ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

Double facette du dynamisme du secteur des TIC

Bulletin de veille technologique

Avril 2017, Abidjan
Côte d'Ivoire

Editorial

Le secteur des Technologies de l'Information et de la Communication est en perpétuelle évolution favorisant ainsi l'émergence, sans discontinuer, de produits innovants pour répondre aux besoins des populations.

La plupart de ces innovations ont un intérêt certain pour les consommateurs, comme par exemple les smartphones et les tablettes. Cependant ces innovations ne vont pas sans alimenter le marché de la contrefaçon.

Deux marchés se côtoient, chacune répondant dans une certaine mesure aux besoins des populations et participant du développement de l'économie numérique. En effet, d'une marnière peu glorieuse, la contrefaçon fournit à une frange de la population, ne disposant pas suffisamment de moyens financiers, la possibilité de se procurer des équipements TIC. De ce fait, elle concourt à la réduction de la fracture numérique. Cependant, laisser un tel marché à terme aura une conséquence néfaste sur l'innovation.

Le phénomène de la contrefaçon est d'autant plus préoccupant que les risques sont réels, non seulement pour les opérateurs et les Etats en terme de revenus et de taxes voire de sécurité nationale, mais aussi pour les populations car leur santé ainsi que la qualité des services consommés en dépend. La lutte contre la contrefaçon doit être une priorité et passée par des mesures de surveillance et de protection du marché.

Le développement du marché des télécommunications ainsi que celui des équipements terminaux s'est fortement appuyé sur le concept de SIM permettant d'accéder en toute sécurité au réseau et à un ensemble de services comme l'itinérance internationale ou les contacts téléphoniques indépendamment du terminal. Certes le consommateur à le libre choix du terminal pour sa connexion à un réseau mobile mais son accès au service est conditionné par l'acquisition d'un SIM détenu par l'opérateur réseau.

L'évolution vers l'eSIM offre des perspectives nouvelles pour l'ensemble de l'écosystème mobile dans le sens où il apporte plus de flexibilité aussi bien aux consommateurs, aux opérateurs qu'aux fournisseurs de services. L'eSIM laisse entrevoir de profondes mutations dans le business model des opérateurs de télécommunication qu'il convient d'anticiper.

Ce bulletin vise à attirer l'attention sur les évolutions positives et négatives du marché des composants d'accès usagers aux réseaux de télécommunications nécessaires au développement et à la bonne marche de l'économie numérique.

BILE Diéméléou

Directeur Général de l'ARTCI

Bulletin
de veille technologique -
Avril 2017
ARTCI, Côte d'Ivoire

Directeur de Publication:

M. BILE Diéméléou

Rédacteur en Chef:

M. KOUAKOU Guy-Michel

Equipe de rédaction:

M. ZEBOUA Patrick

M. YAO N'Guessan Kevin

M. ADOPO Antony Virgil

Mlle LASME Mel Paule Renée

Contacts

Marcory Anoumanbo, 18 BP 2203 Abidjan 18.

Tél : + 225 20 34 58 80

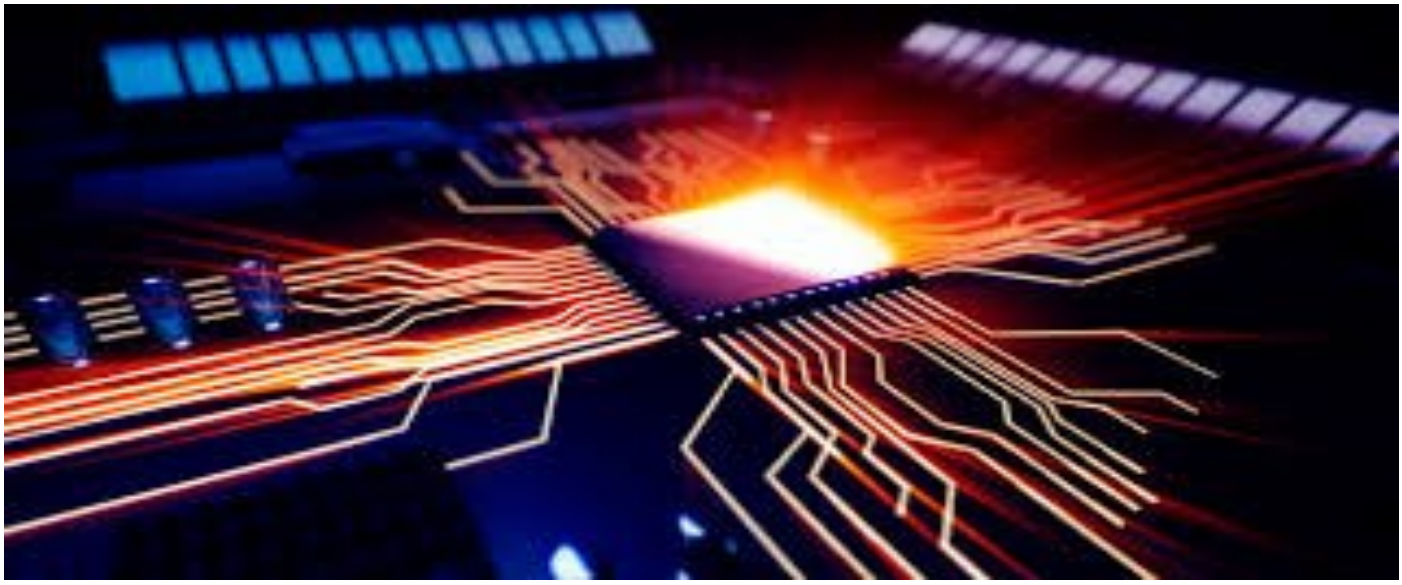
Fax : + 225 20 34 43 75

...Au lecteur

Parce que votre avis compte, nous serions heureux de recevoir vos suggestions et remarques, afin d'améliorer nos prochaines publications, à :

veilletechno@artci.ci

Sommaire



eSIM

INTRODUCTION

C'est en 1974 que la carte SIM (Subscriber Identity Module) a été inventée. Son inventeur, Roland Moreno dépose la même année son premier brevet – Moreno a déposé 45 brevets liés à la carte à puce – mais c'est huit ans plus tard que l'industrie sera convaincue de la nécessité de ce nouveau dispositif de stockage des informations.

Ainsi, depuis son déploiement au début des années 1990, la carte SIM a été un support indéniable aux réseaux mobiles permettant de stocker de façon sécurisée les informations d'identification et d'authentification.

