu'ils achètent un produit authentique, et un marché secondaire", sur lequel les acheteurs font délibérément l'acquisition de produits de contrefaçon ou de produits piratés, soucieux de faire une bonne affaire. Une personne qui ne voit pas d'inconvénients à acheter une chemise ou un sac à main de contrefaçon ne voudra peut-être pas forcément acheter des médicaments ou du matériel électrique contrefaits. Différentes stratégies s'imposent si l'on veut lutter contre la contrefaçon sur ces deux marchés, d'où la nécessité de savoir sur quel marché tel ou tel produit est commercialisé.

Pour lutter efficacement contre la contrefaçon de produits sur le marché primaire, on peut par exemple organiser des campagnes d'information destinées à attirer l'attention des consommateurs sur les risques liés à l'acquisition de produits de contrefaçon, alors que pour les produits commercialisés sur le marché secondaire, il faudra peut-être imposer des sanctions plus lourdes.

Le kit d'aide en ligne sur la chaîne logistique de l'IP Crime Group du Royaume-Uni (IP Crime Group Supply Chain Toolkit) [71] a pour but de sensibiliser l'opinion au problème de la contrefaçon de produits qui sont introduits dans les chaînes d'approvisionnement licites des entreprises et fournit des indications sur la manière de protéger les actifs intellectuels. On trouvera à la Figure 14 un aperçu du processus permettant à une entreprise de réduire les risques d'entrée de produits de contrefaçon dans sa chaîne d'approvisionnement.

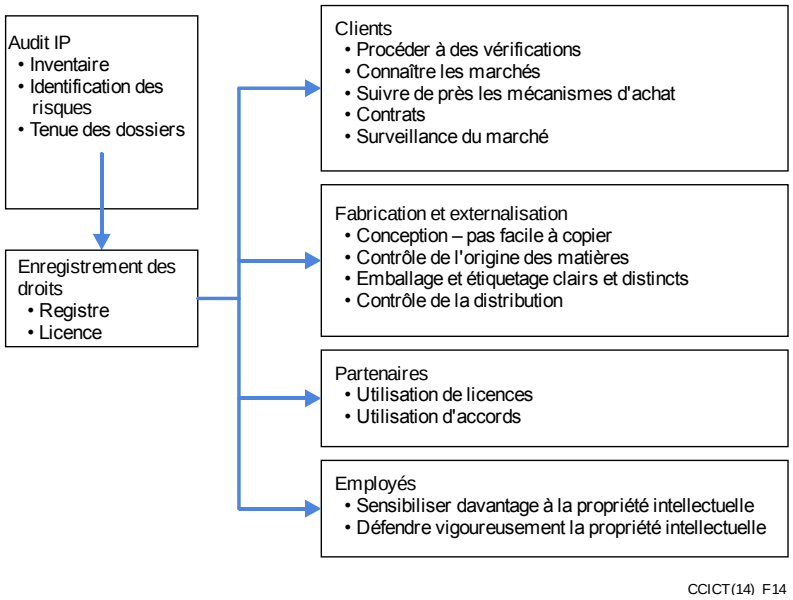


Figure 14 – Protection des droits de propriété intellectuelle (adapté du kit d'aide en ligne de l'IP Crime Group [71])

Le Forum MMF a élaboré un Guide de ressources à l'intention des gouvernements, qui propose les diverses mesures suivantes:

- Apporter des modifications aux cadres juridiques et réglementaires, afin de limiter l'activation de dispositifs de contrefaçon sur les réseaux de télécommunication.
- Imposer des restrictions à l'importation des dispositifs et accessoires mobiles qui ne sont pas conformes aux normes du secteur, qui n'ont pas été approuvés ou qui ne sont pas conformes au cadre législatif et réglementaire d'un pays.
- Nouer les alliances nécessaires à l'échelle mondiale entre les entreprises et les différentes autorités concernées et rechercher des solutions aux fins de la validation des produits d'origine par les autorités, les consommateurs et les circuits de vente.
- Mettre au point des solutions techniques harmonisées et innovantes, visant à limiter la possibilité d'activer des dispositifs mobiles contrefaits sur les réseaux de télécommunication.
- Opter pour des normes susceptibles de conduire à des caractéristiques de sécurité renforcées (numéros d'identification individuels uniques, par exemple), pour décourager la fabrication de produits de contrefaçon et d'autres produits illicites.

Cette approche va forcément plus loin que l'action coercitive traditionnelle et consiste plutôt à bloquer ces dispositifs pour qu'ils ne puissent pas fonctionner sur les réseaux. Cela étant, l'application des lois, les campagnes de sensibilisation et la surveillance du marché garderont toute leur importance et les fabricants de téléphones mobiles continueront, chaque fois que possible, de collaborer avec les autorités nationales.

10 Conclusions

La contrefaçon est un phénomène de plus en plus préoccupant qui a des incidences sur une gamme toujours plus large de produits. Dans le secteur des TIC, les téléphones mobiles constituent une cible de choix, puisqu'environ 250 millions de téléphones mobiles de contrefaçon se vendent chaque année, ce qui représente près de 15% à 20% du marché mondial. La contrefaçon a non

seulement des conséquences économiques évidentes pour les fabricants de produits authentiques (dépréciation de la marque, manque à gagner, atteinte aux droits d'auteur ou contrefaçon de marque, concurrence déloyale), les revendeurs agréés et les gouvernements (les contrefacteurs échappent au paiement de l'impôt, ce qui impose un surcoût pour assurer la conformité à la législation nationale applicable, il devient nécessaire de réagir aux menaces qui pèsent sur la sécurité publique et les pertes d'emploi sont importantes), sans parler des risques pour la santé, la sécurité et la vie privée des consommateurs, des aspects liés à la sécurité publique et des incidences négatives pour les opérateurs de réseaux (baisse de la qualité de service, risques de brouillages, problèmes de compatibilité électromagnétique (CEM) et interruption du réseau). La plupart de ces téléphones mobiles de contrefaçon sont fabriqués dans un pays asiatique, d'où proviennent la plus grande partie des composants électroniques contrefaits résultant du recyclage dans le secteur informel des déchets d'équipements électriques et électroniques provenant des pays développés. Telles sont les conclusions qui se dégagent d'une audition devant la Commission des forces armées du Sénat américain sur les composants électroniques de contrefaçon dans la chaîne d'approvisionnement de la défense [9]. Il va sans dire qu'il reste encore beaucoup à faire pour pouvoir localiser les sources des équipements de contrefaçon et pour contrer ce phénomène avant que les produits ne soient exportés dans le monde entier.

Bien qu'il existe des instruments juridiques pour lutter contre la contrefaçon, leur mise en application reste très insuffisante. Dans son rapport publié en 2008, l'OCDE concluait que "l'ampleur et les conséquences de la contrefaçon et du piratage étaient telles qu'elles imposaient de la part des pouvoirs publics, des entreprises et des consommateurs des mesures énergiques en même temps qu'une action plus forte. Dans cette perspective, il est indispensable d'accroître l'efficacité de l'application de la loi et de renforcer les aides publiques pour lutter contre la contrefaçon et le piratage. Une coopération accrue entre les gouvernements et avec les industriels, serait bénéfique, ainsi qu'une meilleure collecte des données".

Les gouvernements se sont davantage investis dans la recherche de solutions à ce problème et nombreux sont ceux qui organisent des campagnes de sensibilisation, en fournissant des avis et en engageant plus activement des poursuites contre les délinquants, comme on a pu le constater récemment en Chine. Les gouvernements doivent non seulement faire appliquer les réglementations relatives aux DPI, mais aussi mettre en oeuvre la Convention de Bâle, pour veiller à ce que les appareils usagés et en fin de vie soient gérés d'une manière écologiquement rationnelle, au lieu de contribuer à l'économie informelle des produits de contrefaçon. Des pratiques de recyclage éthiques devraient par ailleurs être adoptées dans le monde entier.

Les gouvernements voudront peut-être également rattacher leurs activités de surveillance du marché à celles menées par les autorités douanières, pour améliorer les capacités de détection des produits de contrefaçon. Les saisies d'équipements TIC de contrefaçon devraient être considérées comme des déchets d'équipements électriques et électroniques et traités conformément aux systèmes de gestion écologiquement rationnelle des déchets.

Les entreprises et les groupes industriels touchés par la contrefaçon ont organisé des campagnes d'information et exercé des pressions pour faire valoir leurs intérêts. Il semble cependant qu'une plus grande sensibilisation de l'opinion aux problèmes de la contrefaçon soit encore nécessaire. Aux Etats-Unis, en vertu de la Loi d'autorisation de la défense nationale (National Defence Authorisation Act – NDAA) de 2012, il appartient aux fournisseurs de détecter les faux composants et de prendre les mesures correctives nécessaires dans les cas où de faux composants ont été intégrés dans des produits.

Il faut également attirer l'attention des consommateurs sur les dangers de l'achat d'équipements de contrefaçon et leur faire prendre conscience du fait que l'utilisation de produits de contrefaçon n'est pas sans risque, ces produits ne fonctionnant peut-être pas aussi bien que des produits authentiques.

Il est évident que bon nombre d'organismes nationaux et internationaux ainsi que les fabricants, les revendeurs et les médias mettent régulièrement en avant les problèmes que posent les produits de contrefaçon pour les consommateurs. Il n'en demeure pas moins que bien souvent, ceux-ci choisissent sciemment de faire l'acquisition de produits de contrefaçon, quelles que soient les conséquences que cela pourrait avoir, apparemment pour des raisons de prix.

On pourrait aussi lutter contre la contrefaçon par le biais de la gestion du cycle de vie des équipements, non seulement au niveau de la chaîne d'approvisionnement, mais aussi au niveau des processus de retour, de réutilisation et de recyclage pendant toute la durée du cycle de vie des équipements. Pour assurer la gestion du cycle de vie, il faut disposer de moyens d'identification et d'authentification des articles et des procédés afin d'en garder la trace en toute sécurité. Ce suivi devrait néanmoins être effectué comme il se doit et de manière adaptée à sa finalité, dans la mesure où les techniques automatiques d'identification et de captage des données (AIDC), telles que les techniques RFID, soulèvent d'importants problèmes de confidentialité, un lien pouvant être établi entre les objets et leurs propriétaires Il convient en conséquence de veiller, lors de la normalisation, au respect de la vie privée des consommateurs et d'éviter de faire exagérément pression sur les utilisateurs de produits TIC par l'intermédiaire de mécanismes d'enregistrement des identificateurs. En outre, il convient de protéger les consommateurs contre toute déconnexion arbitraire des réseaux.

Il est possible de recourir aux techniques AIDC et aux normes relatives à la gestion de la chaîne d'approvisionnement pour lutter contre la contrefaçon, comme nous l'avons vu plus haut.

La lutte contre la contrefaçon passe aussi par une coopération entre tous les secteurs d'activité. Des outils génériques (par exemple ceux utilisés pour détecter les faux passeports et les faux billets) ainsi qu'un large éventail de mécanismes propres à un produit ou un secteur de mesures ciblées, avec le concours du secteur public et du secteur privé, pourraient ainsi être mis à la disposition des instances chargées de faire respecter la loi, par exemple les autorités douanières.

Dans le secteur de la téléphonie mobile, différentes administrations et autorités de régulation utilisent actuellement, ou projettent d'utiliser, un certain nombre de systèmes fondés sur l'enregistrement des numéros IMEI pour identifier les terminaux mobiles authentiques et importés légalement. Diverses initiatives ont également été prises au niveau régional, en vue d'échanger des informations sur les terminaux mobiles d'origine illégale. Tous ces mécanismes peuvent cependant donner lieu à des problèmes pour les utilisateurs légitimes. Ainsi, un utilisateur qui se rend à l'étranger et utilise une carte SIM locale dans son dispositif risque de se retrouver pris au piège d'une liste blanche, qui l'empêchera de se servir de son dispositif. De tels mécanismes peuvent être source de difficultés pour la libre circulation des marchandises. Dans les autres secteurs des TIC, il n'existe pas de mécanismes de ce type en raison de la nature des produits et de la structure des entreprises.

Bien que certains pays aient déployé avec succès des solutions reposant sur l'utilisation de numéros IMEI pour endiguer le phénomène de la contrefaçon des téléphones mobiles, d'autres, et notamment les pays en développement, éprouvent encore de nombreuses difficultés à trouver des solutions efficaces au problème de la contrefaçon des dispositifs. Les solutions mises en place aujourd'hui dans certains pays consistent à bloquer sur les réseaux les téléphones mobiles comportant des numéros IMEI non valables, à bloquer l'utilisation des équipements non homologués par le régulateur, à bloquer l'importation illégale de ces dispositifs ou encore à prendre d'autres mesures axées sur la sensibilisation des consommateur, l'application des lois et les réformes apportées à la législation à l'échelle nationale.

Les principales organisations internationales de normalisation ont passé en revue les questions relatives à la lutte contre la contrefaçon. Il n'existe actuellement aucune Recommandation de l'UIT permettant, par exemple, de comparer les différents systèmes en place de lutte contre la contrefaçon, de décrire un cadre adapté et d'étudier la qualité de fonctionnement et l'interopérabilité à l'échelle mondiale. L'UIT et les autres parties prenantes intéressées ont un rôle déterminant à jouer en encourageant la coordination entre les parties concernées, pour définir des moyens de traiter cette question aux niveaux international et régional. De plus, l'UIT est chargée d'aider les membres à prendre les mesures nécessaires pour prévenir ou mettre en évidence l'altération volontaire ou la duplication des identificateurs de dispositif uniques.

Le présent rapport technique traite des questions se rapportant uniquement à la lutte contre la contrefaçon: définition de la contrefaçon, conséquences de ce phénomène, accords sur les DPI et leur exécution, instances du secteur privé chargées de la lutte contre la contrefaçon, mesures prises pour contrer ce phénomène et organisations intervenant dans la lutte contre la contrefaçon. L'UIT devrait étudier cette question de manière plus approfondie, afin d'aider les autorités de régulation à protéger les consommateurs, les opérateurs et les gouvernements contre les conséquences négatives de la contrefaçon de dispositifs.

11 Participation de l'UIT

Par sa Résolution 177, la Conférence de plénipotentiaires de l'UIT tenue en 2010 (PP-10) "*a invité les Etats Membres et les Membres de Secteur* à tenir compte des cadres juridiques et réglementaires d'autres pays concernant les équipements qui nuisent à la qualité de l'infrastructure et des services de télécommunication de ces pays, en prenant notamment en considération les préoccupations des pays en développement en matière de contrefaçon d'équipements" [72].

Il est demandé à l'UIT d'examiner la question de la contrefaçon d'équipements TIC au titre de la Résolution 79 de la CMDT-14, intitulée: "Rôle des télécommunications/technologies de l'information et de la communication dans la lutte contre la contrefaçon de dispositifs de télécommunication/d'information et de communication et le traitement de ce problème" et de la Résolution COM5/4 de la PP-14, intitulée "Lutter contre la contrefaçon de dispositifs de télécommunication fondés sur les technologies de l'information et de la communication".

La Commission d'études 11 (CE 11) étudie le problème de la contrefaçon au titre de la Question 8 et l'UIT a organisé un atelier sur le thème "Lutter contre les équipements TIC de contrefaçon et de qualité médiocre" à Genève en novembre 2014. http://www.UIT.int/en/UIT-T/C-I/Pages/WSHP_counterfeit.aspx.

