Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Q.5051

(03/2020)

SÉRIE Q: COMMUTATION ET SIGNALISATION ET MESURES ET TESTS ASSOCIÉS

Lutte contre la contrefaçon et le vol d'équipements TIC

Cadre pour la lutte contre l'utilisation de dispositifs mobiles volés

Recommandation UIT-T Q.5051

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION ET MESURES ET TESTS ASSOCIÉS

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4, 5, 6, R1 ET R2	Q.120–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.799
INTERFACE Q3	Q.800–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	Q.1700–Q.1799
SPÉCIFICATIONS DE LA SIGNALISATION RELATIVE À LA COMMANDE D'APPEL INDÉPENDANTE DU SUPPORT	Q.1900–Q.1999
RNIS À LARGE BANDE	Q.2000–Q.2999
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX DE PROCHAINE GÉNÉRATION	Q.3000–Q.3709
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX PILOTÉS PAR LOGICIEL (SDN)	Q.3710–Q.3899
SPÉCIFICATIONS DE TEST	Q.3900–Q.4099
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX IMT-2020	Q.5000–Q.5049
LUTTE CONTRE LA CONTREFAÇON ET LE VOL D'ÉQUIPEMENTS TIC	**Q.5050–Q.5069**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Q.5051

Cadre pour la lutte contre l'utilisation de dispositifs mobiles volés

Résumé

La Recommandation UIT-T Q.5051 présente un cadre définissant les exigences ainsi qu'un large éventail de mesures complètes qu'il est recommandé de mettre en œuvre pour lutter contre le vol de dispositifs mobiles et la réutilisation des dispositifs mobiles volés.

Ces dernières années, l'amélioration des fonctionnalités et des capacités offertes par les dispositifs mobiles a eu pour effet de renforcer l'importance et l'utilisation de ces dispositifs dans la vie quotidienne. Dans certains pays, ce phénomène s'accompagne d'une recrudescence des comportements visant à voler ces dispositifs et à en tirer profit, non seulement par la vente des équipements eux-mêmes, mais aussi par l'utilisation illégale des données qu'ils contiennent.

Pour faire face à ces comportements, il faut mettre en œuvre des initiatives visant à prévenir le vol de dispositifs mobiles et la réutilisation de dispositifs mobiles volés et à protéger les données des consommateurs stockées sur ces dispositifs contre toute utilisation illégale. Il est fréquent que des dispositifs soient volés dans un pays où des mesures d'atténuation visant à lutter contre l'utilisation de dispositifs volés peuvent exister, puis vendus dans d'autres pays ou régions dans lesquels de telles mesures d'atténuation n'ont pas été mises en place. Il est donc essentiel, pour que ces initiatives portent leurs fruits, de mettre en place une coordination et un échange d'informations entre les gouvernements et les opérateurs pour lutter contre le vol de dispositifs mobiles et la réutilisation de dispositifs mobiles volés à l'échelle mondiale. Dans le cas contraire, il existe un risque que le trafic de dispositifs volés s'étende au-delà des frontières internationales.

On notera que la plupart des solutions mises en œuvre à l'heure actuelle pour prévenir le vol et la réutilisation des dispositifs utilisent des listes d'identifiants uniques. Une solution couramment employée par les trafiquants pour contourner ces solutions consiste donc à altérer le dispositif afin de modifier son identifiant unique, bien souvent en choisissant un identifiant appartenant déjà à un dispositif authentique. De cette façon, l'équipement peut retourner sur le marché et se connecter aux réseaux mobiles.

Pour faire face à ce phénomène, de nombreux pays s'emploient non seulement à lutter contre l'utilisation de dispositifs mobiles volés, mais aussi à empêcher les dispositifs reprogrammés avec des identifiants uniques non autorisés, c'est-à-dire des identifiants qui ont été altérés volontairement, d'accéder de nouveau au réseau. Parallèlement, les pouvoirs publics d'autres pays sont mis à rude épreuve et sont incertains de la stratégie qu'il est préférable d'adopter, à cause, dans bien des cas, d'un manque de connaissances ou de savoir-faire nécessaires pour comprendre ce problème et les solutions possibles et prendre des décisions éclairées afin de déployer des solutions, adaptées à la situation du pays, qui pourraient être efficaces. Dans ce contexte, des lignes directrices sont nécessaires pour résoudre ce problème, comme cela est indiqué dans le Résolution 97 (Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T Q.5051	13-03-2020	11	11.1002/1000/14140

Mots clés

Lutte contre l'utilisation de dispositifs mobiles volés, conformité, cadre, exigences, sécurité.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T Q.5051

Cadre pour la lutte contre l'utilisation de dispositifs mobiles volés

1 Domaine d'application

La présente Recommandation définit un cadre de référence ainsi que les exigences dont il conviendrait de tenir compte lors de la mise en œuvre de solutions visant à lutter contre l'utilisation de dispositifs mobiles volés.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

[UIT-T Q.5050] Recommandation UIT-T Q.5050 (2019), *Cadre pour des solutions permettant de lutter contre la contrefaçon de dispositifs TIC*.