Au fur et à mesure, la carte SIM s'est de plus en plus miniaturisée pour répondre aux besoins de construire des appareils de plus en plus fins dans lesquels chaque millimètre compte. Quatre formats de carte SIM existent:

- Le format ID-1 utilisé dans les cartes bancaires;
- Le format ID-0000 ou Standard SIM qui est la carte à puce classique des téléphones portables et des traceurs GPS;
- Le format 3FF ou Micro SIM;
- Le format 4FF ou Nano SIM.

Mais jusqu'où ira la miniaturisation ?

La GSMA a publié en 2016 des spécifications de ce qu'elle a appelé eSIM ou « embedded SIM » pour « SIM embarquée ». Il s'agit de SIM intégrée dans un appareil électronique comme une montre, un bracelet fitness ou un smartphone qui pourra être activée à distance.

Avec ces évolutions, la carte SIM est-elle appelée à disparaître sous sa forme actuelle?

QU'EST CE QUE L'ESIM?

Le terme « eSIM » fait référence à un nouveau standard de la GSMA. C'est en février 2016 que la GSMA a publié une première version des spécifications de l'eSIM pour permettre aux consommateurs d'ajouter les équipements de nouvelle génération (montre connectée, bracelets de fitness, trackers, etc.) à un abonnement mobile et les connecter de façon sécurisée à un réseau mobile. La deuxième version publiée en novembre 2016 a été étendue aux smartphones et tablettes. Ainsi, un utilisateur peut enregistrer dans son équipement mobile plusieurs profils opérateurs et faire le meilleur choix de réseau au moment opportun sans avoir à acquérir une nouvelle carte SIM.

L'eSIM est donc au final une carte SIM intégrée à un équipement (mobiles, tablettes ou objets connectés) et reprogrammable au besoin.

Selon Silicon.fr[1], la nécessité d'une SIM embarquée s'est fait d'abord sentir chez les constructeurs automobiles pour des questions de fiabilité du composant en regard des vibrations et risques de chocs des véhicules. Ainsi, pour répondre aux besoins des applications machine-to-machine (M2M), la MIM (Machine Identification Module) a été standardisée en 2010.

Conscient des risques de transformation du marché, la GSMA va lancer en 2014 des travaux sur le téléchargement à distance des identifiants de connexion qui aboutiront en février 2016 sur les premières spécifications eSIM.

Les spécifications de l'eSIM sont dites RSP (pour Remote SIM provisioning) et permettent de mettre en œuvre le téléchargement à distance de manière sécurisée de l'ensemble des paramètres de l'opérateur dans l'eSIM.

On distingue aujourd'hui trois types de SIM dits de nouvelle génération résultats des propositions ou expérimentations de l'industrie :

- Les SIM intégrés ou eSIM : une carte SIM physique intégrée de manière permanente dans l'appareil ;
- Les Cartes SIM 'reprogrammables' à distance : carte SIM qui peut être retirée de l'appareil (par exemple, Apple SIM) et reprogrammée pour adopter le profil d'un opérateur donné ;
- Les Soft SIM : collection d'applications logicielles et de données qui résident dans la mémoire et le processeur de l'appareil et qui dotent celui-automatiquement de fonctionnalités à l'image d'une carte SIM reprogrammable.

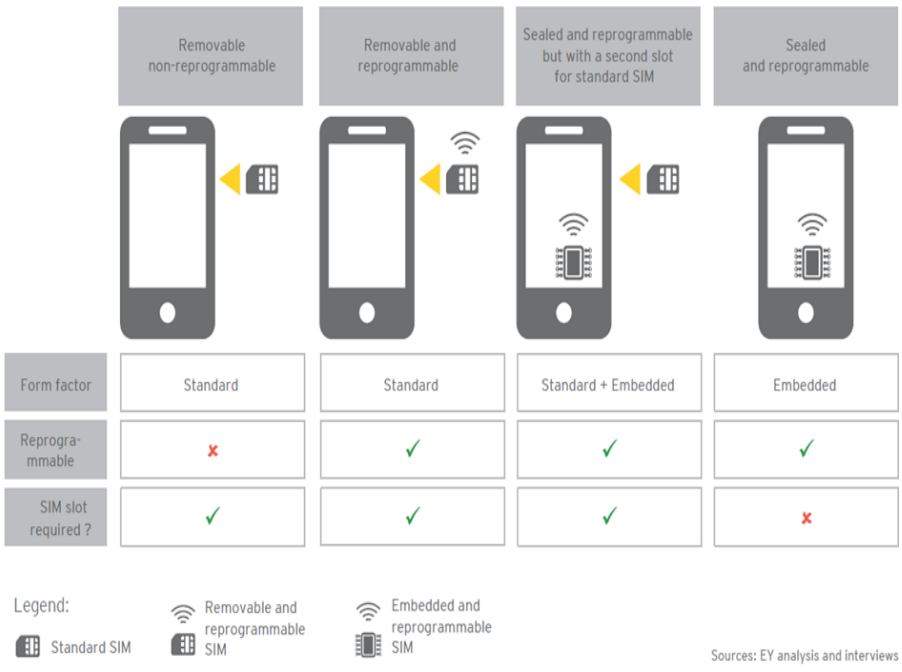


Figure 1 - Exemple de SIM de nouvelle génération

Pour Alex Sinclair de la GSMA, l'eSIM est « la seule spécification globale et interopérable qui a le soutien de l'industrie mobile »[2]. Mais s'il y a une chose qui les lie toutes, c'est la particularité pour ces cartes SIM de nouvelle génération d'être reprogrammée à distance.

De la resistance de l'industrie a l'acceptation

En 2011, Apple a breveté aux USA[3] une plateforme sur laquelle les opérateurs de réseaux mobiles proposeraient de façon concurrente les offres de services de leur réseau à destination des appareils de la marque.

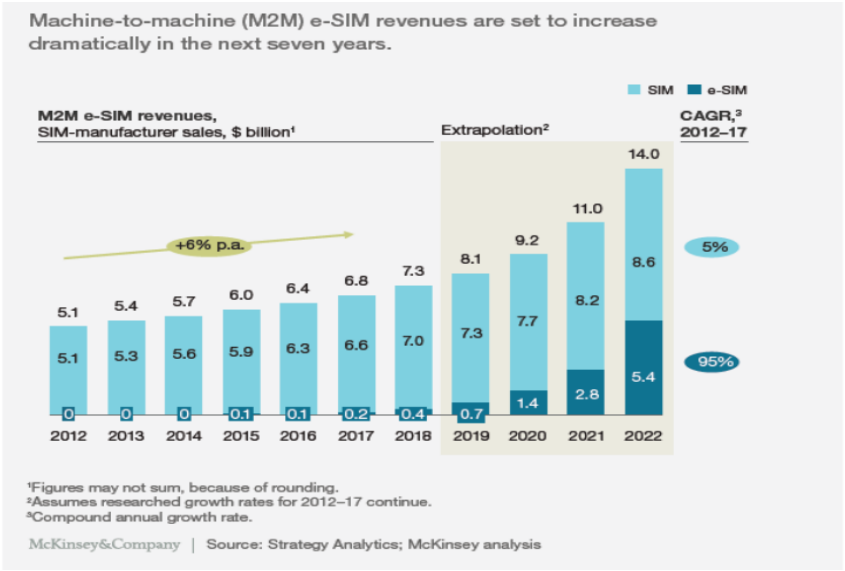
quelque peu résistants face à ces changements. Cette réticence est attribuable au fait que les opérateurs ont toujours été en contact direct avec leurs clients quel que soit le terminal utilisé. L'introduction de l'eSIM entrainerait certainement l'effritement sinon la disparition de ce lien très étroit avec l'abonné.