Les Commissions d'études 16 et 17 de l'UIT-T ont élaboré des Recommandations relatives à l'identification et à l'authentification des objets.

La Commission d'études 5 de l'UIT-T (CE5) est chargée de concevoir des méthodes visant à réduire les effets de l'utilisation des TIC sur l'environnement, par exemple au moyen du recyclage.

Le Directeur du TSB a créé un Groupe ad hoc (AHG) sur les DPI: http://www.UIT.int/en/UIT-T/ipr/Pages/adhoc.aspx, qui est responsable des études relatives, notamment, aux politiques en matière de brevets, aux lignes directrices relatives aux droits d'auteur afférents aux logiciels et aux lignes directrices relatives aux marques. Ce Groupe tient des réunions depuis 1998. L'UIT et l'OMPI ont également organisé conjointement des colloques consacrés, par exemple, aux noms de domaines multilingues, en 2001, (http://www.UIT.int/mlds/) et au "règlement des différends au carrefour des technologies de l'information et de la communication et de la propriété intellectuelle" en 2009: http://www.wipo.int/amc/en/events/workshops/2009/UIT/index.html. Enfin, l'UIT a également organisé une table ronde sur les brevets en 2012, afin d'offrir aux entreprises, aux organismes de normalisation et aux régulateurs un cadre neutre pour déterminer si les politiques

actuelles en matière de brevets et les pratiques en vigueur dans le secteur apportent une réponse adaptée aux besoins des différentes parties prenantes. http://www.UIT.int/en/UIT-T/Workshops-and-Seminars/patent/Pages/default.aspx. A ce jour, ce Groupe n'a pas étudié la question de la contrefaçon.

L'UIT a donc un rôle à jouer dans l'étude du problème de la contrefaçon des équipements TIC.

Le rapport de la CE 1 du Secteur du développement des télécommunications de l'UIT (UIT-D), intitulé "Réglementation et protection du consommateur dans un environnement placé sous le signe de la convergence" (mars 2013), élaboré dans le cadre de la Résolution 64 de la Conférence mondiale de développement des télécommunications de l'UIT (Hyderabad, 2010), indique que les autorités de régulation doivent relever le défi consistant à protéger les innovateurs, les créateurs et les consommateurs contre la contrefaçon et le piratage associé à la distribution en ligne (de plus en plus souvent transfrontière) de biens et de services.

Conformément aux lignes directrices à l'intention des pays en développement sur l'installation de laboratoires de tests d'évaluation de la conformité dans différentes régions publiées par le Secteur du développement des télécommunications de l'UIT en mai 2012, les Etats Membres ont indiqué que les équipements de contrefaçon aggravaient encore les problèmes de conformité et d'interopérabilité http://www.UIT.int/UIT-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf. Il est noté ce qui suit dans ces lignes directrices: "la suspicion d'arrivée sur le marché de produits de qualité inférieure qui ont été refusés dans d'autres pays lors des tests est une autre source de préoccupation, de même que l'importation et le déploiement de produits contrefaits. L'un des points essentiels pour mettre fin à ces préoccupations est la mise en place d'un système d'homologation solide et de laboratoires de test travaillant selon un ensemble de normes techniques, ainsi que d'un système et de capacités de tests permettant d'homologuer et de surveiller les technologies de communication qui sont déployées sur le marché, accompagnés d'une surveillance, de contrôles et de moyens d'application. L'absence d'exigences techniques, de systèmes d'homologation et de laboratoires de test dans un pays ou une région signifie que la protection du marché est très insuffisante".

La mise en oeuvre de plusieurs normes émanant d'organismes différents pour un même produit peut nuire considérablement aux tests et à l'interopérabilité. Il convient de reconnaître qu'un système de test, aussi intéressant qu'il puisse paraître, ne suffira pas à lui seul à apporter de réels changements pour remédier au problème de la contrefaçon.

Il convient en outre de noter qu'étant donné que les contrefacteurs ont recours à des moyens de plus en plus perfectionnés, il arrive que des produits de contrefaçon soient conformes aux prescriptions techniques requises et puissent fonctionner en toute compatibilité avec des produits authentiques. Ainsi, il se peut que des produits de contrefaçon soient conformes à une série de normes techniques pertinentes et aux tests de conformité et d'interopérabilité. En pareil cas, seul le titulaire de la marque sera à même de distinguer avec précision les produits de contrefaçon des produits authentiques, en procédant à une évaluation des produits.

Le problème de la contrefaçon des équipements TIC a été abordé lors de l'Atelier régional de l'UIT sur la réduction de l'écart en matière de normalisation (BSG) pour la région des Etats arabes et la région Afrique (Algérie, 26-28 septembre 2011). A cette occasion, une directive a été élaborée en vue d'encourager l'échange d'informations au niveau régional, par le biais de la création d'une base de données contenant les produits de contrefaçon inscrits sur une liste noire. http://www.UIT.int/UIT-T/newslog/UIT+Regional+Workshop+On+Bridging+The+Standardization+Gap+For+Arab+And+Africa+Regions+Interactive+Training+Session+And+Academia+Session.aspx.

Le Groupe consultatif de la normalisation des télécommunications de l'UIT-T (GCNT), au cours d'une séance d'information consacrée aux questions de conformité et d'interopérabilité (Genève, 13 janvier 2012), et le Forum de l'UIT sur la conformité et l'interopérabilité pour la région des Etats arabes et la région Afrique (Tunisie, 5-7 novembre 2012), ont mis en lumière la conclusion de la région des Etats arabes selon laquelle la contrefaçon d'équipements constitue un problème particulièrement préoccupant, notamment sur le marché des combinés mobiles, et souligné la nécessité d'une coopération à l'échelle mondiale dans ce domaine. http://www.UIT.int/UIT-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/Presentations/Session5/CI%20Forum%202012_Tunis_AAlDin_S5_4.pdf], [http://www.UIT.int/dms_pub/UIT-t/oth/06/5B/T065B00000E0005PPTE.pptx.

Le problème du vol de dispositifs mobiles, du marché gris et des dispositifs de contrefaçon, ainsi que ses incidences pour les entreprises, les opérateurs, les gouvernements et les utilisateurs, ont été examinés lors de la réunion des Associations de régulateurs organisée par le Secteur du développement des télécommunications de l'UIT (Sri Lanka, Colombo, 1er octobre 2012) conformément à la Résolution 48 (Rév.Hyderabad, 2010) sur le renforcement de la coopération entre régulateurs des télécommunications. En vertu de cette Résolution, l'UIT est invitée à organiser, coordonner et faciliter les activités visant à promouvoir l'échange d'informations entre régulateurs et organismes de réglementation sur les grandes questions de réglementation, aux niveaux international et régional. Des représentants de 10 associations régionales de régulateurs, dont ARCTEL-CPLP, AREGNET, ARTAC, EMERG, FRATEL, REGULATEL, OCCUR, FTRA, SATRC et l'APT, ont noté que les mesures prises sur le plan régional pouvaient être très utiles, par exemple dans les domaines suivants:

- Partage des bases de données de listes noires de modèles GSM et CDMA, grâce à la signature d'accords bilatéraux ou multilatéraux.
- Lutter par les professionnels du secteur des recommandations en matière de sécurité visant à lutter contre la reprogrammation de la reproduction des numéros IMEI ou du numéro de série électronique (ESN) du fabricant.
- Création de mécanismes réglementaires budgétaires ou douaniers garantissant que les combinés importés sont soumis à un contrôle renforcé, afin de lutter contre l'exportation ou la réexportation de terminaux mobiles volés ou de leurs composants.
- Organisation de campagnes visant à sensibiliser le public à la nécessité de signaler le vol ou la perte de terminaux mobiles.

De nombreuses associations régionales ont fait part de leur expérience à ce sujet, conscientes qu'il s'agit d'un problème crucial qui doit être résolu en coopération avec les professionnels du secteur et les opérateurs. Les participants à la réunion des associations de régulateurs ont adopté une recommandation invitant l'UIT, en collaboration avec la GSM Association, à mener des études sur le problème du vol de mobiles, du marché gris et des appareils de contrefaçon, et à établir des lignes directrices et des recommandations en la matière. http://www.UIT.int/UIT-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/FinalReport_RA12.pdf.

12 Références

[1] *L'impact économique de la contrefaçon et du piratage,* OCDE, juin 2008.

[2] http://www.oecd.org/dataoecd/57/27/44088872.pdf.

[3] http://www.icc-ccs.org/icc/cib.

[4] *Estimating the global economic and social impacts of counterfeiting and piracy*. http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf.

[5] Intellectual Property Rights Fiscal Year 2100 Seizure Statistics U.S. Customs and Border Protection. http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf.

[6] http://www.havocscope.com/counterfeit-hp-printing-supplies.

[7] http://www.spotafakephone.com/.

[8] IDC February 2012 http://www.idc.com/getdoc.jsp?containerId=prUS23297412.

[9] http://www.levin.senate.gov/newsroom/press/release/background-memo-senate-armed-services-committee-hearing-on-counterfeit-electronic-parts-in-the-dod-supply-chain.

[10] *Defence Industrial Base Assessment: Counterfeit Electronics*, janvier 2010 http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

[11] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf HR 1540 SEC. 818.

[12] In *WIPO Intellectual Property Handbook* http://www.wipo.int/export/sites/www/about-ip/en/iprm/pdf/ip_handbook.pdf.

[13] UK IP Toolkit 2009.

[14] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html.

[15] http://www.wipo.int/treaties/en/ip/washington.

[16] www.wcoipm.org et http://www.wcoomd.org/en/topics/enforcement-and-compliance/activities-and-programmes/ep_intellectual_property_rights.aspx.

[17] http://www.canadainternational.gc.ca/g8/summit-sommet/2009/ipeg.aspx?view=d.

[18] http://www.unece.org/trade/wp6/SectoralInitiatives/MARS/MARS.html.

[19] http://www.ipo.gov.uk/ipenforce/ipenforce-resources.htm.

[20] http://www.aca.or.ke.

[21] http://www.iccwbo.org/bascap/id6169/index.html.

[22] http://www.iccwbo.org/bascap/id7608/index.html.

[23] http://www.pasdirectory.com.

[24] http://www.iccwbo.org/bascap/id42204/index.html.

[25] http://www.iccwbo.org/policy/ip/id2950/index.html.

[26] https://iacc.org.

[27] http://www.ascdi.com/asna/vendors/counterfit_task_force/default.aspx.

[28] http://www.anticounterfeitingforum.org.uk.

[29] http://archive.basel.int/convention/basics.html.

[30] http://www.ier.org.tw/smm/6_PAS_141_2011_Reuse_Of_WEEE_And_UEEE.pdf.

[31] http://www.bbc.co.uk/panorama/hi/front_page/newsid_9483000/9483148.stm.

[32] http://www.bbc.co.uk/news/world-europe-10846395.

[33] *Recycling – From E-Waste to Resources*, PNUE, 2009.

[34] Directive 2002/96/EC.

[35] BSI PAS141:2011, *Reuse of used and waste electrical and electronic equipment* (UEEE et WEEE). Process Management Specification (mars 2011) http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030245346.

[36] http://www.numberingplans.com/?page=analysis&sub=imeinr.

[37] IMEI Allocation and Approval Process, Version 7.0, GSMA, 31 octobre 2013.

[38] http://www.gsma.com/imei-database.

[39] http://www.dailytrust.com.ng/index.php?option=com_content&view=article&id=160408:kenya-to-demobilise-all-fake-phones&catid=1:news&Itemid=2.

[40] Annual Report of the National Commission for the State Regulation of Communications and Informatization for 2012. http://en.nkrzi.gov.ua/1324743665/.

[41] GS1 EPC Tag Data Standard 1.6, 9 Septembre 2011. http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf.

[42] ISO/IEC 15459, *Unique identifiers*.

Part 1:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units*.

Part 2:2006, *Information technology – Unique identifiers – Registration procedures*.

Part 3:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 3: Common rules*.

Part 4:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 4: Individual products and product packages*.

Part 5:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 5: Individual returnable transport items (RTIs)*.

Part 6:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 6: Groupings*.

Part 8:2009, *Information technology – Part 8: Grouping of transport units*.

[43] ISO 6346:1995, *Freight containers – Coding, identification and marking*.

[44] ISO 3779:2009, *Road vehicles – Vehicle identification number (VIN) – Content and structure*.

[45] ISO 10486:1992, *Passenger cars – Car radio identification number (CRIN)*.

[46] ISO 2108:2005, *Information and documentation – International standard book number (ISBN)*.

[47] ISO 3297:2007, *Information and documentation – International standard serial number (ISSN)*.

[48] ISO 12931:2012, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*.

[49] http://www.uidcenter.org/learning-about-ucode.

[50] Recommandation UIT-T X.668 (2008) | ISO/IEC 9834-9:2008, *Technologies de l'information – Interconnexion des systèmes ouverts – Procédures opérationnelles des organismes d'enregistrement de l'OSI: Enregistrement des arcs d'identificateur d'objet pour les applications et services utilisant l'identification à base d'étiquettes.*

[51] Recommandation UIT-T F.771 (2008), *Description et spécifications du service d'accès aux informations multimédias déclenché par l'identification à base d'étiquettes.*

[52] Recommandation UIT-T H.621 (2008), *Architecture du système d'accès aux informations multimédias déclenché par l'identification à base d'étiquettes.*

[53] ISO 28219:2009, *Packaging – Labelling and direct product marking with linear bar code and two-dimensional symbols*.

[54] ISO 22742:2010, *Packaging – Linear bar code and two-dimensional symbols for product packaging*.

[55] ISO 15394:2009, *Packaging – Bar code and two-dimensional symbols for shipping, transport and receiving labels*.

[56] ISO/IEC 15963:2009, *Information technology – Radio frequency identification for item management – Unique identification for RF tags*.

[57] ISO/IEC 29167-1:2014, *Information technology – Automatic identification and data capture techniques – Part 1: Security services for RFID air interfaces*.

[58] ISO/IEC TR 24729-4:2009, *Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security*.

[59] http://www.gs1.org/gsmp/kc/epcglobal.

[60] Recommandation UIT-T X.509 (2012) | ISO/IEC 9594-8:2014, – *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[61] IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[62] IETF RFC 3279 (2002), *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[63] http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Procedures%20and%20Facilitation/safe_package/safe_package_I_2011.pdf.

[64] IEC/TS 62668-1 ed2.0 (2014), *Process management for avionics – Counterfeiting prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*.

[65] IEC/TS 62668-2 ed1.0 (2014), *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources*.

[66] Adapté du règlement (CE) n° 765/2008 concernant la surveillance du marché, art. 2 (17), http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/WP6_2009_13e_final.pdf.

[67] Recommendation M. on the: *Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods.* http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf.

[68] http://www.nia.din.de/gremien/NA+043-01-31+AA/en/54773446.html.

[69] http://www.anticounterfeitingforum.org.uk/best_practice.aspx.

[70] http://www.cti-us.com/CCAP.htm].

[71] http://www.ipo.gov.uk/ipctoolkit.pdf.

[72] http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf.

[73] Etablissement de systèmes de conformité et d'interopérabilité – Principes directeurs de base (UIT, 2014).

[74] Lignes directrices à l'intention des pays en développement relatives à l'installation de laboratoires de tests d'évaluation de la conformité dans différentes régions, UIT, 2012: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf.

[75] IEC 62321:2008, *Electrotechnical products – Determination of levels of six regulated substances (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ethers).*

[76] Recommandation UIT -T E.164 (2010), Plan de numérotage des télécommunications publiques internationales.