[UIT-T X.1058] Recommandation UIT-T X.1058 (2017), *Technologie de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des informations d'identification personnelle*.

[UIT-T X.1127] Recommandation UIT-T X.1127 (2017), *Exigences et architecture fonctionnelles de sécurité pour les mesures de protection contre le vol de téléphones mobiles*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 utilisateur du dispositif [UIT-T X.1127]: utilisateur autorisé du dispositif mobile.

3.1.2 neutralisation à distance [b-GSMA]: moyen permettant de désactiver les fonctions cruciales d'un dispositif mobile. Il s'agit en substance d'une fonction intégrée au dispositif mobile qui, lorsqu'elle est activée, par exemple par un message envoyé au dispositif dans un certain format, fait que ce dispositif mobile cesse de fonctionner comme prévu et ne peut être réactivé ou réutilisé que si son propriétaire autorise sa réactivation.

3.1.3 téléphone mobile [b-UIT-T X.Sup.19]: appareil électronique utilisé pour passer des appels téléphoniques et envoyer des messages textuels dans un vaste espace géographique par un accès radio aux réseaux publics de téléphonie mobile, tout en permettant à l'utilisateur de se déplacer.

3.1.4 téléphone intelligent, smartphone [b-UIT-T X.Sup.19]: téléphone mobile doté de puissantes capacités de calcul, d'une connectivité hétérogène et d'un système d'exploitation évolué qui fournit une plateforme pour les applications de tierce partie.

3.1.5 dispositif TIC altéré [UIT-T Q.5050]: dispositif fondé sur les technologies de l'information et de la communication (TIC) dont des composants, des logiciels, l'identificateur unique, des éléments protégés par des droits de propriété intellectuelle ou des marques de fabrique ont fait l'objet d'une tentative d'altération ou ont été effectivement altérés sans le consentement exprès du fabricant ou de son représentant légal.

3.1.6 identifiant/identificateur unique [UIT-T Q.5050]: identificateur associé à un dispositif unique qui vise à l'identifier de manière univoque.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 identifiant non valide: identifiant unique qui n'est pas conforme au format défini dans les normes techniques ou qui ne figure pas dans la base de données de référence des identifiants de dispositif distribuée par l'entité de gestion responsable.

3.2.2 identifiant cloné: identifiant de dispositif valide dûment attribué à un dispositif par l'entité de gestion responsable mais qui est utilisé par d'autres dispositifs.

3.2.3 identifiant unique fiable: identifiant qui doit être unique pour chacun des équipements qu'il est censé identifier, ne peut être attribué que par une entité de gestion responsable et ne devrait pas être modifié par des parties non autorisées.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

EIR registre des identités d'équipement (*equipment identity register*)

IMEI identité internationale d'équipement mobile (*international mobile equipment identity*)

IMSI identité internationale d'abonné mobile (*international mobile subscriber identity*)

PII informations d'identification personnelle (*personally identifiable information*)

RUI identifiant unique fiable (*reliable unique idientifier*)

TAC code d'attribution de type (*type allocation code*)

5 Conventions

La présente Recommandation emploie les formes verbales ci-après lors de la formulation des dispositions:

a) L'expression "il est nécessaire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

b) Le terme "devrait" et l'expression "il est recommandé" indiquent des exigences qui sont recommandées mais qui ne sont pas absolument nécessaires. Ces exigences ne sont donc pas indispensables pour déclarer la conformité.

c) Le terme "peut" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Il ne doit pas être interprété comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de service de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité à la présente Recommandation.

6 Aspects généraux

Ces dernières années, l'amélioration des fonctionnalités et des capacités offertes par les dispositifs mobiles a eu pour effet de renforcer l'importance et l'utilisation de ces dispositifs dans la vie quotidienne. Dans certains pays, ce phénomène s'accompagne d'une recrudescence des comportements visant à voler ces dispositifs et à en tirer profit, non seulement par la vente des équipements eux-mêmes, mais aussi par l'utilisation illégale des données qu'ils contiennent.