A l'époque, cette nouvelle technologie d'Apple venait perturber l'industrie car la fonctionnalité de carte SIM reprogrammable permettait aux utilisateurs des appareils Apple de choisir parmi une multitude de profils d'opérateur disponibles.

Aujourd'hui, l'industrie réagit beaucoup plus favorablement aux eSIM. Le GSMA représente l'un des catalyseurs de ce changement à travers la promotion auprès des acteurs de l'écosystème d'une architecture de référence normalisée afin d'introduire les eSIM.

Figure 2 - Acteurs soutenant l'initiative eSIM de la GSMA

Trois ans plus tard, en 2014, Apple a lancé sa propre carte SIM, la carte Apple SIM. Intégrée dans les tablettes iPad Air 2 et iPad Mini 3, au Royaume-Uni et aux États-Unis, cette Apple SIM reprogrammable permet aux clients de sélectionner un opérateur de réseau de mobile de manière dynamique, directement à partir de l'appareil. Cette technologie accorde aux utilisateurs plus de liberté en ce qui concerne la sélection du réseau. Elle a également changé le paysage concurrentiel des opérateurs.



Les acteurs de l'industrie ont été

Par ailleurs, en raison du développement de l'Internet des Objets et des applications M2M, le revenu des eSIM devrait être presqu'équivalent à celui des cartes SIM traditionnelles d'ici 2022 (8.6 milliards $ pour les cartes SIM traditionnelles contre 5.4 milliards $ pour les eSIM selon McKinsey).

Le marché de l'eSIM devrait bénéficier de l'industrie du M2M considérant que les gadgets et futurs appareils connectés seront majoritairement équipés de cette technologie leur permettant de façon autonome de choisir un réseau plutôt qu'un autre.

ARCHITECTURE

Les spécifications de la GSMA restent la première et unique spécification de l'eSIM.

C'est une architecture sécurisée qui permet de télécharger un profil et de l'installer sur son équipement. L'eSIM permettra donc aux usagers de changer d'opérateur sans avoir à remplacer la puce. Cette architecture induit indubitablement un gain de temps et une plus grande souplesse aussi bien pour les clients que pour les fabricants. En outre l'effectivité de la mise en œuvre de l'eSIM est une opportunité pour les équipementiers pour affiner le design des terminaux débarrassés d'un logement pour une SIM amovible. Cette architecture intégrée commune permettra aussi le développement de nouvelles gammes de produits du type Internet des Objets.

Trois nouveaux équipements se déclinent pour gérer les eSIM dans la norme déclinée par le GSMA :

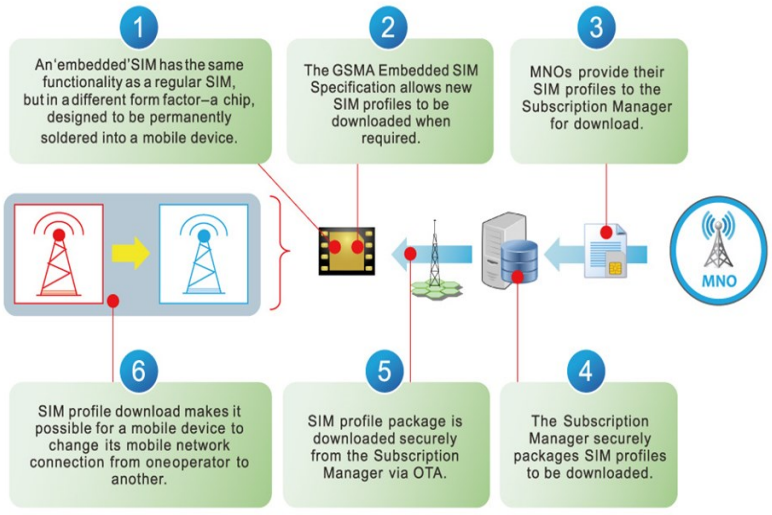


Figure 3 - Architecture simplifiée du GSMA de fonctionnement de l'eSIM

UNITÉ DE GÉNÉRATION DE PROFIL (PROFIL GENERATION UNIT)

La génération de profil eSIM utilisera les mêmes méthodes que celles utilisées pour les profils SIM habituels. Les fournisseurs de cartes SIM utilisent habituellement les détails d'authentification fournis par les opérateurs de réseau mobile pour générer des clés exclusives d'accès au réseau. Plutôt que de stocker ces détails sur les cartes SIM physiques, elles seront uniquement sauvegardées sous forme numérique dans les unités de génération de profil et attendront une demande de Téléchargement déclenchée par le circuit intégré universel intégrée (e-UICC) dans le terminal.

UNITÉ DE DISTRIBUTION DE PROFIL (PROFILE DELIVERY UNIT)

La connexion entre l'e-UICC dans l'appareil et le service de génération de profil est établie par l'unité de distribution de profil, qui est responsable du cryptage du profil généré avant qu'il puisse être transmis au terminal. Bien que théoriquement tous les participants au nouvel écosystème eSIM puissent délivrer le service de distribution de profil, les plus susceptibles de le faire seront les fournisseurs de SIM ou les opérateurs de réseau mobile - physiques et virtuels.

Unité de distribution de profil (Profile delivery unit)

Les équipements terminaux disposant d'une technologie eSIM peuvent au préalable n'être associés à aucun réseau mobile, ou encore avoir un réseau présélectionné. Dans tous les cas, une option devrait permettre de choisir parmi plusieurs fournisseurs. Le serveur universel de découverte joue un rôle central car il est l'équipement responsable qui établira le lien entre les terminaux et les unités de gestion des profils afin de visualiser les différents fournisseurs. Il est préférable que la découverte des profils soit réalisée par un acteur indépendant afin de s'assurer que tous les profils disponibles sur un marché (sans restrictions sur les tarifs et les opérateurs) sont présentés.

In fine, l'architecture des serveurs UD peut être assimilée (ou comparable) à celle des serveurs DNS.