[77] ISO/IEC 15962:2013, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions*.

[78] ISO/IEC 15961:2004, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface*.

[79] Recommandation UIT -T X.1255 (2013), *Cadre pour la découverte des informations relatives à la gestion d'identité.*

[80] ISO/IEC 15420:2009, *Information technology – Automatic identification and data capture techniques – EAN/UPC bar code symbology specification*.

[81] ISO/IEC 16388:2007, *Information technology – Automatic identification and data capture techniques – Code 39 bar code symbology specification*.

[82] ISO/IEC 15417:2007, *Information technology -- Automatic identification and data capture techniques – Code 128 bar code symbology specification.*

[83] ISO/IEC 15438:2006, *Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification.*

[84] ISO/IEC 16023:2000, *Information technology – International symbology specification – MaxiCode.*

[85] ISO/IEC 18004:2006, *Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification*.

[86] ISO/IEC 16022:2006, *Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification*.

[87] DIN 66401 (2010), *Unique Identification Mark (UIM)*.

[88] ANSI MH10.8.2-2010, *Data Identifier and Application Identifier Standard*.

[89] ANSI/HIBC 2.3-2009, *The Health Industry Bar Code (HIBC) Supplier*.

[90] ISO/IEC 7816-6:2004, *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange*.

[91] ISO 14816:2005, *Road transport and traffic telematics – Automatic vehicle and equipment identification – Numbering and data structure*.

[92] ANSI INCITS 256-2007, *Radio Frequency Identification (RFID)*.

[93] ANSI INCITS 371.1-2003, *Information technology – Real Time Locating Systems (RTLS) Part 1: 2.4 GHz Air Interface Protocol*.

[94] ISO/IEC 18000-6:2013, *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*.

[95] ISO/IEC 18000-3:2010, *Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz*.

[96] ISO 11784:1996, *Radio frequency identification of animals – Code structure*.

[97] ISO 11785:1996, *Radio frequency identification of animals – Technical concept*.

[98] ISO/IEC 18000 (All Parts), *Information technology – Radio frequency identification for item management*.

[99] ISO 17363:2013, *Supply chain applications of RFID – Freight containers*.

[100] ISO 17364:2013, *Supply chain applications of RFID – Returnable transport items (RTIs) and returnable packaging items (RPIs).*

[101] ISO 17365:2013, *Supply chain applications of RFID – Transport units*.

[102] ISO 17366:20`3, *Supply chain applications of RFID – Product packaging*.

[103] ISO 17367:2013, *Supply chain applications of RFID – Product packaging*.

[104] ISO 18185 (All Parts), *Freight containers – Electronic seals*.

[105] ISO/IEC 29160:2012, *Information technology – Radio frequency identification for item management – RFID Emblem*.

[106] ISO/IEC 15693, *Identification cards – Contactless integrated circuit cards – Vicinity cards*.

[107] ISO 28000:2007, *Specification for security management systems for the supply chain*.

[108] ISO 28001:2007, *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance.*

[109] ISO 28003:2007, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*.

[110] ISO 28004-1:2007, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*.

[111] ISO 28005-2:2011, *Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements.*

[112] SAE AS5553 (2013), *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*.

[113] SAE ARP6178 (2011), *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*.

[114] SAE AS6081 (2012), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors.*

[115] SAE AS6171 (2010), *Test Methods Standards; Counterfeit Electronic Parts*.

[116] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.

[117] IDEA-STD-1010A (2006), *Acceptability of Electronic Components Distributed in the Open Market*.

[118] IDEA-QMS-9090 (2013), *Quality Management System Standard*.

Glossaire

AC	Classe d'attribution (*allocation class*)
ADI	Code d'identification aérospatiale et défense (*aerospace and defence identifier*)
AIDC	Identification et captage de données automatiques (*automatic identification and data capture*)
ALE	Evénements reçus au niveau de la couche d'application (*application layer event*)
AMRC	Système d'accès multiple par répartition en code
AWP	Automated Working Place
CB	Organisme de certification (*certification body*)
CBV	Vocabulaire normalisé (*core business vocabulary*)
cc	Code de classe
CD	Disque compact (*compact disc*)
CDR	Relevé détaillé des communications (*call detail record*)
CEIR	Registre central d'identités d'équipements (*central equipment identity register*)
CEM	Compatibilité électromagnétique
CI	Circuit intégré
CIPS	Système global de protection des informations (*comprehensive information protection system*)
CMS	Composants montés en surface
CoPC	Certification de compétence de personnes (*certification of personnel competencies*)
DB	Bases de données (*database*)
DCI	Configuration et initialisation de découverte (*discovery, configuration and initialisation*)
DNS	Système des noms de domaine (*domain name system*)
DPI	Droits de propriété intellectuelle
DVD	Disques numériques polyvalents (*digital versatile disc*)
EIR	Registre d'identités d'équipements (*equipment identity register*)
EPC	Code produit électronique (*electronic product code*)
EPCIS	Services d'informations sur les EPC (*epc information service*)
GDTI	Code international d'identification d'un type de document (*global document type identifier*)
GIAI	Code international d'identification des actifs (*global individual asset identifier*)
GID	Identifiant général (*general identifier*)
GII	Programme d'implantation de numéros IMEI authentiques (*genuine imei implant programme*)
GINC	Code international d'identification d'un groupement d'unités logistiques (*global identification number for consignment*)

GLN	Code lieu-fonction international (*global location number*)
GRAI	Code d'identification des supports réutilisables (*global returnable asset identifier*)
GSIN	Code international d'identification d'une expédition (*global shipment identification number*)
GSM	Système mondial de communications mobiles (*global system for mobile communications*)
GSRN	Code international d'identification d'une relation de service (*global service relation number*)
GT	Groupe de travail
GTIN	Code article international (*global trade item number*)
HF	Haute fréquence (*high frequency*)
ic	Code d'identification d'objets individuels (*identification code*)
ID	Identifiant (*identification*)
IMEI	Identité internationale d'équipement mobile (*international mobile equipment identity*)
IP	Propriété intellectuelle (*intellectual property*)
IP	Protocole Internet (*Internet protocol*)
IPM	Interface public membres (*interface public-members*)
ISBN	International Standard Book Number
ISSN	International Standard Serial Number
IT	Technologies de l'information (*information technology*)
LLRP	Low Level Reader Protocol
LTE	Evolution à long terme (*long-term evolution*)
ME	Identifiant du type d'équipement mobile (*mobile equipment*)
MEID	Identifiants d'équipement mobile (mobile equipment identity)
MIIM	Gestion et identification d'élément mobile (*mobile item identification and management*)
MRA	Accords de reconnaissance mutuelle (*mutual recognition agreement*)
MSC	Mobile Switching Centre
MSISDN	Mobile Subscriber Integrated Services Digital Network
NIR	Niveaux d'exposition aux rayonnements non ionisants (*non-ionizing radiation*)
OID	Identificateur d'objet (*object identifier*)
ONS	Service de nommage d'objets (*object naming service*)
QoS	Qualité de service
RF	Radiofréquences
RFID	Identification par radiofréquences (*radio frequency identification*)
RM	Gestion des lecteurs (*reader management*)
RoHS	Restriction of Hazardous Substances

RP	Protocole lecteur (*reader protocol*)
RUIM	Module d'identité d'utilisateur amovible (*removable user identity module*)
SFP	Réseau mondial de fournisseurs de fonctionnalités de sécurité (security features provider)
SGLN	Numéro de série international de localisation avec ou sans extension (*global location number with or without extension*)
SGTIN	Numéro international d'identification commerciale de série (*serialized global trade item number*)
SIM	Module d'identité de l'abonné mobile (*subscriber identity module*)
SLDc	Code domaine de deuxième niveau (*second level domain code*)
SMS	Short Message Service
SNMP	Protocole simple de gestion de réseau (*simple network management protocol*)
SS7	Système de signalisation N°°7
SSCC	Code de colis de série (*serial shipping container code*)
TAC	Code d'attribution type (*type allocation code*)
TC	Comité technique (*technical committee*)
TDS	Norme relative aux données des étiquettes (*tag data standard*)
TDT	Traduction de données des étiquettes (*tag data translation*)
TIC	Technologies de l'information et de la communication
TID	Etiquette d'identification (*tag id*)
TLDc	Code domaine de premier niveau (*top level domain code*)
TV	Télévision
UHF	Ondes décimétriques (*ultra high frequency*)
UII	Identificateur d'article unique (*unique item identifier*)
UIM	Marque d'identification unique (*unique identification mark*)
UMTS	Système de télécommunications mobiles universelles (*universal mobile telecommunications system*)
UPC	Code produit universel (universal product code)
URL	Localisateur uniforme de ressource (*uniform resource locator*)
USB	Bus série universel (*universal serial bus*)

Annexe A

Systèmes d'identification des dispositifs mobiles de contrefaçon

Comme nous l'avons vu précédemment dans le présent rapport technique, la contrefaçon de dispositifs mobiles est un problème particulièrement préoccupant et diverses initiatives ont été prises pour en endiguer la progression. Le but de certains systèmes d'identification était au départ de s'assurer que les dispositifs mobiles étaient importés conformément aux procédures juridiques (et non pas en contrebande) et, par la suite, d'établir avec certitude qu'ils n'étaient pas contrefaits. Ces systèmes présentent en outre un grand nombre de caractéristiques communes avec les initiatives spécialement conçues pour remédier au problème de la contrefaçon, par exemple ceux qui reposent sur l'authentification d'un identificateur unique (numéro IMEI).

On trouvera dans les paragraphes qui suivent quelques exemples de mesures prises actuellement par des autorités nationales ainsi qu'au niveau régional.

A.1 Exemple de mesures prises par des administrations et des autorités de régulation nationales

A.1.1 Azerbaïdjan

Le système d'enregistrement des dispositifs mobiles (MDRS) http://www.rabita.az/en/c-media/news/details/134 a été mis en place au sein du Centre ICC (Information Computer Centre) du Ministère des communications et des technologies de l'information, conformément aux "Règles applicables à l'enregistrement des dispositifs mobiles" approuvées en vertu de la décision N° 212, datée du 28 décembre 2011, du Conseil des ministres de la République d'Azerbaïdjan.

L'objectif de l'enregistrement des dispositifs mobiles est d'empêcher l'importation de dispositifs de mauvaise qualité et d'origine inconnue qui ne satisfont pas aux normes techniques requises, par exemple celles qui visent à limiter l'émission de rayonnements électromagnétiques nocifs, et à accroître la visibilité ainsi que la compétitivité des équipementiers. Le système d'enregistrement empêche l'utilisation des dispositifs mobiles perdus ou volés ainsi que ceux qui sont importés illégalement dans le pays.

Depuis le 1er mars 2013, les opérateurs mobiles introduisent chaque jour dans un système de base de données centralisé les numéros IMEI des dispositifs mobiles utilisés en Azerbaijan. Le Ministère des communications et des technologies de l'information a répertorié plus de 12 millions de dispositifs GSM enregistrés après le lancement du système MDRS. Quelque 300 000 dispositifs non conformes aux normes peuvent continuer à fonctionner avec leurs numéros de téléphone mobile actuels, mais les nouveaux dispositifs qui ne répondent pas aux normes ne seront pas utilisables dans le pays. http://www.mincom.gov.az/media-en/news-2/details/1840.

Les numéros IMEI de tous les dispositifs mobiles utilisés dans le réseau avant le 1er mai 2013 ont été considérés comme enregistrés et fonctionnent donc librement dans les réseaux. Après le lancement du système d'enregistrement, le numéro IMEI de chaque dispositif mobile importé dans le pays à usage privé (avec une carte SIM par l'un des opérateurs mobiles nationaux) doit être enregistré dans un délai de 30 jours à compter de la date de son raccordement au réseau. Cette règle ne s'applique pas aux dispositifs mobiles en itinérance utilisant des cartes SIM fournies par des opérateurs étrangers.

Les abonnés peuvent déterminer si leurs dispositifs sont autorisés à partir de leurs numéros IMEI, en utilisant une page web spéciale (imei.az) ou des messages SMS.

Le système de base de données centralisé a été mis en place au sein du Centre ICC (Information Computer Centre) du Ministère des communications et des technologies de l'information; parallèlement, les opérateurs mobiles ont installé les équipements appropriés, qui sont synchronisés avec la base de données centrale. Le logiciel utilisé pour le système MDRS a été conçu par des spécialistes du pays.

A.1.2 Brésil

SIGA – Système intégré de gestion des dispositifs

En vertu du règlement applicable aux services mobiles de l'Agence nationale des télécommunications du Brésil (Anatel), les opérateurs ne doivent admettre sur leurs réseaux que les dispositifs certifiés par Anatel et les utilisateurs ne doivent utiliser que ces dispositifs (Article 8, IV et Article 10, V du règlement applicable aux services approuvé conformément à la Résolution 477/2007[9]). Sur la base de cette réglementation, Anatel a demandé aux opérateurs mobiles brésiliens de mettre en place conjointement une solution technique destinée à freiner l'utilisation des dispositifs mobiles non certifiés, volontairement altérés ou dont les numéros IMEI ont été clonés.

Le plan d'action soumis par les opérateurs en vue de satisfaire à cette obligation définissait les grandes lignes de la solution technique à mettre en oeuvre, les critères susceptibles d'être utilisés sur la base d'utilisateurs réels, afin d'atténuer le plus possible les conséquences pour la population, ainsi que les critères applicables aux nouveaux utilisateurs après que la solution sera opérationnelle, de façon que seuls les dispositifs conformes au règlement d'Anatel puissent accéder au réseau. Des critères ont également été définis à l'usage des utilisateurs mobiles, afin d'éviter tout désagrément pour les utilisateurs nationaux ou étrangers, et des campagnes de sensibilisation ont été organisées à l'intention des utilisateurs du réseau mobile.

Le plan d'action a été approuvé par Anatel en 2012, compte tenu des aspects techniques et réglementaires. La solution, baptisée SIGA (Système intégré de gestion des dispositifs) est actuellement mise en place sur la base des hypothèses techniques suivantes:

- solution centralisée élaborée conjointement par tous les opérateurs mobiles brésiliens;
- solution intégrée avec les opérateurs de plates-formes mobiles;
- solution automatisée permettant de saisir des informations moyennant une intervention humaine limitée;
- solution évolutive et extensible en fonction de la croissance et de la complexité;
- solution dynamique et souple, les règles pouvant être adaptées dans le temps;
- solution comprenant plusieurs sources d'information, par exemple les relevés détaillés des communications (CDR, call detail record), et associant les opérateurs de systèmes de gestion, y compris l'utilisation de bases de données internationales, selon le cas;
- solution efficace pour que des mesures puissent être prises afin de réduire l'utilisation des dispositifs illicites;
- solution devant permettre de limiter autant que possible les incidences potentielles sur les utilisateurs finals ordinaires;
- solution fiable et sécurisée.

[9] http://legislacao.anatel.gov.br/resolucoes/2007/9-resolucao-477.

A l'heure actuelle, l'exploitation technique du système SIGA est assurée par ABR Telecom[10], association technique créée en tant que coentreprise, qui réunit la plupart des opérateurs de télécommunication brésiliens, en vue d'élaborer, de déployer et d'exploiter des solutions techniques centralisées pour le marché des télécommunications du Brésil.