Pour faire face à ces comportements, il faut mettre en œuvre des initiatives visant à prévenir le vol de dispositifs mobiles et la réutilisation de dispositifs mobiles volés et à protéger les données des consommateurs stockées sur ces dispositifs contre toute utilisation illégale. Il est fréquent que des dispositifs soient volés dans un pays où des mesures d'atténuation visant à lutter contre l'utilisation de dispositifs volés peuvent exister, puis vendus dans d'autres pays ou régions dans lesquels de telles mesures d'atténuation n'ont pas été mises en place. Il est donc essentiel, pour que ces initiatives portent leurs fruits, de mettre en place une coordination et un échange d'informations entre les gouvernements et les opérateurs des différents pays pour lutter contre le vol de dispositifs mobiles et la réutilisation de dispositifs mobiles volés à l'échelle mondiale. Dans le cas contraire, il existe un risque que le trafic de dispositifs volés au-delà des frontières en soit involontairement facilité.

Pour faire face à ce phénomène, de nombreux pays s'emploient non seulement à lutter contre l'utilisation de dispositifs mobiles volés, mais aussi à empêcher les dispositifs reprogrammés avec des identifiants uniques non autorisés, c'est-à-dire des identifiants qui ont été altérés volontairement, d'accéder de nouveau au réseau mobile. Parallèlement, les pouvoirs publics d'autres pays sont mis à rude épreuve et sont incertains de la stratégie qu'il est préférable d'adopter, à cause, dans bien des cas, d'un manque de connaissances ou de savoir-faire nécessaires pour comprendre ce problème et les solutions possibles et prendre des décisions éclairées afin de déployer une solution, adaptée à la situation du pays, qui pourrait être efficace. Dans ce contexte, des recommandations sont nécessaires pour résoudre ce problème, comme cela est indiqué dans le Résolution 97 (Hammamet, 2016) de l'Assemblée mondiale de normalisation des télécommunications.

La présente Recommandation présente donc un cadre définissant les exigences ainsi qu'un large éventail de mesures complètes qu'il est recommandé de mettre en œuvre pour lutter contre le vol de dispositifs mobiles et la réutilisation des dispositifs mobiles volés.

7 Exigences de haut niveau

Les parties prenantes font face à plusieurs difficultés lors de la mise en œuvre de solutions permettant de lutter contre l'utilisation de dispositifs mobiles volés. Lorsqu'ils mettent en œuvre de telles solutions, les pays devraient tenir compte des exigences énoncées au présent paragraphe.

7.1 Prévenir l'utilisation de dispositifs mobiles volés par un utilisateur non autorisé

Il est nécessaire de mettre en œuvre des solutions visant à désactiver les dispositifs en cas de vol ou de perte, pour les rendre inutilisables par des utilisateurs non autorisés.

Il est nécessaire que ce processus s'opère automatiquement dès lors qu'un utilisateur non autorisé a tenté d'accéder au dispositif un certain nombre de fois (par exemple si l'utilisateur non autorisé échoue après plusieurs tentatives à saisir le mot de passe ou le numéro personnel d'identification (PIN) corrects).

Il est recommandé que ce processus puisse être activé à distance par l'utilisateur autorisé du dispositif lorsqu'il en fait la demande (par exemple en activant la fonction de neutralisation à distance du dispositif perdu ou volé).

Il est nécessaire d'avoir la possibilité de rendre de nouveau utilisable le dispositif s'il est récupéré par l'utilisateur autorisé et de restaurer les données de l'utilisateur sur le dispositif dans toute la mesure possible.

La Recommandation [UIT-T X.1127] traite des exigences et de l'architecture fonctionnelles de sécurité concernant les mesures de protection contre le vol de téléphones mobiles. Elle décrit la mise en œuvre d'un outil de neutralisation à distance à utiliser en cas de perte ou de vol d'un téléphone intelligent. Un tel outil devrait permettre:

- de supprimer à distance les données de l'utilisateur autorisé qui se trouvent sur le téléphone intelligent;
- de rendre le téléphone intelligent inutilisable par un utilisateur non autorisé;
- d'empêcher la réactivation sans la permission de l'utilisateur autorisé, dans la mesure où cela est techniquement possible;
- de rendre de nouveau utilisable le téléphone intelligent s'il est récupéré par l'utilisateur autorisé, et de restaurer les données de l'utilisateur dans le téléphone intelligent dans toute la mesure possible;
- de localiser le dispositif mobile volé ou perdu.

Il est recommandé de sensibiliser les utilisateurs afin qu'ils sachent configurer et utiliser cette fonctionnalité et signalent la perte ou le vol de leur dispositif mobile à leur fournisseur de services, ou à la police ou aux autorités judiciaires, de façon à empêcher les dispositifs d'accéder aux réseaux mobiles et à permettre aux organismes chargés de l'application de la loi de prendre les mesures voulues.