Evolution du marché

L'avènement de l'eSIM induit de nouveaux modèles d'affaires et une reconfiguration de la chaine de valeur.

L'utilisation des eSIM signifie que les fabricants de puces négocient directement avec les fabricants d'équipements d'origine tels qu'Apple et Samsung plutôt qu'avec les opérateurs de réseaux mobiles. La fabrication et la distribution de cartes SIM physiques risquent de devenir à terme obsolètes. Les fabricants de cartes SIM traditionnelles pourraient donc se positionner comme les acteurs les mieux outillés, de par leur expérience, sur les éléments clés de l'architecture telle que la gestion du service de génération de profils.

Les cartes SIM physiques, cependant, ne devraient pas disparaître du marché au cours des prochaines années. Les cartes SIM traditionnelles et la nouvelle norme devraient coexister pendant un long moment.

La carte SIM traditionnelle demeure, depuis l'avènement de la téléphonie mobile, un mécanisme efficace pour lier un client à un opérateur. L'eSIM offre l'opportunité au consommateur de choisir à volonté des réseaux basés sur des critères tels que le coût, la vitesse et la qualité de service. Cette option dispense ainsi le consommateur de posséder plusieurs cartes SIM et incite à une plus grande transparence tarifaire.

Quel impact sur les opérateurs de téléphonie mobile?

La plupart des opérateurs de réseau mobile ont déjà lancé des études pour évaluer non seulement l'impact des exigences architecturales de l'eSIM sur leurs réseaux, y compris les modifications apportées aux systèmes et procédés informatiques existants, mais aussi l'effet potentiel sur le marketing et la création de valeur, etc.

Le tableau ci-après, donne quelques changements qui pourraient subvenir au niveau des opérateurs de téléphonie mobile :

- **Coût** : Une diminution potentielle des coûts de fabrication et de distribution des cartes SIM pour les opérateurs.
- **Le client est Roi** : Comme il sera plus facile pour un consommateur de changer d'opérateurs, la concurrence au niveau des prix peut devenir le principal facteur de différenciation. Un

consommateur pourrait s'abonner à plusieurs opérateurs en fonction de plusieurs endroits différents dans un pays. Ce qui constitue un manque à gagner pour les opérateurs.

- **Marketing & Ventes** : La facilité de changement d'opérateurs réseaux peut affaiblir la position de certains opérateurs mobiles dominants qui peuvent voir leurs marges se réduire. Cette situation soulève un risque de subventions croisées.
- **Roaming** : L'une des plus grandes perturbations induites par le eSIM pourrait avoir lieu au niveau de l'itinérance (nationale et internationale). Les tarifs en itinérance encore élevés dans certaines régions du monde par rapport aux tarifs internationaux, le voyageur en itinérance pourra en quelques clics choisir un opérateur local qui propose des tarifs internationaux plus attractifs. Au niveau national, l'utilisateur choisira de façon dynamique l'opérateur disposant de la meilleure couverture ou de la meilleure qualité de services dans une région donnée.
- **Points de contact clients** : Les eSIM éliminent la nécessité pour les clients d'aller en boutique et d'acquérir une carte SIM lors de la mise en service. Les interactions face-à-face dans les « magasins/agences » sont des occasions d'influencer les décisions des clients. Partant de ce constat, les opérateurs devront évaluer l'impact potentiel de la perte de cette absence de contact client et envisager de nouvelles façons d'attirer ou de fidéliser les clients.
- **Marchés prépayés** : Il est tentant de dire que les marchés prépayés seront moins impactés vu la flexibilité déjà offerte par ce type d'abonnement. L'eSIM pourrait être une solution pour l'abonné prépayé en lui évitant de recourir à plusieurs cartes SIM pour bénéficier des meilleures offres comme c'est le cas actuellement sur la plupart des marchés émergents.

QUEL IMPACT RÈGLEMENTAIRE?

La modification de l'environnement avec l'avènement de l'eSIM fait naître un certain nombre de questions qui constituent de véritables enjeux pour les régulateurs de télécommunications :

- **Ressources de numérotation** : L'une des premières questions de fond reste la gestion de la numérotation. Vu que l'équipement peut choisir dynamiquement le réseau, cela suscite plusieurs interrogations parmi lesquelles: quel opérateur sera censé régler la redevance lié à la numérotation ? y aurait-il une chambre de compensation ? quel impact sur la portabilité des numéros ?
- **Identification de l'abonné** : L'identification des abonnés est opérée physiquement lors de l'achat de cartes SIM. Avec les possibilités offertes par la technologie eSIM, comment le processus d'identification des abonnés sera-t-il impacté ?

- **MVNO** : La prolifération des eSIM va favoriser la concurrence entre MVNO et opérateur traditionnel en créant probablement un «marché au comptant». Le MVNO pourra être le tiers chargé de fournir une technologie intermédiaire qui oriente le basculement d'un équipement vers un réseau sur la base d'une évaluation dynamique de plusieurs réseaux en fonction du coût, de la congestion et de la puissance du signal.. Partant de ce cas d'utilisation, un MVNO pourrait s'engager auprès de plusieurs opérateurs de réseau et fournir des tarifs finaux compétitifs au consommateur final sans pour autant révéler l'identité de l'opérateur en amont sur lequel il s'appuie.

AUTRES CHANGEMENTS

- **Fabricants d'objets connectés** : Les fabricants d'objets connectés ont la possibilité d'intégrer une e-SIM vierge dans le terminal qui peut être activé quelque soit le réseau dans n'importe quel pays. Cela offre aux fabricants la possibilité d'être directement en contact avec les consommateurs et réduit de facto l'intermédiation des opérateurs avec tous les coûts afférents.
- **OTT** : Les OTT devront être les grands bénéficiaires de cette technologie. La possibilité de switcher entre les réseaux en leur sera d'un grand avantage vu que ces services sont fournis sur la base d'Internet.

CONCLUSION

Les applications machine-to-machine (M2M) utilise avec succès depuis plusieurs années l'architecture de la SIM embarquée. Les premiers produits grand public utilisant l'eSIM sont attendus pour 2017 sans pour autant sonner le glas de la carte SIM traditionnelle qui devrait encore exister pendant un bout de temps en attendant que l'industrie adopte complètement l'eSIM.

L'eSIM bouleversera va sans aucun doute l'industrie des télécommunications et apportera certainement plus de souplesse non seulement aux utilisateurs mais aussi aux opérateurs mobiles. Les fabricants de carte SIM y trouveront aussi leur compte en faisant bénéficier au marché de l'eSIM leur expertise acquise dans le domaine des SIM traditionnelles.

Cependant, d'une manière ou d'une autre, l'équilibre du marché pourrait être rompu.