Ce projet repose sur une étroite interaction avec les autres parties concernées – par exemple Anatel, les autorités douanières, l'Association des opérateurs (SindiTelebrasil), les opérateurs, les équipementiers, l'Union des fabricants (ABINEE) et ABR Telecom, de manière à garantir le succès du système SIGA. Le problème est néanmoins complexe, étant donné qu'il concerne tous les domaines d'activité d'un opérateur, plusieurs acteurs du marché ainsi que l'utilisateur final. Il faut donc procéder à un examen approfondi de toutes les mesures nécessaires.

Le système SIGA, en service sur le réseau des opérateurs depuis mars 2014, permet de recueillir les renseignements nécessaires pour analyser la taille du marché des dispositifs non conformes à la réglementation du Brésil, afin que toutes les parties concernées puissent définir les mesures à prendre afin de garantir que ces dispositifs contrefaits, de qualité médiocre et non autorisés soient supprimés du réseau avec le minimum de conséquences pour le consommateur.

L'une des mesures envisageables actuellement à l'étude pour satisfaire ces conditions consiste à créer une base de données des anciens dispositifs recensant tous les cas (relation unique entre un terminal et ses utilisateurs) autorisés à continuer de fonctionner sur le réseau, mais à bloquer l'accès au réseau de tous les nouveaux terminaux illicites. Les conséquences pour l'utilisateur s'en trouvent ainsi considérablement réduites et la base de données des anciens dispositifs devrait disparaître au fur et à mesure de leur remplacement.

En outre, il est important d'associer aux discussions les entités qui représentent les utilisateurs et de mettre en oeuvre un plan de communication bien conçu, avant de prendre des mesures susceptibles d'influer directement sur l'utilisateur (blocage ou suspension du dispositif par exemple).

Dans cette optique, le plan de communication SIGA est actuellement élaboré par les opérateurs, Anatel, et l'Union des fabricants. Ce plan devrait être mis en place par toutes ces entités, dans le cadre d'une action concertée, sur tous les circuits de consommation (annonces publicitaires, factures des opérateurs et centres d'appels par exemple), en attirant l'attention des utilisateurs sur les avantages de l'achat de terminaux certifiés ainsi que sur les risques qu'ils prennent lorsqu'ils utilisent des terminaux contrefaits et de qualité médiocre sur le marché brésilien.

Des renseignements détaillés sur les aspects techniques de ce projet peuvent être obtenus directement auprès de l'Agence nationale des télécommunications (Anatel) de l'Administration brésilienne[11].

A.1.3 Colombie

En 2011, le Ministère des technologies de l'information et de la communication a pris le décret 1630, afin de mettre en place des mécanismes destinés à limiter la commercialisation et la vente de terminaux, nouveaux ou usagés, et à créer deux types de bases de données centralisées: la première comporte un registre des numéros IMEI de terminaux ayant fait l'objet d'une déclaration de vol ou de perte, qui vise à en empêcher l'utilisation ou l'activation, et la seconde comprend un registre dans lequel sont consignés les numéros IMEI des terminaux importés ou fabriqués légalement dans le pays et associés à un numéro d'identification du propriétaire ou de l'abonné.

La Loi 1453 du 24 juin 2011, relative à la sécurité des citoyens, contient une disposition prévoyant des peines d'emprisonnement allant de 6 à 8 ans pour les personnes qui altèrent volontairement,

---

[10] http://www.abrtelecom.com.br.

[11] prre@anatel.gov.br.

reprogramment, renomment ou modifient le numéro IMEI d'un dispositif mobile, ainsi que pour les personnes qui activent des dispositifs ayant fait l'objet d'une déclaration de vol. En outre, les équipements altérés sont confisqués http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf.

Ces initiatives ont été prises afin de limiter la vente et l'utilisation de dispositifs mobiles volés, mais devraient également avoir une incidence sur l'utilisation des produits de contrefaçon.

A.1.4 Egypte

En 2008, l'Autorité nationale de régulation des télécommunications (NTRA) a créé un département de surveillance du marché, afin de promouvoir ses activités d'homologation. En 2010, l'Egypte s'est dotée d'un système de lutte contre l'utilisation des équipements terminaux mobiles de contrefaçon. Ce système utilise les bases de données relatives aux codes IMEI de la GSMA pour obtenir une mise à jour hebdomadaire de la liste blanche de codes TAC IMEI ainsi qu'un registre central d'identités d'équipement (EIR) (base de données IMEI). Cette solution avait pour but de limiter l'utilisation des combinés dotés de numéros illicites, faux, non valables et clonés, à lutter contre le vol de combinés et à répondre aux préoccupations en matière de santé et de sécurité.

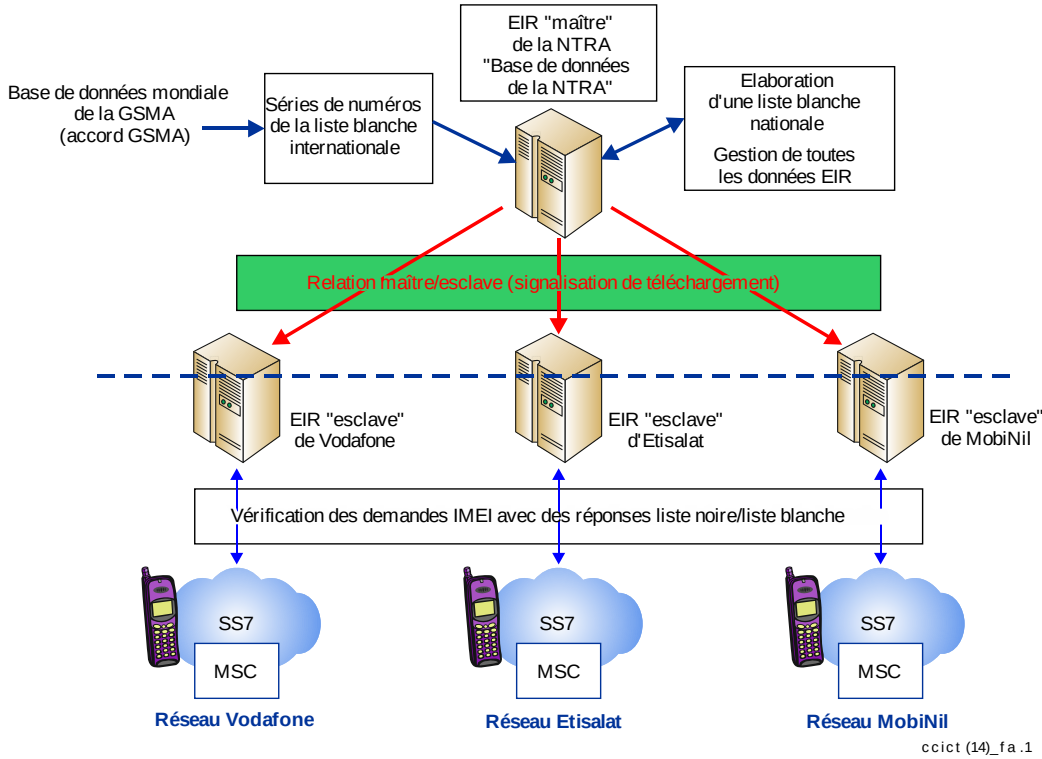


Figure A.1 – Solution de base de données centrale EIR IMEI en Egypte

D'après la NTRA, on recensait 3,5 millions de combinés mobiles avec le code IMEI illégal 13579024681122, 250 000 combinés avec des numéros IMEI clonés, 500 000 combinés avec de faux numéros IMEI, 350 000 combinés avec des numéros IMEI affichant uniquement des zéros et 100 000 combinés sans code IMEI. http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/CI_Forum_Tunis_2012_Report.pdf.

En février 2010, la NTRA a annoncé que les trois opérateurs mobiles nationaux allaient bloquer les services destinés à tous les utilisateurs anonymes ainsi que les téléphones cellulaires sans code IMEI sur le marché égyptien. http://www.cellular-news.com/story/42911.php.

A.1.5 Indonésie

L'Indonésie a durci les conditions régissant l'importation de téléphones cellulaires en janvier 2013, en imposant des procédures techniques et des normes à respecter, des restrictions à la distribution ainsi que des restrictions portuaires, des mesures de contrôle avant expédition ainsi qu'une obligation de préenregistrement de numéros IMEI avant l'importation. Ces prescriptions font l'objet du décret N° 81/2012 du Ministère de l'industrie et du décret N° 82/2012 du Ministère du commerce. http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151703.pdf.

A.1.6 Kenya

A.1.6.1 Introduction

Selon l'Agence anti-contrefaçon (ACA) du Kenya, la concurrence déloyale entre produits de contrefaçon et produits authentiques coûterait chaque année aux milieux d'affaires (fabricants locaux, investisseurs et innovateurs) 50 milliards Sh. (soit environ 596 millions USD), faisant ainsi peser sur de nombreuses entreprises une menace de fermeture ou de relocalisation. Pour les gouvernements et l'économie, le manque à gagner imputable à la contrefaçon s'établirait, d'après les estimations, à plus de 19 milliards Sh. (soit environ 227 millions USD) par an en raison de l'évasion fiscale.http://www.aca.go.ke/index.php?option=com_docman&task=doc_download&gid=20&Itemid=471.

Les médicaments, les produits électroniques, les CD et les logiciels piratés, les boissons alcooliques, les téléphones mobiles et les produits agricoles figurent au nombre des produits les plus touchés.

La Commission des communications du Kenya, instituée en vertu de la Loi du Kenya sur l'information et les communications (Cap 411A), a pour mandat de délivrer des licences pour les services d'information et de communication et de réguler ces services. Aux termes de l'Article 25 de ladite Loi, la Commission est habilitée à octroyer des licences pour l'exploitation et la fourniture de systèmes et de services de télécommunication, sous réserve de certaines conditions. L'une des conditions à satisfaire au titre de ces licences est d'homologuer les équipements de communication, afin de vérifier qu'ils sont compatibles avec les réseaux publics de communication. Dans ce contexte, en vertu du Règlement 3 de la Loi du Kenya sur l'information et les communications (importation, homologation et distribution des équipements de communication) de 2010, tous les combinés téléphoniques mobiles doivent être homologués par la Commission avant d'être raccordés aux réseaux publics http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf.

L'objectif fondamental du processus d'homologation est avant tout de protéger le public contre les effets négatifs que peuvent avoir les téléphones mobiles de contrefaçon ou de qualité médiocre, notamment sur le plan technique et économique et sur celui de la santé et de la sécurité. On trouvera au paragraphe A.1.6.2 des renseignements complémentaires sur les problèmes que pose la contrefaçon de combinés dans le secteur des TIC. Un appareil mobile dépourvu d'identité internationale d'équipement mobile (IMEI) appropriée ne peut être homologué.

C'est pour ces raisons que l'utilisation des dispositifs téléphoniques mobiles de contrefaçon doit être progressivement supprimée, mais il faudra pour ce faire tenir dûment compte des intérêts de toutes les parties prenantes. En conséquence, cette suppression s'effectuera progressivement jusqu'au 30 septembre 2012, date à laquelle les téléphones mobiles de contrefaçon seront déconnectés par les autorités kenyannes.

Afin de veiller à ce que les intérêts et les préoccupations des parties prenantes soient pris en considération, la Commission organise, depuis octobre 2011, une série de consultations ouvertes entre les acteurs du secteur des TIC, divers organismes publics et d'autres parties prenantes, en vue de remédier aux problèmes que pose la contrefaçon des téléphones mobiles pour les professionnels du secteur et l'économie dans son ensemble. A l'issue de ces consultations, des mesures concrètes ont été approuvées pour faire face à ce problème.

Au nombre des mesures adoptées figure l'organisation par la Commission d'une campagne de sensibilisation du public destinée à informer les abonnés des effets négatifs des appareils de contrefaçon; l'établissement d'un système qui sera utilisé par le public pour déterminer si les combinés qu'ils possèdent sont authentiques; la mise en place de systèmes permettant de bloquer les téléphones de contrefaçon dans les réseaux mobiles et la fourniture de services d'assistance à la clientèle.

Autre initiative importante: l'adoption, par tous les organismes publics concernés, de mesures de surveillance et de mesures restrictives en ce qui concerne les dispositifs mobiles de contrefaçon. Un système de vérification des combinés avec accès à la base de données GSMA a été créé, pour permettre aux abonnés de vérifier la validité de leur téléphone par l'intermédiaire des numéros IMEI soumis. De plus, on a mis en oeuvre un système permettant de bloquer les combinés de contrefaçon dans les réseaux mobiles.

Grâce à ces activités, le Kenya a progressivement supprimé 1,89 million de téléphones mobiles contrefaits après le 30 septembre 2012.

A.1.6.2 Retrait progressif des combinés téléphoniques mobiles contrefaits

1) Considérations générales

a) Mise en oeuvre d'un système de registre des identités d'équipements (EIR)

L'utilisation des téléphones mobiles au Kenya, loin d'être un luxe, est aujourd'hui une nécessité, comme en atteste l'accroissement du nombre d'abonnés, qui s'élève actuellement à environ 29,2 millions. Cependant, la mise en oeuvre de services de communication mobiles se heurte au problème du vol de téléphones mobiles et à l'augmentation du nombre de délits commis à l'aide de mobiles, ce qui fait peser des risques considérables sur la sécurité.

Pour parer à ces menaces, la Commission a procédé, en 2001, à une série de consultations avec les opérateurs mobiles en place titulaires de licence, en vue de trouver une solution durable au problème. Dans l'intervalle, l'Organisation des communications de l'Afrique de l'Est (EACO) a adopté une résolution en vertu de laquelle il a notamment été demandé aux régulateurs et aux opérateurs de la région de réfléchir à la façon de contrôler au mieux le vol de combinés mobiles à l'intérieur de la région.

Au cours de ces consultations, il a été noté que la caractéristique inhérente aux réseaux mobiles, à savoir le "registre des identités d'équipements", (EIR) offrait un moyen de faire face au problème du vol des téléphones mobiles. Le registre EIR peut vérifier le numéro international d'identité unique de l'équipement mobile (IMEI) de chaque téléphone ayant accès au réseau mobile et tenir un registre de ces mêmes numéros. Ces renseignements seront ensuite mis à la disposition des autorités qui en ont besoin, dans la mesure du possible.

A cette fin, un mémorandum d'accord (MOU) a été conclu entre tous les opérateurs mobiles au sujet de la mise en oeuvre du système EIR, mémorandum, qui ouvrira la voie à la mise en oeuvre du système au niveau régional. Il a également été noté que l'existence de combinés mobiles de

contrefaçon, qui comprennent le plus souvent des numéros IMEI en double ou de faux numéros IMEI, risque de conduire à une situation où lorsqu'un tel dispositif acquis de manière illégale est suivi et désactivé au moyen du système EIR, plusieurs autres combinés dotés de numéros IMEI analogues seront eux aussi vraisemblablement désactivés.

C'est dans ce contexte qu'est apparue la nécessité de remédier au problème de la présence de combinés de contrefaçon sur le marché avant la mise en oeuvre intégrale du système EIR, car ce système ne sera efficace que si les combinés de contrefaçon sont supprimés, comme cela est préconisé sur le plan international.

b) Mise en oeuvre du cadre juridique et réglementaire concernant les combinés mobiles

i) Cadre juridique et réglementaire

Du point de vue du secteur des communications, le cadre juridique et réglementaire régissant les combinés est l'Article 25 de la Loi du Kenya sur l'information et les communications – Cap 4II A. En vertu des licences octroyées au titre de cette Loi, les titulaires de licences ne peuvent offrir de services qu'à ceux qui utilisent un appareil homologué.