7.2 Empêcher les dispositifs mobiles volés d'accéder au réseau

Il est nécessaire de mettre en place des solutions visant à empêcher les dispositifs mobiles volés d'accéder aux réseaux mobiles, de préférence au moyen de systèmes automatisés pouvant faire l'objet d'une vérification.

Il est nécessaire que seules les personnes autorisées, comme le propriétaire légitime du dispositif, puissent demander à ce qu'un dispositif mobile volé soit supprimé de tous les réseaux du pays.

Il est recommandé d'élaborer un cadre de politique générale visant à prévenir l'utilisation de dispositifs volés sur le réseau.

Il importe de noter que les dispositifs bloqués sur les réseaux mobiles sur la base de leur identifiant unique peuvent toujours accéder aux réseaux qui ne vérifient pas l'identifiant unique des dispositifs mobiles, tels que les réseaux WiFi (fidélité hertzienne). Ainsi, il est important de compléter cette méthode en mettant en œuvre d'autres mesures, comme celles visées au § 7.1.

7.3 Empêcher l'utilisation de dispositifs volés dotés d'identifiants ayant subi une altération volontaire ou d'identifiants uniques clonés

Il est nécessaire de mettre en place une solution permettant d'identifier les dispositifs mobiles qui sont dotés d'identifiants uniques ayant été altérés volontairement ou clonés et de les distinguer des dispositifs authentiques, de manière extrêmement précise, afin que des mesures de rupture puissent être mises en œuvre, de préférence au moyen de systèmes automatisés et sans conséquence pour les dispositifs authentiques.

Il est recommandé d'intégrer des bases de données de référence dans cette solution afin de pouvoir identifier les informations concernant les dispositifs authentiques et l'origine légale de ces dispositifs. Il conviendrait d'utiliser des bases de données d'enregistrement nationales permettant d'identifier les dispositifs importés et acquis légalement, ainsi que des bases de données concernant les identifiants uniques attribués aux fabricants et d'autres caractéristiques de ces dispositifs, afin d'alimenter les bases de données de référence et ainsi de distinguer plus facilement les dispositifs authentiques de ceux ayant subi une altération volontaire.

Dans le cadre de cette solution, il est nécessaire de tenir compte du fait qu'un identifiant unique ayant été altéré volontairement peut prendre différentes formes, qu'il faut prendre en compte dans le cadre du processus de détection et de contrôle. On peut ainsi avoir affaire à un identifiant non valide, cloné ou, le cas échéant, non homologué ou non enregistré dans les bases de données de référence nationales.

7.4 Empêcher les dispositifs mobiles volés dans d'autres pays d'accéder au réseau

Il est recommandé que la législation et la réglementation locales favorisent la coordination et l'échange d'informations entre les gouvernements et les opérateurs de différents pays pour prévenir l'utilisation de dispositifs volés, quel que soit le pays où a eu lieu le vol.

Faute de mesures visant à encourager et à faciliter l'échange international de données, le trafic international de dispositifs volés continuera de se développer librement: des dispositifs continueront d'être volés dans un pays puis exportés vers d'autres pays ou régions pour y être vendus.

Pour résoudre ce problème, il est recommandé que toutes les parties prenantes, dans tous les pays, aient accès à une base de données mondiale des dispositifs volés pour pouvoir signaler le vol d'un dispositif et vérifier le statut d'un dispositif.

Des "listes noires" de dispositifs au niveau local et national devraient être partagées et mises à la disposition de la communauté internationale. Pour ce faire, il faudrait exiger la connexion à la base de données mondiale des dispositifs volés et le partage des données relatives aux dispositifs volés au niveau local avec cette base de données.

7.5 Limiter les conséquences pour les consommateurs

Il convient de tenir compte des conséquences pour les consommateurs lors de la mise en œuvre de toute solution visant à lutter contre l'utilisation de dispositifs mobiles volés. Lorsque plusieurs méthodes permettant d'atteindre le même objectif s'offrent au consommateur, il convient d'adopter celle qui limite le plus l'incidence globale sur les consommateurs légitimes.

Il est recommandé que les dispositifs dotés d'identifiants non valides qui accèdent au réseau pour la première fois soient contrôlés après qu'une notification préalable a été adressée aux utilisateurs afin de leur octroyer des délais suffisants pour présenter la preuve qu'ils ont acquis le dispositif légalement et d'éviter que les dispositifs en question ne se voient soudainement refuser l'accès au service.