Les nouveaux entrants et business model relatif aux eSIM auront un impact non négligeable sur le marché des télécommunications mobiles et de l'Internet des Objets au cours des deux à cinq prochaines années.

La régulation devra donc anticiper les évolutions à venir afin de répondre efficacement aux problématiques soulevées par la technologie eSIM.

Notes et références

1. http://www.silicon.fr/esim-carte-sim-embarquee-saliver-gemalto-165485.html
2. http://www.gsma.com/newsroom/press-release/gsma-releases-remote-provisioning-specification/
3. Tony Fadell. Dynamic carrier selection. US Patent 20,110,130,140, filed February 7, 2011, and issued June 2, 2011.
4. http://www.itespresso.fr/esim-supplanter-carte-sim-samsung-gear-s2-classic-121869.html#
5. http://www.businesswire.com/news/home/20160218005061/en/GSMA-RELEASES-REMOTE-PROVISIONING-SPECIFICATION-CONSUMERS-CONNECT
6. http://www.gsma.com/rsp/
7. http://www.gsma.com/rsp/2017/01/04/mobile-world-congress-2017-seminar-esim-new-sim-new-generation-connected-consumer-devices/
8. http://www.zdnet.fr/actualites/esim-un-nouveau-modele-pour-les-operateurs-39822662.htm
9. https://assistance.orange.fr/objets-connectes/installer-et-utiliser/montres/samsung/samsung-gear-s2-3g-esim/debuter-et-prendre-en-main/activer-votre-montre/carte-esim-presentation_193694-738518
10. http://www.pocket-lint.com/news/134640-what-is-an-esim-and-how-will-it-change-smartphones-for-the-better
11. https://www.mouchardgps.fr/tout-savoir-sur-les-cartes-sim
12. http://www.lexpress.fr/actualite/societe/qui-etait-roland-moreno-l-inventeur-de-la-carte-a-puce_1109970.html
13. http://www.mckinsey.com/industries/telecommunications/our-insights/e-sim-for-consumers-a-game-changer-in-mobile-telecommunications
14. https://fr.wikipedia.org/wiki/International_Mobile_Equipment_Identity
15. http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/
16. http://www.gsma.com/managedservices/mobile-equipment-identity/about-imei/
17. http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database/
18. http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/operator-best-practices/
19. http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/coloured-lists/
20. http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-advice-for-mobile-phone-users/mobile-phone-theft
21. http://www.imei.info/
22. https://drfone.wondershare.com/fr/imei/imei-check-online.html
23. http://www.gsmforum.tv/-deblocage-reparation-iphone-2g-3g-3gs-4-4s/22662-meilleure-site-de-check-iphone-imei.html
24. http://www.tutoriels-android.com/2015/11/comment-reconnaitre-un-vrai-smartphone-d-un-clone.html
25. https://www.micromagma.ma/guide/dossiers/item/6414-comme-reconnaitre-un-vrai-smartphone-d-une-contrefacon
26. http://www.prodigemobile.com/tutoriel/reperer-smartphone-contrefacon/
27. http://www.androidpit.fr/comment-reconnaitre-faux-smartphone
28. http://www.phonandroid.com/comment-reperer-smartphone-contrefacon.html

La contrefaçon des équipements TIC

LA CONTREFAÇON

INTRODUCTION

D'une façon générale, la contrefaçon est un phénomène présent dans la quasi-totalité des secteurs d'activités. Selon 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 environ 600 milliards USD par an[1]. Ce qui représente un manque à gagner non négligeable pour le secteur privé et pour les Etats. Cependant, les conséquences de la contrefaçon ne sont pas qu'économiques. La contrefaçon a aussi un impact sur la santé et la qualité de service pour les consommateurs. Pour ce qui concerne spécifiquement le domaine des TIC, on note une prolifération inquiétante de produits contrefaits, et ce, sur toutes les gammes de produits.

Alors que la contrefaçon a des conséquences indéniables sur nos sociétés, et malgré les actions déjà entreprises, les pays en développement ne sont pas encore arrivés à maîtriser le phénomène de sorte à proposer des solutions de lutte probantes pour endiguer ce phénomène.

QU'EST-CE QU'UN ÉQUIPEMENT TIC CONTREFAIT?

Globalement, l'opinion publique ne fait pas de différence entre les équipements dits contrefaits et ceux dits non conformes car non homologués. On parle de contrefaçon uniquement quand les droits à la propriété intellectuelle sont violés. Ainsi, 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 » comme « 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 peuvent être

distinguée dans ses aspects essentiels de cette marque de fabrique ou de commerce, et qui de ce fait portent 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 de l'accord sur les ADPIC).

Plus spécifiquement, les dispositifs TIC concernés par cette contrefaçon sont de tout ordre et vont des téléphones portables qui représentent manifestement la cible principale des contrefacteurs, aux ordinateurs sans oublier leurs composants : puces, batteries, accessoires… tout y passe.

COMMENT SE DÉCLINE LA CONTREFAÇON?

Le phénomène de la contrefaçon est appuyé par un large réseau de distribution dont il est difficile de mesurer l'étendue. C'est le « black market » ou « marché noir ». De nos jours, ce réseau repose fortement sur Internet. Le moindre qu'on puisse dire, c'est que le marché ivoirien n'est pas en reste.

L'industrie de la contrefaçon en ligne est désormais aux mains de véritables réseaux qui posséderaient une capacité d'investissement importante. Le commerce électronique constitue une véritable aubaine pour eux. Ainsi, ils développent depuis quelques années, de véritables stratégies marketing et de référencement sur Internet. Avec l'accessibilité à Internet et aux réseaux sociaux à tous, les revendeurs bénéficient d'une plateforme libérale qui, conjuguée à l'anonymat, favorise le développement de la vente illicite des équipements contrefaits.

De plus, pour l'extension de leurs activités, les contrefacteurs ou vendeurs de produits contrefaits ne ciblent plus seulement les amateurs de « faux » mais aussi les consommateurs en quête de bonnes affaires, facilement dupés par leurs interlocuteurs aux allures toujours plus « professionnelles » et « légitimes ».

Outre Internet pour échapper au paiement d'impôts, les contrefacteurs profitent également de la porosité des frontières physiques. En effet, la plupart des pays en développement ne disposent pas de moyens technologiques efficaces pour contrôler l'entrée des équipements et composants TIC selon les normes internationales. Par conséquent, le filtrage aux frontières est peu efficace.