En outre, conformément au Règlement du Kenya sur l'information et les communications (importation, homologation et distribution des équipements de communication) de 2010, il est expressément prévu que tous les combinés doivent être homologués. Il est important de noter que conformément aux dispositions de la Commission en matière d'homologation, un combiné GSM dépourvu d'un numéro IMEI valable ou dont le numéro IMEI a été falsifié ne peut être homologué. De ce fait, tous les combinés sans numéro IMEI valable ou comportant un numéro IMEI cloné sont par nature illicites, de sorte que leur utilisation sera contraire à la Loi précitée.

ii) Directive récente de la Commission et réaction des opérateurs

En mai 2011, la Commission a demandé à tous les opérateurs de réseaux mobiles de retirer progressivement les combinés de contrefaçon de leurs réseaux avant le 30 septembre 2011. Cette directive allait dans le sens des textes législatifs régissant le secteur des communications.

2) Consultations avec le secteur privé

Dès qu'ils ont pris connaissance de cette directive, les acteurs du secteur des communications mobiles ont demandé un réexamen de la directive en question, faisant valoir qu'un grand nombre d'abonnés utilisaient des téléphones comportant le même numéro IMEI ou un numéro IMEI défectueux. En outre, les opérateurs craignaient que la déconnexion de plus de deux millions de combinés de contrefaçon en service n'ait des conséquences défavorables sur leurs recettes.

Pour assurer l'application de la directive moyennant un minimum d'interruptions de service, la Commission a créé un Comité ouvert, composé principalement de représentants d'opérateurs mobiles, des ministères et d'organes publics concernés, d'équipementiers, de fournisseurs et de la société civile.

La série de consultations entre les professionnels du secteur des TIC et divers organismes publics doit également permettre de résoudre les problèmes que pose la contrefaçon des téléphones mobiles pour les entreprises et l'économie dans son ensemble. L'Association GSM (GSMA) a souligné que le marché des téléphones volés en Europe, ou provenant purement et simplement de la contrefaçon, était relativement important au Kenya. Forte de l'expérience qu'elle a acquise au niveau international pour contrer ce phénomène, la GSMA a grandement contribué au processus mis en oeuvre au Kenya, en fournissant des avis dans le cadre de plusieurs missions techniques. A ce jour, il a été décidé au titre de ces consultations d'agir concrètement en faveur de l'initiative.

Pour l'essentiel, la Commission a organisé une campagne visant à sensibiliser le public aux effets négatifs des dispositifs de contrefaçon, et les fabricants de téléphones mobiles se sont engagés à mettre en place un système qui sera utilisé par le public pour déterminer si leurs téléphones sont authentiques ou non. En outre, les opérateurs de réseaux ont mis sur pied des systèmes permettant de bloquer les dispositifs de contrefaçon dans leurs réseaux et de fournir des services d'assistance à la clientèle. Pour leur part, les organismes publics ont intensifié leurs activités de surveillance et pris des mesures énergiques pour lutter contre la contrefaçon de téléphones mobiles.

L'organisation de cette campagne de sensibilisation du public est allée de pair avec l'établissement d'un système de vérification des combinés donnant accès à la base de données de la GSMA, qui permet aux abonnés de vérifier la validité de leur téléphone grâce à un numéro IMEI notifié. http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf.

A.1.7 Rwanda

L'Agence rwandaise de régulation des services d'utilité publique (RURA) a annoncé qu'elle se proposait d'interdire l'importation de dispositifs mobiles contrefaits au Rwanda en 2013, sans toutefois bloquer les dispositifs de contrefaçon déjà en service. http://www.newtimes.co.rw/news/views/article_print.php?i=15290&a=64650&icon=Print. Au Rwanda, un autre problème tient au fait que certains téléphones de contrefaçon réacheminent les appels à destination des codes courts harmonisés de l'Organisation des communications de l'Afrique de l'Est (EACO) 100 (service à la clientèle), 101 (recharge en Tanzanie) et 102 (vérification des factures en Tanzanie) à 112 (services d'urgence, police). La RURA a donc été amenée à réattribuer temporairement un code court différent pour le service d'information à la clientèle http://www.eaco.int/docs/19_congress_report.pdf.

A.1.8 Sri Lanka

En Mars 2013, la Commission de régulation des télécommunications du Sri Lanka (TRCSL) a lancé un appel à déclaration d'intérêt en vue de "concevoir, de développer et d'installer un Registre central d'identités d'équipements (CEIR) pour les réseaux mobiles du Sri Lanka". http://www.trc.gov.lk/images/pdf/eoi_ceir_07032013.pdf.

Afin de réduire l'importance du marché de la contrefaçon de téléphones mobiles, de décourager le vol de téléphones mobiles et de protéger les intérêts des consommateurs, la TRCSL projette de mettre en place un Registre central d'identités d'équipements (CEIR) qui est connecté aux Registres EIR de tous les opérateurs mobiles. Le CEIR fait fonction de système central pour tous les opérateurs de réseaux et leur permet d'obtenir des renseignements sur les terminaux mobiles à proscrire: ainsi, les dispositifs placés sur une liste noire dans un réseau ne pourront pas fonctionner sur d'autres réseaux, même en cas de changement de la carte SIM (module d'identité de l'abonné mobile) du dispositif.

Conformément aux prescriptions imposées par la TRCSL, le CEIR doit assurer les fonctions suivantes:

i) Capacité de tenir à jour la base de données de numéros IMEI de tous les dispositifs enregistrés sur les réseaux mobiles.

ii) Capacité d'identifier les numéros IMEI:

   a) non attribués;

   b) non valables, en double ou exclusivement constitués de zéros.

iii) La base de données CEIR doit contenir les renseignements suivants sur les dispositifs enregistrés auprès de tous les réseaux mobiles du Sri Lanka:

a) numéros IMEI;

b) statut du numéro IMEI (blanc, gris, noir);

c) date de création de l'enregistrement;

d) date de mise à jour du dernier enregistrement;

e) numéro de modèle du dispositif;

f) motif du statut du numéro IMEI (non valable, volé, cloné, valable).

iv) Capacité de bloquer les services destinés aux abonnés disposant d'appareils enregistrés avec numéros IMEI non valables ou placés sur une liste noire.

v) Capacité d'identifier le modèle et la version du dispositif ainsi que d'autres renseignements.

vi) Permettre la création d'un nouvel enregistrement dans la base de données contenant les numéros IMEI, chaque fois qu'un nouveau compte d'abonné est activé.

vii) Mise à disposition des informations actualisées de la base de données contenant les listes noire/blanche/grise des opérateurs, de façon à empêcher le clonage dans l'ensemble des réseaux et à tenir à jour les renseignements figurant dans la base de données.

viii) Mise à jour périodique de la base de données de numéros IMEI sur la base des renseignements les plus récents relatifs aux assignations de numéros IMEI valables, à l'aide des méthodes disponibles les plus efficaces.

ix) Capacité d'identifier les numéros IMEI contrefaits, en les comparant avec ceux fournis par la GSMA.

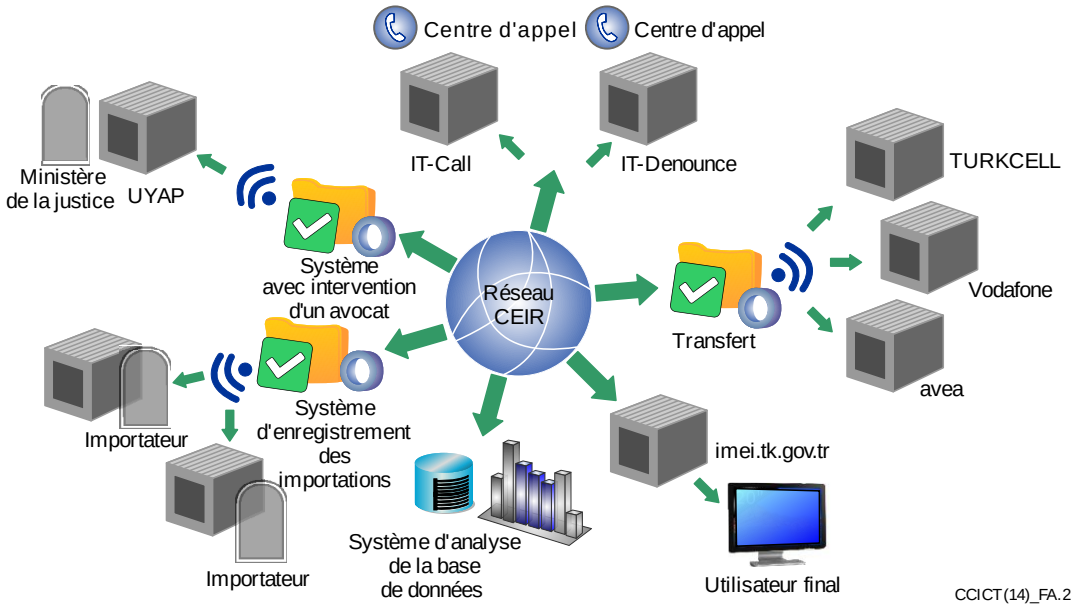
x) Capacité d'interfonctionnement avec tous les éléments de réseau et toutes les interfaces appropriés des opérateurs mobiles.

xi) La base de données du CEIR utilisera une méthode d'entrée souple (saisie manuelle des données, fichiers plats contenant des mises à jour des séries de numéros IMEI).

xii) Vérification par le CEIR du format des numéros IMEI, pour vérifier la validité de ce format et de la série.

A.1.9 Turquie

En 2006, l'Autorité des technologies de l'information et de la communication (ICTA) de la Turquie a créé un Registre central d'identités d'équipements (CEIR) pour empêcher l'utilisation de téléphones mobiles non enregistrés, la perte de recettes fiscales, la concurrence déloyale dans le secteur, le piratage et l'automatisation des processus d'importation. Cette infrastructure a été mise en place pour freiner l'importation illégale de dispositifs et déconnecter du réseau hertzien les dispositifs entrés en contrebande, perdus ou volés, ou encore ceux portant des numéros IMEI clonés.



https://www.icta.mu/mediaoffice/publi.htm

Figure A.2 – Structure du Registre central d'identités d'équipements

En vertu de la Loi sur les radiocommunications, les numéros IMEI sont classés de la façon suivante:

- Liste blanche: comprend les numéros IMEI des dispositifs enregistrés et dont les informations d'identité électronique n'ont pas été modifiées.
- Liste noire: comprend les numéros IMEI entrant dans la catégorie des dispositifs manquants ou volés et dont les informations d'identité électronique ont été modifiées. Les opérateurs de télécommunication sont habilités à supprimer l'accès de ces dispositifs aux communications hertziennes.
- Liste grise: comprend les numéros IMEI qui ne font pas partie de la liste blanche ou de la liste noire et qui ont accès aux communications hertziennes. Les opérateurs de télécommunication sont tenus d'analyser les données détaillées des appels provenant de ces dispositifs et d'informer l'ICTA. Ils doivent aussi informer les utilisateurs de ces dispositifs, en leur envoyant un message texte selon lequel leur dispositif ne figure pas sur la liste blanche.
- Liste blanche adaptée: comprend les numéros IMEI qui sont des "clones" des dispositifs avec numéros RNIS d'abonné mobile (MSISDN) d'utilisateurs ayant versé un droit d'enregistrement. On trouve également dans cette liste les dispositifs ayant fait l'objet d'un contrat d'abonnement avec un opérateur de télécommunication et utilisés momentanément en Turquie avec le numéro MSISDN.

D'après le rapport annuel 2010 de l'ICTA, on recensait fin 2010 131 836 847 numéros IMEI enregistrés légalement et 14 308 239 numéros IMEI figurant sur la liste noire des numéros IMEI pour diverses raisons: perte, contrebande, vol et clonage.
https://www.icta.mu/mediaoffice/publi.htm.

A.1.10 Ouganda

La Commission des communications de l'Ouganda (UCC) a lancé un projet visant à supprimer progressivement les téléphones de contrefaçon du marché national http://ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES.html. Il ressort d'une étude certifiée par l'UCC que près de 30% des téléphones mobiles en vente sur le marché ougandais sont des faux. Cette étude montre également que les pertes fiscales de l'Etat dues à la revente de téléphones mobiles faux ou contrefaits s'élevaient à environ 15 milliards Schilling (soit 5 400 millions USD en novembre 2014). http://www.monitor.co.ug/Business/Commodities/Survey+finds+30++of+Ugandan+phones+fake/-/688610/1527408/-/elvou8z/-/index.html.

En décembre 2012, l'UCC a publié un document consultatif intitulé "Echéances et répartition des tâches pour la suppression des téléphones mobiles de contrefaçon", qui définit le projet et les quatre phases de mise en oeuvre suivantes: http://www.ucc.co.ug/files/downloads/Counterfeit%20phones%20Consultative%20Document.pdf.

PHASE 1: Vérification des téléphones mobiles

Pendant cette phase, les clients pourront vérifier le statut de leur téléphone en utilisant les applications Internet, les applications SMS ou ces deux applications.

Il est conseillé aux consommateurs de vérifier immédiatement si leurs téléphones mobiles sont licites en ayant recours à l'une des deux solutions décrites ci-dessus.

PHASE 2: Déni de service pour les nouveaux téléphones contrefaits

Au cours de cette phase, les nouveaux téléphones mobiles contrefaits pour lesquels aucun abonnement n'a été souscrit auprès d'un opérateur de réseau se verront refuser l'accès à tous les réseaux. La date proposée de mise en oeuvre de cette phase était le 31 janvier 2013.

PHASE 3: Déconnexion de tous les téléphones mobiles contrefaits

Lors de cette phase, tous les téléphones mobiles contrefaits, y compris ceux pour lesquels un abonnement a déjà été souscrit auprès d'un opérateur de réseau, seront déconnectés. La date proposée de mise en oeuvre de cette mesure était le 1er juillet 2013.

PHASE 4: Bilan du projet

Durant cette phase, la Commission examinera les résultats de la mise en oeuvre du projet et les questions relatives à la gestion des déchets d'équipements électriques et électroniques et au clonage des numéros IMEI. Les propositions relatives à l'examen de divers problèmes pendant cette phase sont encore à l'étude.

A.1.11 Ukraine

A.1.11.1 Introduction

En 2008, le problème immédiat le plus urgent à résoudre était l'importation de terminaux mobiles de contrebande, qui représentaient 93% à 95% du marché. Ces combinés d'origine inconnue ne répondaient pas, pour la plupart, aux normes de l'Ukraine, tant sur le plan des caractéristiques techniques que sur celui de la sécurité. La Commission nationale pour la réglementation d'Etat des communications et de l'informatisation (NCCIR) a été habilitée, en vertu de la loi de l'Ukraine sur "les ressources en fréquences radioélectriques de l'Ukraine", à imposer des mesures additionnelles visant à protéger le marché ukrainien contre l'importation illicite de terminaux mobiles non autorisés ou de mauvaise qualité.

La NCCIR a défini une procédure réglementaire applicable à l'importation de terminaux mobiles. Dans le cadre de la mise en oeuvre technique de la procédure d'importation, le système automatique d'information pour l'enregistrement des terminaux mobiles en Ukraine (AISMTRU) a été créé et mis en service par le Centre des radiofréquences de l'Etat ukrainien (UCRF) en 2009. En conséquence, les importations illégales de terminaux mobiles ont enregistré un repli spectaculaire, puisqu'elles représentaient entre 5 et 7% du marché en 2010, et que cette baisse s'est poursuivie au cours des années suivantes.

En Ukraine, les numéros IMEI sont utilisés pour créer une base de données des dispositifs légalement importés dans le pays. Les listes ci-après sont tenues à jour: "liste blanche" des dispositifs importés légalement, "liste grise" des dispositifs dans le statut n'est pas confirmé et "liste noire" des dispositifs dont l'accès au service est refusé. Un accès est fourni aux autorités réglementaires et douanières, aux opérateurs de réseaux et au grand public disposant de niveaux appropriés de privilèges d'accès.

L'AISMTRU s'acquitte des fonctions suivantes:

- automatisation du traitement des demandes des importateurs visant à mener à bien les procédures réglementaires d'enregistrement et d'utilisation des équipements terminaux dans les réseaux de télécommunication;
- mesures visant à empêcher l'importation "parallèle" (marché gris) illégale de terminaux mobiles sur le territoire ukrainien;
- lutte contre le vol de combinés;
- automatisation du flux de travail de l'UCRF et amélioration de l'efficacité des activités entre l'UCRF et les protagonistes du marché des terminaux;
- détermination des codes IMEI "clonés" et blocage des terminaux portant des codes IMEI "clonés".

On trouvera des renseignements détaillés sur l'AISMTRU au paragraphe A.1.11.2.

En vertu de la législation de l'Ukraine, la vente de terminaux mobiles comportant des codes IMEI non enregistrés auprès de l'AISMTRU est interdite. L'AISMTRU comprend essentiellement la base de données générale, qui tient à jour des listes "blanche", "grise" et "noire" des codes IMEI des terminaux mobiles. Lorsqu'un terminal est raccordé et enregistré pour la première fois auprès d'un opérateur de réseau, son code IMEI est automatiquement transféré par l'opérateur mobile dans la base de données générales. L'AISMTRU communique les codes IMEI qui ne figurent pas dans la liste "blanche", identifie les téléphones mobiles contrefaits et enregistre les codes IMEI correspondants dans la liste "grise". Tous les propriétaires des terminaux concernés sont informés par SMS et doivent confirmer l'origine légale de leur terminal dans un délai de 90 jours à compter de la date d'inscription dans la liste "grise".

Les codes IMEI des terminaux volés sont inscrits dans la liste "noire" à la demande d'une autorité chargée de l'application de la loi, ce qui prive de tout intérêt le vol de terminaux. On applique la même procédure pour le verrouillage du terminal, à la demande des propriétaires de téléphones perdus. Les opérateurs de réseaux ne fournissent aucun service aux terminaux inscrits sur la liste "noire".

L'objectif de la protection des consommateurs est atteint grâce à la mise en oeuvre de l'outil qui permet à un consommateur de vérifier aisément si un terminal mobile est licite avant de l'acheter Tout consommateur peut vérifier le statut du code IMEI du terminal en envoyant un SMS avec ce code au numéro national "307", ou en utilisant le portail Internet de l'UCRF. Il ne faut pas plus de 10 secondes pour procéder à cette vérification.

Grâce à la mise en oeuvre du système AISMTRU, il existe un marché de terminaux licites en Ukraine et l'importation "parallèle" (marché gris) illégale de terminaux mobiles a considérablement reculé dans le pays. La part de terminaux mobiles importés illégalement, qui s'établissait entre 93% et 95% en 2008, ne représentait plus que 5% à 7% en 2010 et pendant les années suivantes. L'Etat a perçu des recettes provenant des droits de douane à l'importation des terminaux mobiles d'un montant supérieur à 500 millions USD pendant la période 2010-2012, contre 30 millions USD au cours des trois années précédentes. Le marché ukrainien des terminaux mobiles comprend essentiellement les terminaux mobiles qui satisfont aux caractéristiques techniques requises en matière d'utilisation en Ukraine.

A.1.11.2 Système automatique d'information pour l'enregistrement des terminaux mobiles en Ukraine (AISMTRU)

A.1.11.2.1 Considérations générales

Le développement rapide des services de communication mobiles (cellulaires) fournis par les opérateurs et la prédominance de ce type de services de télécommunication en Ukraine ont favorisé un essor rapide du marché des terminaux mobiles en Ukraine et, par conséquent, l'accroissement de l'importation de ces produits.

On entend par "terminal mobile" un combiné mobile ou tout autre équipement d'utilisateur final d'un réseau de télécommunication doté d'un identificateur international (code IMEI) et pouvant être identifié dans le réseau au moyen de ce code.

En 2008, le marché de l'Ukraine a été confronté à une situation critique: en effet, 93% à 95% des produits présents sur le marché étaient des produits d'importation parallèle du "marché gris "ou, pour dire les choses simplement, des biens importés en contrebande. De plus, ces produits étaient en grande partie représentés par des copies de combinés de marque d'origine inconnue, qui ne satisfaisaient pas aux normes de l'Ukraine en termes de caractéristiques techniques ou de sécurité. Les diverses mesures de régulation du marché qui ont été prises n'ont pas permis de remédier à cette situation et les terminaux n'étaient pas fabriqués en Ukraine.

C'est pourquoi l'autorité indépendante de régulation, à savoir la Commission nationale pour la réglementation d'Etat des communications et de l'informatisation (NCCIR) – a été habilitée, en vertu de la loi de l'Ukraine "sur les ressources en fréquences radioélectriques de l'Ukraine", à imposer des mesures additionnelles visant à protéger le marché ukrainien contre l'importation illicite de terminaux mobiles non autorisés ou de mauvaise qualité.

A.1.11.2.2 Objectifs

Afin de contrôler l'importation, la commercialisation et l'utilisation de terminaux, la NCCIR a défini les objectifs suivants:

1) Protéger le marché ukrainien contre les terminaux mobiles de mauvaise qualité, susceptibles de ne pas être autorisés ou de présenter un danger pour la santé.
2) Faire en sorte que les services de communication mobiles soient de bonne qualité.
3) Résoudre les problèmes sociaux liés au vol de téléphones mobiles, notamment par les enfants.
4) Lutter contre l'importation et la commercialisation illégales de terminaux mobiles sur le marché ukrainien.

Des procédures ont été élaborées concernant l'importation et la commercialisation d'équipements mobiles, compte dûment tenu des objectifs ci-dessus. Ces procédures ont fait l'objet de lois officielles: procédure applicable à l'importation d'équipements électroniques de radiocommunication et de dispositifs émetteurs de rayonnements et procédure applicable à la commercialisation d'équipements électroniques et de dispositifs émetteurs en Ukraine.

A.1.11.2.3 Procédures d'importation

L'importation d'équipements radioélectriques en Ukraine est contrôlée par les autorités douanières conformément aux conditions suivantes:

- Fourniture d'un document sur la conformité de l'équipement radioélectrique aux réglementations techniques.
- Conformité au Registre des équipements électroniques de radiocommunication et aux dispositifs émetteurs de rayonnements dont l'utilisation est autorisée en Ukraine dans les bandes de fréquences couramment utilisées.
- Absence, dans le Registre, d'équipements électroniques de radiocommunication et de dispositifs émetteurs de rayonnements dont l'utilisation est interdite en Ukraine dans les bandes de fréquences couramment utilisées.

Les codes IMEI, soumis par l'importateur à l'UCRF, sont traités et inscrits dans la "liste blanche" de la base de données générale des codes IMEI. Pour l'enregistrement des identificateurs internationaux des équipements terminaux légalement importés en Ukraine, le Service national des douanes de l'Ukraine fournit chaque jour à l'UCRF un extrait de la déclaration en douane (sous forme électronique) pour l'importation des équipements électroniques de radiocommunication

Dans le cadre de la mise en oeuvre technique de la procédure d'importation réglementaire décrite ci-dessus, le système automatique d'information pour l'enregistrement des terminaux mobiles en Ukraine (AISMTRU) a été créé et mis en service par l'UCRF le 1er juillet 2009.

Conformément à la loi de l'Ukraine "sur la confirmation de la conformité", la conformité des équipements terminaux doit être certifiée par les organismes agréés par le Régulateur (NCCIR).

A.1.11.2.4 Fonctions du système AISMTRU

Les fonctions du système AISMTRU sont décrites au paragraphe A.1.11.1:

- automatisation du traitement des demandes des importateurs;
- mesures visant à empêcher l'importation "parallèle" (marché gris) illégale de terminaux mobiles sur le territoire ukrainien;
- lutte contre le vol de combinés;
- automatisation du flux de travail de l'UCRF et amélioration de l'efficacité des activités entre l'UCRF et les protagonistes du marché des terminaux;
- détermination des codes IMEI "clonés" et blocage des terminaux portant des codes IMEI "clonés".

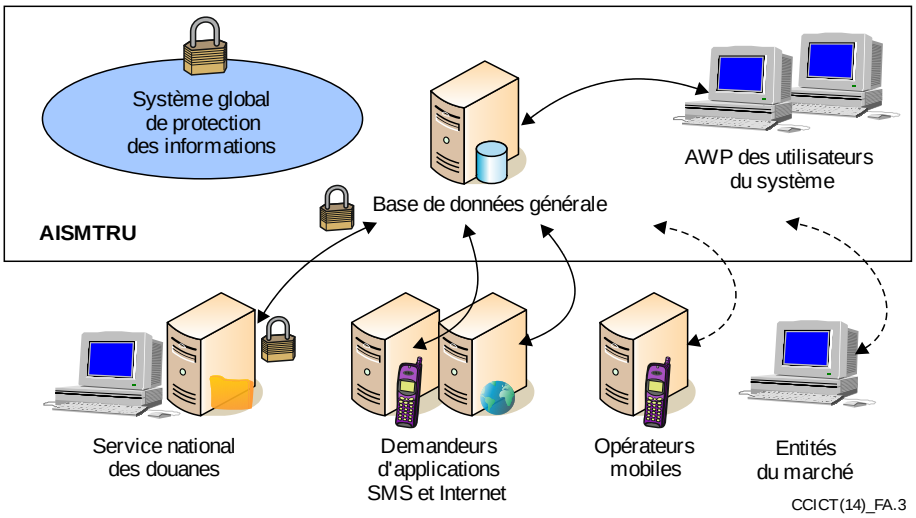


Figure A.3 – Fonctions du système AISMTRU

A.1.11.2.5 Autorisation

En vertu de la législation en vigueur, les entités ci-après sont autorisées à utiliser le système AISMTRU:

- Centre des radiofréquences de l'Etat ukrainien;
- Commission nationale pour la réglementation d'Etat des communications et de l'informatisation;
- opérateurs mobiles;
- service national des douanes;
- Ministère de l'intérieur;
- acheteurs et utilisateurs de terminaux mobiles; et
- importateurs.

A.1.11.2.6 Base de données générale de codes IMEI

L'AISMTRU comprend essentiellement la base de données générale de codes IMEI, qui tient à jour trois listes communément appelées:

- "Liste blanche": registre des codes IMEI des terminaux légalement importés ou fabriqués en Ukraine.
- "Liste grise": registre de la base de données générales comportant les codes IMEI des terminaux qui ne figurent pas sur la "liste blanche" ou la "liste noire" au moment où le terminal est enregistré pour la première fois auprès d'un opérateur de réseau de télécommunication.
- "Liste noire": registre des codes IMEI des terminaux ne pouvant être desservis par les réseaux des opérateurs (terminaux volés ou perdus, terminaux dont l'origine légale n'est pas confirmée dans un délai de 90 jours à compter de la date d'inscription dans la liste "grise").

Le sous-système de mise à jour de la base de données générale de codes IMEI offre aux utilisateurs autorisés de l'UCRF un moyen d'inscrire des données dans la "liste blanche". Les listes "grise" et "noire" sont générées automatiquement. Les utilisateurs autorisés de l'UCRF disposent d'un droit limité de modifier le statut de tel ou tel code IMEI figurant dans les listes "grise" et "noire".

Chaque mesure prise par l'utilisateur autorisé de l'UCRF est confirmée par une signature numérique électronique d'un utilisateur individuel.

Le sous-système est doté d'une fonction d'importation de données qui lui permet de transférer les données des importateurs de terminaux et des opérateurs mobiles dans le Registre de codes IMEI.

Grâce au traitement des données provenant de la "liste blanche" et les données provenant des opérateurs, des importateurs et du service des douanes, il est possible de créer et de tenir à jour des registres des listes "grise" et "noire".

Au cours de la première étape de la mise en service du système, il a été possible d'atteindre les deux objectifs suivants:

1) Protection du marché ukrainien contre les terminaux mobiles non autorisés de mauvaise qualité et susceptibles de présenter un danger pour la santé des utilisateurs.

2) Lutte contre l'importation illégale de terminaux mobiles et leur commercialisation sur le marché ukrainien.

Par la suite, on a mis au point un système pour veiller à ce que tous les objectifs soient atteints, et pour décourager le vol de terminaux mobiles, notamment par les enfants.

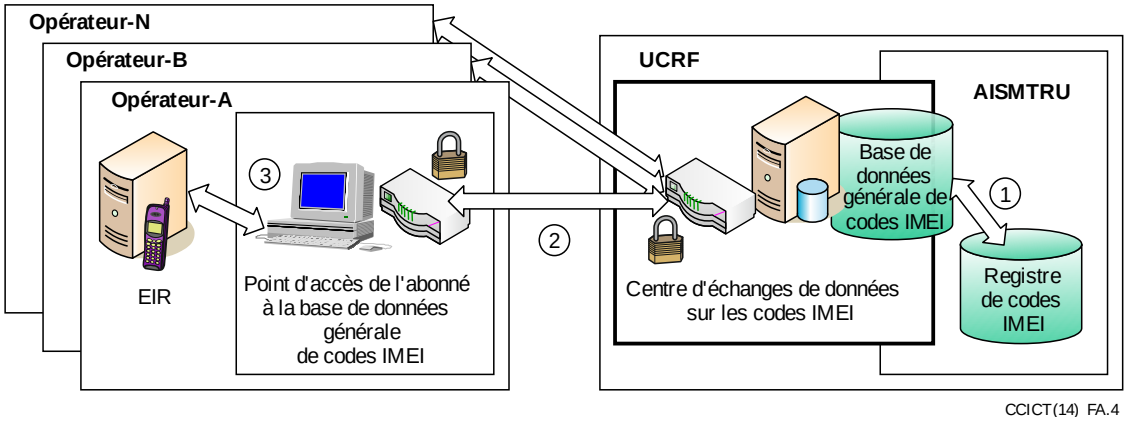


Figure A.4 – Registre EIR et base de données générale de codes IMEI

Dans un deuxième temps, on a mis en place un sous-système d'échange de codes IMEI provenant des listes "blanche", "grise" et "noire" entre le système AISMTRU et les opérateurs mobiles nationaux. A ce stade, l'échange de codes IMEI était effectué manuellement.

En outre, des sous-systèmes d'échange de données ont été mis en place, avec le Ministère de l'intérieur, afin de l'informer sur les terminaux volés ou perdus, et avec les services des douanes afin de leur communiquer des informations sur les terminaux importés.

Pour assurer une interaction active avec système AISMTRU, les opérateurs et l'UCRF ont fourni l'appui suivant:

- tenue à jour du registre d'identités d'équipements (EIR);
- point d'accès de l'abonné à la base de données générale de codes IMEI (point d'accès de l'abonné);
- canal d'interaction entre le point d'accès de l'abonné et le registre EIR;
- application de signatures et de certificats numériques pour les utilisateurs autorisés.