LES CONSÉQUENCES DE LA CONTREFAÇON

Dans son rapport technique sur la contrefaçon d'équipements TIC, l'UIT montre que la contrefaçon des équipements TIC a une conséquence particulière sur la société que n'ont pas nécessairement d'autres types de violations des droits de propriété intellectuelle. Et pour cause, globalement, les produits de contrefaçon sont des produits qui n'ont pas été testés en bonne et due forme, ni homologués conformément aux prescriptions réglementaires applicables. Ce qui confère à ces produits un caractère dangereux étayé notamment par des cas de décès[2] suite à l'explosion de batteries supposées contrefaites, 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).

Quoique généralisé, le phénomène de la contrefaçon touche beaucoup plus les téléphones mobiles. Notons que dans le secteur des TIC,

environ 250[3] millions de téléphones mobiles de contrefaçon se vendent chaque année, ce qui représente près de 15 à 20% du marché mondial. Dès lors, avec la croissance de la téléphonie mobile, les conséquences de la contrefaçon dans le secteur des TIC se sont décuplées. Ces effets pervers sont perceptibles à plusieurs niveaux.

Sur le plan technique, les téléphones de contrefaçon, en raison de leurs tarifs abordables, ont surement contribué à l'accroissement de la télédensité (nombre de téléphones par rapport au nombre d'habitants) notamment dans les pays en développement. Même si cet essor représente un avantage pour le secteur des télécommunications, il provoque néanmoins une baisse de la qualité des services de communications, qui influe à son tour sur l'expérience-utilisateur. Par exemple, des travaux de recherche du Mobile Manufacturers Forum (MMF) mettent en évidence une qualité de fonctionnement peu satisfaisante des réseaux télécoms due aux téléphones de contrefaçon : interruption d'un appel sur quatre, délai de transfert et échec de transfert dans le cas d'un transfert sur trois.

Sur le plan socio-économique, les dispositifs TIC de contrefaçon peuvent avoir des conséquences fâcheuses. Pour le secteur privé, ils entraînent un manque à gagner, une dépréciation de l'image et de la réputation de la marque commerciale et une diminution de la confiance des consommateurs finaux. Aussi, les pratiques de concurrence déloyale, étant donné le volume des ventes et les bas prix pratiqués, entraînent une distorsion du marché. Pour les pouvoirs publics, l'impact se traduit par une perte de recettes et de droits de douane et une diminution des recettes fiscales. Par ailleurs, l'Etat risque fort d'être confronté à des problèmes de corruption qui l'obligeraient à mobiliser davantage de ressources pour contrer le phénomène de la contrefaçon. Plus loin, la forte pénétration des équipements TIC contrefaits peut être un frein à l'innovation et aux investissements directs étrangers.

Sous l'angle des incidences sécuritaires, les dispositifs contrefaits constituent potentiellement une menace grave pour la confidentialité et la sécurité des transactions numériques par conséquent pour la vie privée des consommateurs. En outre, la contrefaçon est très liée au phénomène de contrebande, vecteur d'activités criminelles et du terrorisme.

Pour ce qui est des questions liées à la santé, les équipements contrefaits peuvent être dommageables pour la santé des consommateurs en raison des fortes concentrations de substances dangereuses utilisées dans la fabrication de ces dispositifs (Taux de plomb, 35 à 40 fois supérieures aux limites autorisées au niveau mondial[4]). Le risque pour la santé est aussi lié au fait que les produits de contrefaçon peuvent avoir des DAS (débit d'absorption spécifique) supérieurs à la norme (1,6W/kg pour 1 gramme de tissu aux USA et 2W/kg pour 1 gramme de tissu dans l'UE).

Enfin, l'environnement peut s'en voir affecté. En effet, les dispositifs contrefaits peuvent 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 tel que recommandé par la Convention de Bâle sur la gestion rationnelle des appareils usagers et en fin de vie. C'est le cas des 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.

COMMENT RECONNAÎTRE UN PRODUIT CONTREFAIT ?

Cette démarche s'avère de plus en plus compliquée car les contrefacteurs se « professionnalisent ». Pour l'e-consommateur même expérimenté, il est difficile de faire la distinction entre les sites proposant des produits authentiques et ceux présentant des faux car tout a été minutieusement conçu pour le rassurer. Ces sites sont de très bonne qualité en terme d'ergonomie et entièrement calqués sur le modèle de la marque de base. Ils ont des noms de domaines tels *(nomdelamarque) sale.net* ou encore *(nomdelamarque) officialoutlet.com*. A l'image de la marque officielle, ils offrent les mêmes services de conditions de retour, de paiement voire d'assistance technique multilingue, le tout couronné par des abonnements souvent imaginaires à des newsletters. Quant aux prix, ils sont affichés avec une remise de 25 à 75% rarement au-delà, en vue de faire croire à des soldes ou un déstockage massif. Outre cela, les modèles contrefaits sont souvent en vente lorsque la marque officielle annonce une rupture de stock ou un retrait du marché.

Par ailleurs, il existe d'autres moyens plus simples de vérification de l'authenticité des articles. Pour ce faire, il suffit de porter une attention particulière à :

- L'URL de la page : un site sécurisé devrait inclure le protocole 'https'.
- La localisation du site c'est-à-dire s'il est hébergé ou non dans un pays reconnu comme origine de produits de contrefaçon.
- L'existence du produit dans les catalogues en ligne de la marque originelle.
- Les adresses email sur des serveurs de messagerie public, de type 'Gmail' ou 'Hotmail'….

Dans le cadre des échanges physiques, en plus des moyens de détection déjà suggérés, il est également possible à différents égards de tester l'authenticité des équipements TIC.

Dans le cas d'un téléphone portable, de nombreuses astuces en ligne peuvent aider à repérer une contrefaçon. En voici quelques-unes :

- D'abord, bien se renseigner sur le produit à acheter. Le site spotafakephone.com du Mobile Manufacturers Forum (MMF) indique que le consommateur devrait se familiariser avec les caractéristiques et les fonctionnalités des articles authentiques. Une fois les informations en main, il suffit alors de vérifier qu'elles correspondent au modèle visé.
- L'autre astuce est de vérifier la validité du numéro IMEI. Celui-ci est normalement visible sur la coque, la batterie ou sur le coffret, sinon taper le code *#06#. Pour la vérification, plusieurs sites web existent. Wondershare.com dresse par exemple une liste des 5 meilleurs[5] sites web pour faire une vérification IMEI en ligne. Le plus connu et le plus utilisé est IMEI.INFO (http://www.imei.info) sans doute à cause de sa facilité d'utilisation et la prise en charge d'un grand nombre d'appareils.
- Enfin, se méfier des prix bas. Il ne faut pas succomber d'emblée au prix beaucoup trop avantageux. Il faut prendre des précautions si l'appareil est

proposé à un tarif plus bas que celui annoncé par le constructeur.