Ce système, intégré dans le système AISMTRU, vise à synchroniser les travaux du Registre EIR d'opérateurs (mobiles) cellulaires et la base de données générale de codes IMEI, ce qui permet d'échanger automatiquement les listes de codes IMEI entre les registres EIR des réseaux des opérateurs mobiles et la base de données générale de codes IMEI. Ainsi, le code IMEI de chaque terminal, une fois enregistré dans le réseau de l'opérateur, apparaît dans le système AISMTRU, puis est vérifié dans la base de données générale de codes IMEI.

A l'heure actuelle, le serveur de synchronisation prend en charge les modes manuel et automatique pour la connexion avec le Registre EIR des opérateurs.

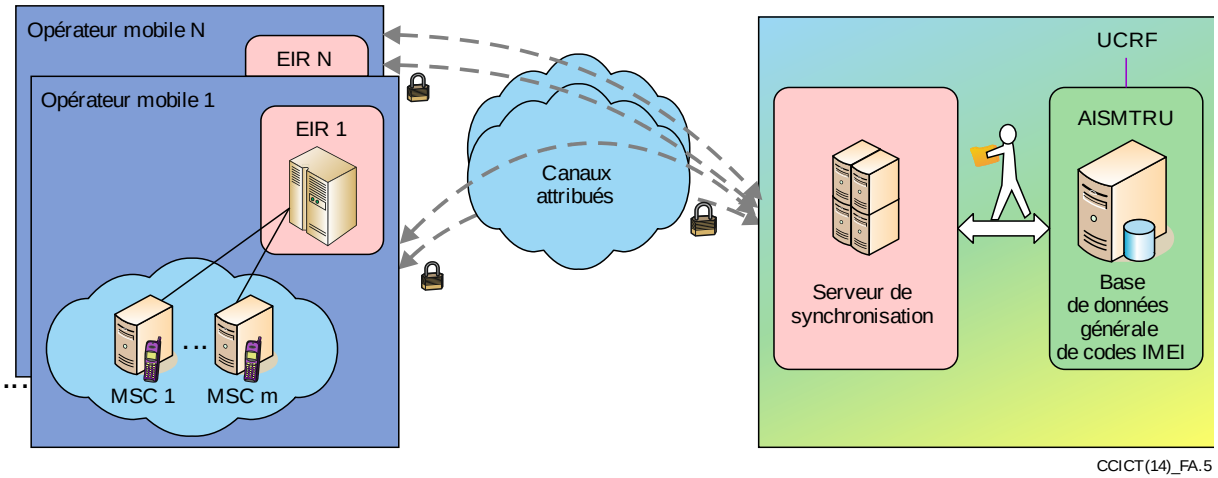


Figure A.5 – Serveur de synchronisation

A.1.11.2.7 Caractéristiques

Les caractéristiques du système sont les suivantes:

- utilisation des normes de l'industrie pour le stockage et le transfert des données (échange de données);
- sécurité garantie des données et du système tout entier;
- utilisation de la norme nationale applicable aux signatures numériques pour garantir l'intégrité et la non-répudiation à tous les stades du traitement des données dans le système;
- structure modulaire du système;
- mode de fonctionnement 24 heures sur 24 et 7 jours sur 7.

A.1.11.2.8 Sécurité des données

Le système global de protection des informations (CIPS) de l'AISMTRU est conforme aux dispositions de la législation en vigueur, comme en atteste la conclusion positive rendue sur la base des résultats de l'examen effectué par une autorité gouvernementale compétente.

Le système CIPS assure:

- le contrôle de l'accès limité aux renseignements à caractère confidentiel;
- l'identification des risques pour la sécurité qui pèsent sur les renseignements à accès limité qui sont transférés, traités et stockés dans le système;
- la protection de la confidentialité, de l'intégrité et de la disponibilité des renseignements à accès limité contre l'accès non autorisé;

- la prévention de la fuite d'informations lorsque l'on doit pénétrer dans un environnement peu sûr;
- la protection des informations techniques contre l'accès non autorisé, la destruction, l'altération ou le blocage.

La sécurité et la fiabilité sont garantis grâce à:

- l'utilisation de moyens fiables de signature numérique électronique, pour assurer l'authenticité et l'intégrité des informations, l'autorisation et l'authentification des utilisateurs autorisés;
- la mise en oeuvre de signatures numériques électroniques conformément aux normes nationales en vigueur en Ukraine;
- l'existence d'un système de sauvegarde et de rétablissement;
- la tenue à jour de connexions sécurisées (des enregistrements des mesures prises par les utilisateurs ou des événements sont conservés dans le système).

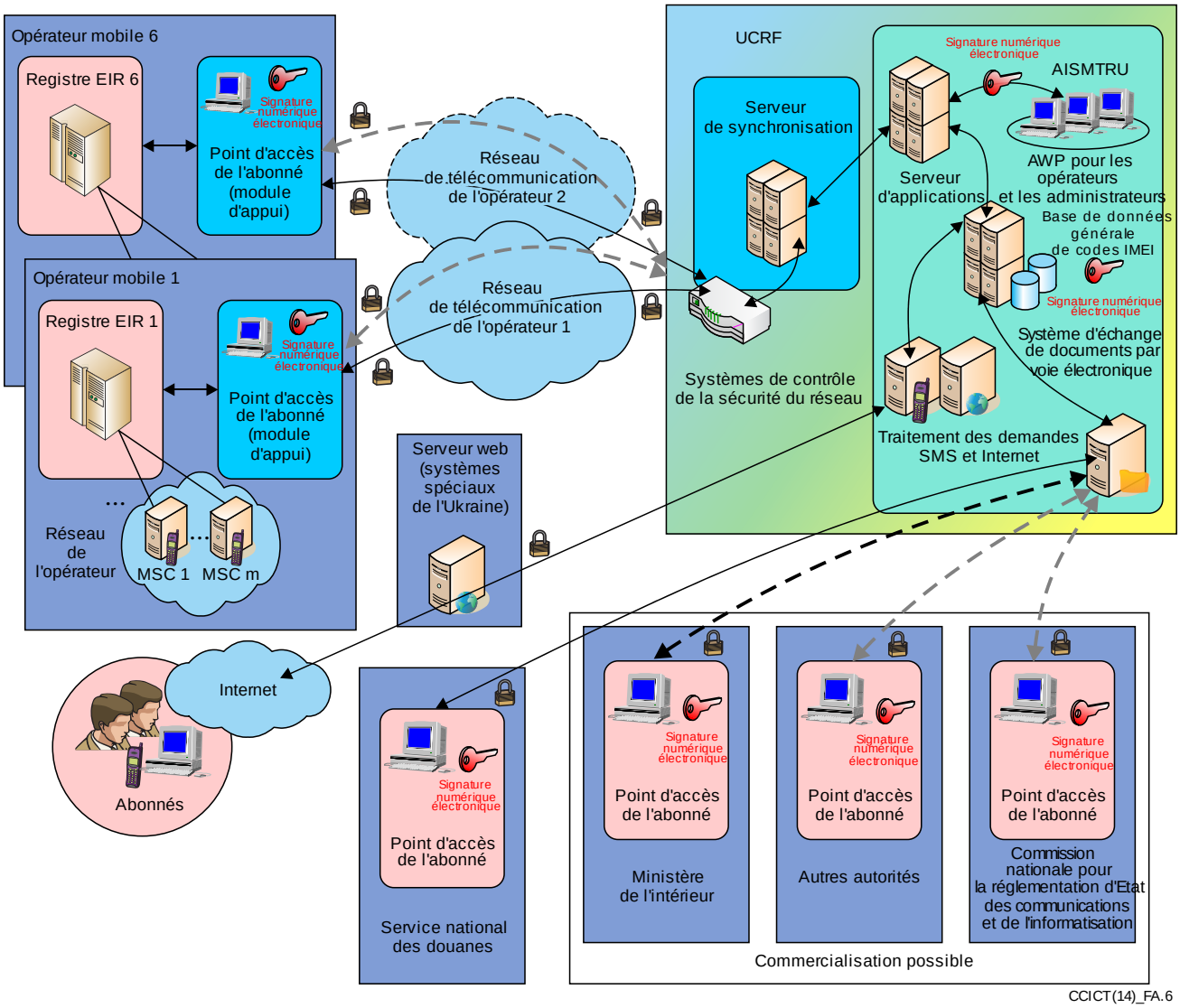


Figure A.6 – Système global de protection des informations (CIPS) de l'AISMTRU

A.1.11.2.9 Conséquences de la mise en oeuvre

1) Protection des consommateurs

Chaque acheteur peut vérifier qu'un terminal mobile est licite avant d'en faire l'acquisition en Ukraine. Pour ce faire, un acheteur peut consulter le site web officiel de l'UCRF ou envoyer un SMS avec un code IMEI de terminal vérifié au numéro "307", qui est commun à tous les opérateurs mobiles. Au bout de quelques secondes, une réponse donne le statut du code IMEI demandé dans la base de données générale des codes IMEI.

Ce mécanisme permet de protéger le marché ukrainien contre les terminaux qui ne sont pas conformes aux prescriptions en matière d'utilisation exigées en Ukraine.

Conformément à la législation ukrainienne actuellement en vigueur, la commercialisation de terminaux mobiles portant des codes IMEI non enregistrés dans la base de données générale des codes IMEI est interdite.

2) Lutte contre le vol de terminaux

Les codes IMEI des terminaux volés sont enregistrés dans la "liste noire" à la demande d'une autorité chargée de l'application de la loi, privant ainsi de tout intérêt le vol de ces terminaux. On applique la même procédure pour le verrouillage du terminal, à la demande des propriétaires de téléphones perdus.

3) Suppression de l'importation illégale

Lors de la première connexion au réseau d'un opérateur, un terminal est immédiatement enregistré auprès du réseau concerné. Les codes IMEI des terminaux, desservis par le réseau d'un opérateur (à l'exception de ceux qui sont en mode itinérance internationale), sont automatiquement transférés en temps utile (de nuit) par les opérateurs mobiles dans la base de données générale des codes IMEI de l'AISMTRU.

L'AISMTRU indique les codes IMEI qui ne figurent pas dans la "liste blanche" de la base de données générale des codes IMEI. Ces codes IMEI sont enregistrés dans la "liste grise". Tous les propriétaires des terminaux concernés sont informés par SMS que leur terminal risque d'être verrouillé dans un délai de 90 jours.

A l'expiration du délai de 90 jours, le code IMEI est transféré de la "liste grise" dans la "liste noire". Les terminaux figurant sur la "liste noire" ne sont pas desservis par les opérateurs (refus d'enregistrement dans le réseau, sauf pour les appels d'urgence vers le numéro "112"). Une connexion avec le réseau d'un autre opérateur ne modifie pas le statut du terminal inscrit sur la "liste grise" ou la "liste noire".

Après avoir été informé par SMS que son terminal risque d'être inscrit dans la "liste grise" au bout d'un délai de 90 jours, le propriétaire peut demander à l'UCRF de lui donner confirmation que le terminal a été importé légalement. Le personnel de l'UCRF examine la demande du propriétaire et, si la légalité de l'importation est confirmée, transfère le code IMEI de la "liste grise" dans la "liste blanche". Au terme de cette procédure, les opérateurs mobiles commencent à fournir des services au terminal sans délai.

Cependant, à l'heure actuelle, les terminaux figurant sur la "liste noire" ne sont pas déconnectés, car l'instrument juridique nécessaire n'existe pas encore.

L'UCRF gère un centre d'appel pour traiter les appels liés aux demandes des utilisateurs de terminaux mobiles concernant le statut du code IMEI et l'importation des terminaux.

4) Mise en conformité du marché des terminaux en Ukraine

- L'importation "parallèle" (marché gris) illégale de terminaux mobiles a considérablement diminué. La part de terminaux mobiles importés illégalement, qui s'établissait entre 93% et 95% en 2008, ne représentait plus que 7,5% en 2008.
- L'Etat a perçu des recettes provenant des droits de douane à l'importation des terminaux mobiles d'un montant supérieur à 500 millions USD pendant la période 2010-2012, contre 30 millions USD au cours des trois années précédentes.
- Le marché ukrainien des terminaux mobiles comprend essentiellement les terminaux mobiles qui satisfont aux caractéristiques techniques requises en matière d'utilisation en Ukraine.
- Au 30 avril 2013, 140 865 260 codes IMEI de terminaux mobiles étaient enregistrés dans la base de données générale des codes IMEI du système AISMTRU.
- Le système AISMTRU a été mis en place en sept mois, aux dépens des fonds perçus par l'UCRF au titre des paiements des importateurs.

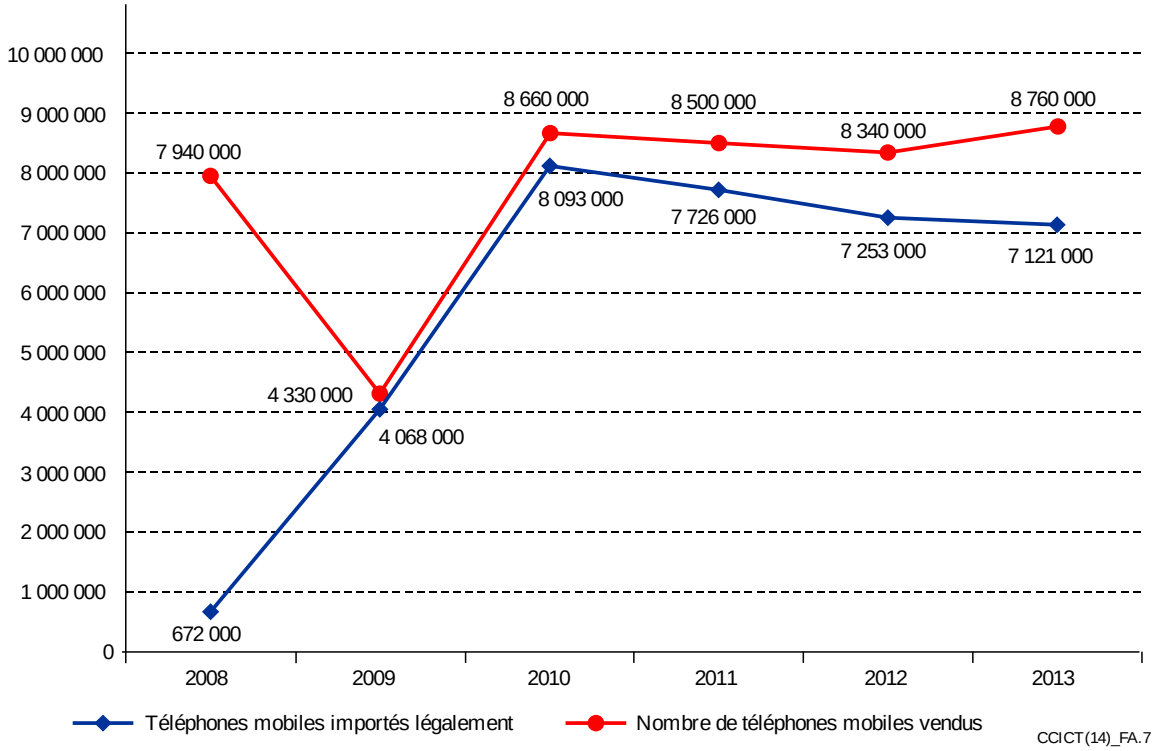


Figure A.7 – Conséquences de la mise en oeuvre du système AISMTRU en Ukraine

A.1.12 Emirats arabes unis (EAU)

En vertu de la législation des EAU en matière de télécommunications, l'utilisation, la vente, l'achat, la distribution et la promotion des dispositifs mobiles de contrefaçon sont interdits. L'Autorité de régulation des télécommunications (TRA) prend toutes les mesures nécessaires pour faire en sorte qu'il soit entièrement mis fin à la vente et à l'utilisation de ces dispositifs aux EAU. Les personnes qui participent à la vente de téléphones mobiles de contrefaçon sont informées et se voient infliger une amende, tandis que, dans certains cas, les licences peuvent être retirées en cas de non-respect de la réglementation.