MESURE DE LUTTE CONTRE LA CONTREFAÇON

Quoique des équipements contrefaits soient facilement détectables, il arrive qu'on ne puisse pas différencier la copie de l'original. Par ailleurs, les logos d'homologation et les icônes sont souvent détournés à dessein, afin d'éviter les contrôles douaniers. Ce qui ne favorise pas souvent les opérations de contrôle même s'il convient de noter qu'il arrive que des produits de contrefaçon soient conformes aux prescriptions réglementaires.

C'est fort de cela que des mécanismes d'identification et des dispositifs de sécurité ont été développés comme méthodes de lutte imparables contre la contrefaçon. On y dénombre :

- **Identité internationale d'équipement mobile (IMEI)** : c'est un numéro à 15 chiffres qui permet d'identifier de manière unique un téléphone mobile. Le système d'attribution des numéros IMEI est hiérarchique et géré par la GSMA : 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. La GSMA tient à jour la base de données IMEI qui contient une « liste blanche » des équipements considérés comme pouvant être utilisés dans le monde entier, une « liste grise » et une « liste noire » des dispositifs non autorisés 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 (Type Attribution Code) 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 opérateurs de réseaux peuvent mettre en œuvre leurs propres registres d'identification des équipements (EIR), dans lesquels ils peuvent télécharger la « liste blanche » pour leur permettre de contrôler les dispositifs qui accèdent à leurs réseaux.

Tableau - Format des numéros IMEI

Code d'attribution	Numéro de	Somme de
NNXXXX YY	ZZZZZZ	A

TAC	Code d'attribution type, précédemment connu sous l'appellation "code d'homo-
NN	Identifiant de l'Entité de notification.
XXXXYY	Identifiant du type d'équipement mobile
ZZZZZZ	Attribué par l'Entité de notification, mais assigné pour chaque équipement ME
A	Somme de contrôle, définie en fonction

- **Identifiants uniques :** Ils sont appelés « codes produit électroniques (EPC) ». Ils permettent d'identifier un objet dans une chaîne de production. Ils sont gérés par EPCglobal[6], organisation qui aide à définir les spécifications applicables aux systèmes mondiaux de chaîne d'approvisionnement.
- **Identification et captage de données automatiques (AIDC)**
  - **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.
  - **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.
- **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.
- **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.
- **Tests** : La Commission électrotechnique internationale (CEI) dirige les systèmes d'évaluation de la conformité[7] : i) IECEE – Système CEI d'évaluation de la conformité des équipements et des composants électrotechniques ; ii) IECEx – Système CEI de certification de conformité aux normes des matériels électriques destinés à être utilisés en atmosphères explosives; iii) 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.
- **Surveillance des marchés** : 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. 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.

LIGNES SUR LA LUTTE CONTRE LA CONTREFAÇON

Pour lutter contre la contrefaçon, plusieurs organismes - équipementiers et distributeurs, organismes publics et instances chargées de faire respecter, consommateurs – proposent des lignes directrices.

Pour endiguer effectivement le phénomène de la contrefaçon des équipements TIC, le Mobile Manufacturers Forum (MMF) a élaboré un Guide de ressources à l'intention des gouvernements. Ces directives vont plus loin que l'action coercitive traditionnelle et consiste plutôt à bloquer les dispositifs contrefaits pour qu'ils ne puissent pas fonctionner sur les réseaux. Elles visent globalement à :

- 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.

Un certain nombre de bonnes pratiques[8] sont proposées par l'Anti-Counterfeiting Forum (ACF). Elles participent à renforcer les mesures générales. Leur objectif est de :

- 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;

- améliorer la traçabilité des produits en utilisant des identificateurs uniques et en contrôlant la documentation.

EXEMPLE DE MESURES DE LUTTE CONTRE LA CONTREFAÇON

Pour lutter contre la contrefaçon, plusieurs mesures sont prises à travers. Ces exemples ci-après sont tirés de la deuxième version du rapport technique de l'UIT[9] intitulé "Contrefaçon d'équipements TIC" approuvée lors de la réunion de la Commission d'études 11 de l'UIT-T tenue à Genève du 2 au 11 décembre 2015.

Pour plus de détails concernant ces exemples et pour d'autres exemples, veuillez-vous référer au document susmentionné.

BRÉSIL

Au Brésil, l'ANATEL (Agence nationale des télécommunications du Brésil) 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.

A la suite d'un plan d'action soumis par les opérateurs et approuvé par l'ANATEL en 2012, une solution technique baptisée SIGA (Système intégré de gestion des dispositifs) a été mise en place.

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, 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.

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.

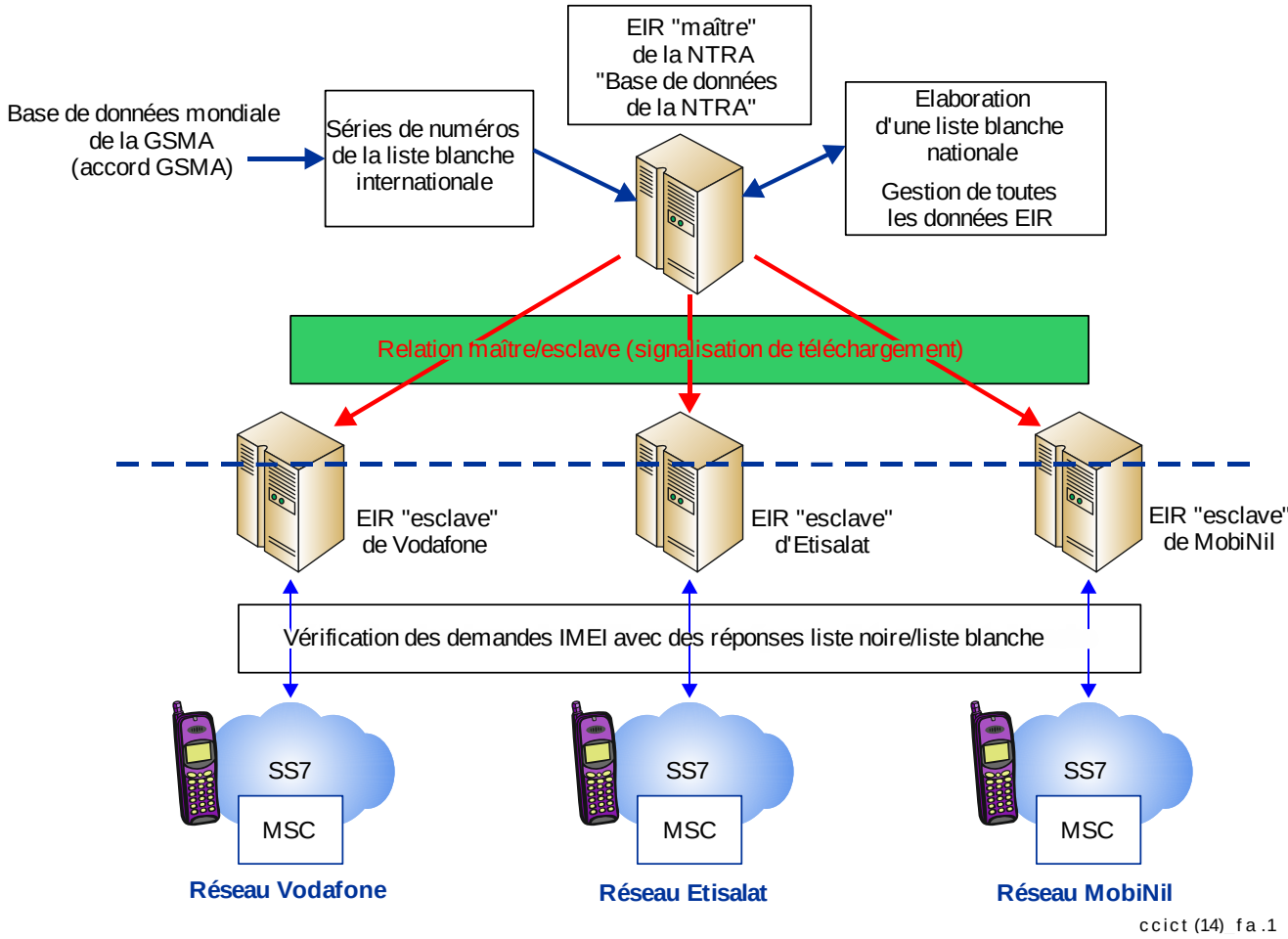


Figure 2 - Solution de base de données centrale EIR IMEI en Egypte

INDONÉSIE

Par décret N° 81/2012 du Ministère de l'industrie et du décret N° 82/2012 du Ministère du commerce, l'Indonésie a durci, en 2013, les conditions régissant l'importation de téléphones cellulaires 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.

OUGANDA

La Commission des communications de l'Ouganda (UCC) a lancé un projet visant à supprimer progressivement les téléphones de contrefaçon du marché national.

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 œuvre suivantes:

- 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 œuvre 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 œuvre 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 œuvre 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.

ACTIVITÉ 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)[10]. 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 poursuivent 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[14] : "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'Union Internationale des Télécommunication (UIT) joue aussi un rôle dans l'étude de la question de la contrefaçon des équipements TIC.

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"[12].

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)[13] 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. Cette commission a approuvé le 15 février 2017, la première version de son rapport technique intitulé « rapport d'enquête sur la contrefaçon des équipements TIC en Afrique ». Ce rapport recommande la mise en place d'un groupe régional africain de la CE 11 de l'UIT.

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 (CE 5) 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) [14] sur les DPI 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.

Le CE 1 du Secteur du développement des télécommunications de l'UIT (UIT-D), le Groupe consultatif de la normalisation des télécommunications de l'UIT-T (GCNT) émettent également des avis sur le caractère préoccupant de la contrefaçon d'équipements.

QUE RETENIR?

Le phénomène de la contrefaçon est une réalité et ses conséquences socio-économiques le sont tout autant.

Avec environ 250 millions de téléphones mobiles de contrefaçon vendus chaque année, soit 15 à 20% du marché mondial, l'impact économique de la contrefaçon est considérable. Cependant, outre les conséquences économiques évidentes, la contrefaçon représente un risque pour la santé, la sécurité et la vie privée des consommateurs et a des incidences négatives sur les réseaux des opérateurs (baisse de la qualité de service, risques de brouillages, problèmes de compatibilité électromagnétique (CEM) et interruption du réseau).

Dans les pays en développement peu regardants sur la qualité, ceci est d'autant plus vrai que les produits vers ses destinations sont fabriqués avec des composants de qualité inférieure. C'est le phénomène de « tropicalisation ».

Pour lutter contre la contrefaçon, des mécanismes

de surveillance du marché doivent être mis en œuvre pour un contrôle rigoureux de la chaîne d'approvisionnement et du cycle de vie des équipements TIC.

Aujourd'hui, la plupart des mesures de lutte contre la contrefaçon des terminaux mobiles s'appuient sur les numéros IMEI. La base de données IMEI constitue un instrument permettant de détecter les dispositifs mobiles de contrefaçon. Mais les problèmes constatés - équipements dépourvus de numéros IMEI ou comportant un numéro IMEI exclusivement constitué de zéros, des numéros IMEI en double ou encore des numéros IMEI attribués par des organismes non autorisés – montrent que la procédure d'attribution des numéros IMEI établie par la GSMA n'est pas infaillible. Il est donc primordial 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.

Faudrait-il donc bloquer les numéros IMEI non conformes ou en double ? Surement pas…

L'alternative serait 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. Il faut pour cela 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.

En définitive, 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, il est à noter que : « 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 ».

Notes et références

1. http://www.icc-ccs.org/icc/cib
2. https://www.contrefacon-riposte.info/securite-des-consommateurs/1041-chine-un-homme-tue-par-lexplosion-de-son-telephone-mobile
3. Rapport technique de l'UIT-T, « *Contrefaçon des TIC* » approuvé lors de la réunion de la Commission d'études 11 de l'UIT-T tenue à Genève du 2 au 11 décembre 2015
4. Centre for Materials for Electronics Technology (C-MET), Inde (Hyderabad)
5. https://drfone.wondershare.com/fr/imei/imei-check-online.html
6. http://www.rfidfr.org/glossaire/byname.epc.php
7. http://www.CEI.ch/about/activities/conformity.htm
8. http://www.anticounterfeitingforum.org.uk/best_practice.aspx
9. http://www.itu.int/pub/T-TUT-CCICT-2015
10. ISO 12931:2012, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*.
11. ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.
12. http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf.
13. http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx.
14. http://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx
15. http://www.itu.int/pub/T-TUT-CCICT
16. http://www.itu.int/pub/T-TUT-CCICT-2014
17. http://www.itu.int/pub/T-TUT-CCICT-2015
18. http://www.itu.int/pub/T-TUT-CCICT-2017

Le service Veille Technologique rattaché à la Direction de l'Economie et marchés, de la Prospective et des Statistiques (DEPS) de l'ARTCI scrute le paysage des TIC afin de déterminer de nouveaux sujets d'informations. Ces sujets permettent d'analyser l'actualité du secteur, de mieux comprendre les enjeux de la régulation et l'impact des TIC dans la vie de tous les jours.

ARTCI
AUTORITE DE REGULATION DES TELECOMMUNICATIONS/TIC DE COTE D'IVOIRE

Avril 2017

Abidjan , Côte d'Ivoire