En 2011, la TRA a lancé une nouvelle campagne de sensibilisation du public visant à décourager l'utilisation des téléphones mobiles de contrefaçon aux EAU (http://www.tra.gov.ae/download.php?filename=public-announcements/IMEI_announcement_en.pdf, http://www.tra.gov.ae/news_TRA_Launches_Fake_Mobile_Awareness_Campaign-354-1.php). En outre, la TRA a annoncé qu'à compter du 1er janvier 2012, tous les téléphones mobiles portant un faux numéro IMEI cesseraient de fonctionner sur le réseau mobile de télécommunication des EAU. La TRA a fait paraître des annonces dans des quotidiens pour avertir les utilisateurs de l'interdiction imminente des téléphones de contrefaçon.

Même si cette mesure avait pour but de rendre obsolètes les téléphones mobiles frauduleux, elle n'a eu aucune incidence sur les abonnements au service, qui ont continué de fonctionner normalement lorsque des dispositifs téléphoniques mobiles authentiques étaient utilisés. Lorsqu'ils envoient un SMS avec le numéro IMEI du dispositif mobile vers le numéro de téléphone "8877", les utilisateurs peuvent recevoir une réponse d'un prestataire de services donnant des renseignements sur le statut de ce dispositif. Les utilisateurs de faux dispositifs sont immédiatement contactés par leur prestataire de services et tous les téléphones non homologués doivent être déconnectés de tous les services de télécommunication, y compris les appels, les textos et l'Internet.

La TRA a fait savoir que les dispositifs mobiles frauduleux pouvaient présenter des risques pour la santé des utilisateurs et a encouragé tous les utilisateurs à prendre les précautions nécessaires lors de l'acquisition de dispositifs et d'équipements mobiles. Selon la TRA, les téléphones de contrefaçon sont souvent à l'origine de fuites de liquides de la batterie et d'explosions, qui libèrent des substances chimiques très toxiques et dangereuses. Comme le montage de ces appareils est de qualité médiocre, les niveaux de rayonnement ne sont pas contrôlés, les batteries tendent à se décharger plus rapidement et la réception du signal est d'ordinaire plus faible.

L'objectif de la TRA était en définitive de supprimer les dispositifs mobiles de contrefaçon des EAU et de sensibiliser le grand public ainsi que les revendeurs aux risques liés à leur utilisation. La TRA a reconnu que les problèmes de la contrefaçon et du piratage étaient lourds de conséquences pour l'économie et les droits de propriété intellectuelle, mais que les téléphones mobiles de contrefaçon étaient également des dispositifs de qualité médiocre, fabriqués sans avoir fait l'objet de tests et de contrôles appropriés.

A.2 Exemples de mesures communes prises à l'échelon régional

A.2.1 Commission interaméricaine des télécommunications (CITEL)

La CITEL a été créée par l'Assemblée générale de l'Organisation des Etats Américains (OEA) en 1994, en vue de promouvoir le développement des télécommunications/TIC dans la région Amériques. Ont qualité de membres de la CITEL tous les Etats Membres de l'Organisation, au nombre de 35, et plus de 100 organismes du secteur des TIC à titre de Membre associé.

Le Comité consultatif permanent I de la CITEL (Télécommunications) a recommandé aux Etats Membres, en 2009, "d'envisager de créer des bases de données dans le cadre d'un programme global de lutte contre la contrefaçon et la fraude" (Rapport final de la 15ème réunion du PCC.I 2 de la CITEL, octobre 2009), et en décembre 2011, le Comité consultatif permanent II: (Radiocommunications, y compris radiodiffusion) (PCC.II) a commencé à étudier les mesures prises par les administrations de télécommunication en ce qui concerne l'utilisation de téléphones mobiles de contrefaçon.

Le PCC.II a décidé de demander aux administrations de fournir des renseignements "sur les mesures et les dispositions réglementaires et administratives adoptées ou en projet concernant les téléphones cellulaires faux, contrefaits et de qualité inférieure et sur leurs conséquences négatives

pour les utilisateurs et les opérateurs, y compris sous l'angle des brouillages, des niveaux d'exposition aux rayonnements non ionisants (NIR) et de l'utilisation de substances chimiques dangereuses ou interdites" (Rapport final de la 18ème réunion de la CITEL, PCC.II, 22 décembre 2011, Décision 121).

La CITEL a également examiné le problème du vol de téléphones mobiles et les deux comités consultatifs permanents ont adopté un certain nombre de résolutions sur cette question.

Le PCC.II a approuvé en septembre 2011 la Résolution 73, intitulée "Etablissement d'un partenariat régional pour lutter contre le vol de terminaux mobiles". En vertu de cette Résolution, le PCC.I était invité à prier la CITEL "d'encourager la mise en place de mesures communes par les Etats Membres en vue de restreindre, dans tous les pays de la région, la mise en service de ces équipements terminaux mobiles volés, et d'adopter des recommandations concrètes à l'intention des opérateurs, afin qu'ils utilisent les ressources qu'offre la technologie et ne permettent pas le raccordement à leurs réseaux d'équipements dont l'origine n'a pas été dûment identifiée, en établissant un partenariat régional pour la lutte contre le vol d'équipements" (Rapport final de la 17ème réunion du PCC.II, 6 septembre 2011, Résolution 73).

Le PCC.I a donné suite à cette demande presque immédiatement, en adoptant une Résolution intitulée "Mesures régionales pour lutter contre le vol de dispositifs terminaux mobiles" (Rapport final de la 19ème réunion du PCC.I de la CITEL, 20 septembre 2011, Résolution 189). Dans cette Résolution, il est pris note du caractère international du problème, étant donné que les dispositifs mobiles sont envoyés vers d'autres pays, chaque fois qu'un pays pris individuellement adopte des mesures de lutte contre le vol de dispositifs, d'où la nécessité de prendre des mesures à l'échelon régional. En plus des mesures relatives à la perte ou au vol de combinés, les Etats Membres sont invités, dans la Résolution, à "envisager d'inclure dans leurs cadres réglementaires l'interdiction de mise en service et de l'utilisation des numéros IMEI ou du numéro de série électronique du fabricant des dispositifs déclarés volés, perdus ou *d'origine illicite* dans les bases de données régionales ou internationales" (en italique dans le texte).

L'Annexe de la Résolution 189 comprend diverses mesures complémentaires visant à "étudier la possibilité de mettre en place des mesures de contrôle de la commercialisation au niveau local des dispositifs terminaux mobiles et leur raccordement aux réseaux" et "à encourager l'établissement de mécanismes réglementaires, budgétaires ou douaniers destinés à veiller à ce que l'importation des dispositifs terminaux mobiles ou de leurs composants [soient] d'origine licite et soient certifiés conformes au cadre réglementaire de chaque Etat Membre, ainsi que de contrôles douaniers visant à empêcher la sortie ou la réexportation de dispositifs mobiles volés ou de leurs composants".

Le PCC.I a adopté en 2012 une Recommandation intitulée "Mesures régionales relatives à l'échange d'informations sur les dispositifs terminaux mobiles déclarés volés, perdus ou récupérés" (Rapport final de la 20ème réunion du PCC.I de la CITEL, 10 juin 2012, Recommandation 16), qui portait également sur les terminaux "d'origine illégale". Les Etats Membres sont invités à "mettre en oeuvre des mesures aux niveaux national, régional et international pour que les fournisseurs de services de télécommunication mobiles puissent échanger des informations sur les dispositifs terminaux mobiles volés, perdus ou illicites dans le cadre des différentes plates-formes opérationnelles et existantes pour les différentes techniques d'accès, afin de lutter contre les marchés informels, de promouvoir la coopération entre les pays et de préserver les principes de sécurité du citoyen et les droits des utilisateurs finals". Il est également recommandé aux Etats Membres "d'envisager de créer une plate-forme de base de données pour l'échange d'informations sur les dispositifs terminaux mobiles volés, perdus ou d'origine illicite au moyen du ou des numéros MEID (identificateur d'équipements mobiles) utilisés par le système d'accès multiple par répartition en code (AMRC) EV-DO (évolution à données optimisées) et le système AMRC/4G de type bimode et, dans de nombreux réseaux, le module d'identité d'utilisateur amovible (RUIM)".

Le PCC.I a également approuvé "un rapport technique" intitulé "Vol ou perte de terminaux mobiles" (Rapport final de la 23ème réunion du PCC.I de la CITEL, 10 octobre 2013, Résolution 217).

En mai 2014, la CITEL a approuvé la Résolution 222 (XXIV-14) – "Renforcement des mesures régionales visant à lutter contre le phénomène de la contrefaçon de dispositifs mobiles de qualité médiocre et non approuvés".

En conséquence, il a été créé un groupe de travail par correspondance chargé d'examiner les mesures régionales de lutte contre le phénomène des dispositifs mobiles contrefaits, de qualité médiocre et non approuvés, afin d'échanger des renseignements, des données d'expérience et de bonnes pratiques techniques et réglementaires avec les Etats Membres sur cette question, l'objectif étant d'élaborer des recommandations et des lignes directrices susceptibles d'être mises en place dans la région Amériques.

En août 2014, le programme de travail de ce groupe de travail par correspondance a été approuvé et inclus dans le mandat du Rapporteur sur la lutte contre la fraude, les pratiques de non-conformité sur le plan réglementaire dans le domaine des télécommunications et les mesures régionales de lutte contre le vol de dispositifs terminaux mobiles, qui a pour tâche:

- d'élaborer une définition de ce que l'on entend par dispositifs mobiles contrefaits, de qualité médiocre et non approuvés;
- d'évaluer la portée et la nature du problème des dispositifs mobiles contrefaits, de qualité médiocre et non approuvés;
- d'encourager l'échange d'informations et de données d'expériences entre les membres de la CITEL en ce qui concerne les mesures prises pour lutter contre la vente et l'utilisation de dispositifs mobiles contrefaits, de qualité médiocre et non approuvés;
- de faire connaître, documents à l'appui, des exemples de bonnes pratiques du monde entier concernant la lutte contre la vente et l'utilisation de dispositifs mobiles contrefaits, de qualité médiocre et non approuvés;
- de proposer l'élaboration de rapports techniques, de recommandations ou de résolutions de la CITEL traitant des mesures techniques et réglementaires à prendre pour lutter contre la vente et l'utilisation de dispositifs mobiles contrefaits, de qualité médiocre et non approuvés dans la région Amériques;
- d'achever les travaux et de rendre compte des résultats obtenus au Rapporteur chargé d'examiner les pratiques de non-conformité sur le plan réglementaire et de lutte contre la fraude dans le domaine des télécommunications.

A.2.2 Communauté de l'Afrique de l'Est (EAC)

En Afrique de l'Est, le manque à gagner dû à l'imitation de produits a représenté plus de 500 millions USD par an (http://www.trademarkea.com/ea-loses-huge-sums-of-money-in-counterfeit-products/). Des produits bon marché et de qualité médiocre fournis par l'intermédiaire de revendeurs et de fabricants étrangers ou locaux reproduisent illégalement des noms de marques et des modèles connus sur leur emballage.

Conformément à un Protocole de marché commun, adopté par la CEA en 2010, on ne pourra venir à bout du problème des produits et du commerce de contrefaçon qu'en instaurant une étroite collaboration.

L'Organisation des communications de l'Afrique de l'Est (EACO) est un organisme régional qui rassemble les organisations de réglementation, des postes, des télécommunications et de la radiodiffusion issues des cinq Etats Membres de la CEA (Kenya, Tanzanie, Rwanda, Burundi et Ouganda). L'EACO s'est penchée sur le problème de la contrefaçon des téléphones mobiles qui inondent les marchés de la région et a approuvé une initiative commune pour y faire face en 2012.

Le Groupe spécial sur le numérotage de l'EACO (CCK-Kenya, TCRA-Tanzania, RURA-Rwanda, ARCT-Burundi, UCC-Uganda) a recommandé en mai 2012 la création d'une base de données nationale et l'adoption de procédures de vérification des combinés pour protéger les consommateurs, les entreprises et les réseaux contre les effets de la contrefaçon (Rapport du groupe spécial sur le numérotage de l'EACO pour 2011-2012).

Le 19ème Congrès de l'EACO tenu en 2012 a été informé de l'état d'avancement de la mise en oeuvre de Registres d'identité d'équipements (EIR) dans la région; certains problèmes rencontrés à cet égard sont décrits sur le site http://www.eaco.int/docs/19_congress_report.pdf. Ces problèmes sont les suivants:

- reproduction en double ou absence d'identités internationales d'équipements mobiles (IMEI);
- méconnaissance par les consommateurs des dangers associés à la contrefaçon d'équipements et insuffisance des connaissances sur la manière de vérifier l'authenticité d'un équipement;
- méconnaissance de la part des fournisseurs et des revendeurs locaux des problèmes associés à la vente d'équipements de qualité inférieure bon marché;
- coût élevé de la mise en oeuvre.

Pour surmonter ces problèmes, les solutions suivantes ont été proposées:

- mener des campagnes de sensibilisation auprès des consommateurs et des fournisseurs locaux;
- octroyer des licences à tous les fournisseurs et revendeurs;
- améliorer les procédures d'homologation;
- créer des bases de données d'équipements; et
- exiger l'enregistrement des cartes SIM.

A.2.3 Association des régulateurs des communications et des télécommunications de la communauté des pays lusophones (ARCTEL-CPLP)

L'Association des régulateurs des communications et des télécommunications de la communauté des pays lusophones (ARCTEL-CPLP) compte parmi ses membres les pays suivants: Angola, Brésil, CaboVerde, Guinée-Bissau, Mozambique, Portugal, Sao Tomé-et-Principe et Timor-Oriental (http://www.arctel-cplp.org). L'ARCTEL-CPLP a présenté un exposé lors du Colloque mondial des régulateurs organisé par l'UIT en 2012 sur les approches régionales adoptées pour lutter contre le vol de dispositifs mobiles, le marché gris et les dispositifs de contrefaçon (https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/Batista3_ARCTEL_Session3_mobilerobbery.pdf).

L'ARCTEL-CPLP a proposé de développer la solution traditionnelle (à savoir les systèmes de bases de données de listes noires) pour l'étendre au niveau régional, moyennant l'adoption des mesures suivantes:

- échange des bases de données de listes noires GSM et AMRC dans le cadre d'accords bilatéraux ou multilatéraux;
- mise en place de mécanismes réglementaires, budgétaires ou douaniers destinés à renforcer les mesures de contrôle à l'importation de combinés et à en empêcher la réexportation;
- respect par les professionnels du secteur des recommandations en matière de sécurité visant à lutter contre la reprogrammation ou la reproduction en double de numéros IMEI ou du numéro d'identification de série électronique du fabricant;
- campagnes de sensibilisation du public à l'importance des déclarations de vol ou de perte de dispositifs terminaux mobiles.