Il est recommandé d'éviter de bloquer les abonnements des utilisateurs lorsque des mesures sont prises pour contrôler les dispositifs dotés d'identifiants ayant subi une altération volontaire ou d'identifiants clonés.

Il est recommandé que des campagnes éducatives et des campagnes de sensibilisation soient menées auprès de la population, par tous les moyens à disposition, au sujet des mesures à prendre, des objectifs recherchés, des avantages ainsi que des options et des mesures auxquelles les utilisateurs peuvent avoir recours en cas de perte ou de vol de leur dispositif ou s'ils acquièrent un dispositif doté d'un identifiant ayant subi une altération volontaire ou d'un identifiant cloné.

Lors de l'adoption de mesures visant à lutter contre l'utilisation de dispositifs dotés d'identifiants ayant subi une altération volontaire ou d'identifiants clonés, il est recommandé de prévoir des périodes de transition ou de grâce. Les dispositifs qui sont déjà utilisés peuvent avoir été acquis de bonne foi et les utilisateurs pourraient ne pas avoir connaissance des risques. S'il est décidé de ne pas bloquer les dispositifs existants, des mesures supplémentaires devraient être prises pour éviter que ces dispositifs soient activés par de nouveaux utilisateurs.

Il est recommandé de mettre en place des moyens efficaces pour recueillir des rapports et des informations auprès des utilisateurs et prendre des mesures, afin de pouvoir suspendre les services et bloquer les identifiants des dispositifs.

Il est recommandé de faciliter la détermination de l'identifiant du dispositif à bloquer sans avoir à demander à l'utilisateur de se souvenir de cet identifiant ou de le retrouver, par exemple en recherchant le relevé des appels du dispositif sur le réseau de l'opérateur afin de trouver l'identifiant du dispositif perdu ou volé.

Il est recommandé de suspendre les services et de bloquer les identifiants des dispositifs perdus ou volés le plus tôt possible. À titre d'exemple, on peut bloquer le dispositif dès lors que la demande en ce sens est approuvée par les parties prenantes responsables de cette opération.

Il est nécessaire de fournir des outils à toutes les parties prenantes pour leur permettre de vérifier si un dispositif a été bloqué.

Il est recommandé que l'entité chargée de bloquer les dispositifs informe l'utilisateur lorsque son dispositif est bloqué ou lui communique les raisons pour lesquelles le dispositif signalé ne peut pas être bloqué, dans le cas où la demande a été rejetée.

7.6 Protéger les données privées des consommateurs

Les données privées des consommateurs devraient être protégées en cas de perte ou de vol d'un dispositif. En premier lieu, il est recommandé de mettre en œuvre des mécanismes visant à interdire à un utilisateur non autorisé d'utiliser le dispositif, y compris d'accéder aux données privées qui y sont stockées.

Il est recommandé de sensibiliser les consommateurs à l'importance de protéger et de sauvegarder leurs données personnelles et à la façon d'utiliser les fonctionnalités qui leur permettent d'effacer à distance les informations d'identification personnelles (PII) contenues dans le dispositif volé.

Il est recommandé que les fonctionnalités dont il est question dans la Recommandation [UIT-T X.1127] soient intégrées par défaut par les fabricants dans tous les nouveaux dispositifs.

Il est recommandé aux parties prenantes de mener une campagne de sensibilisation auprès des consommateurs sur la manière de configurer et d'utiliser ces fonctionnalités.

7.7 Empêcher les dispositifs mobiles volés d'accéder au marché

Il est recommandé aux autorités nationales de régulation des télécommunications de collaborer avec les autres organismes nationaux compétents (par exemple les autorités douanières), afin d'améliorer les mesures de contrôle concernant les dispositifs signalés comme ayant été volés ou perdus au niveau national et dans d'autres pays.

Dans le cadre de cette collaboration, il convient d'envisager de fournir, le cas échéant:

1) Un accès aux bases de données concernant les dispositifs volés, ainsi qu'à d'autres informations, par exemple en ce qui concerne les dispositifs ayant un identifiant non valide ou non homologué, dans la mesure où il est possible d'altérer l'identifiant unique pour que le dispositif ne figure pas dans les bases de données nationales et internationales répertoriant les dispositifs volés.
2) Un accès à une base de données mondiale relative aux identifiants qui ont été attribués à des fabricants légitimes, de sorte que l'on puisse valider la structure des identifiants appartenant à des dispositifs destinés à l'importation.
3) Un accès à la liste des marques et des modèles de dispositifs homologués, afin d'autoriser uniquement l'importation de modèles homologués, conformément à la réglementation nationale applicable.
4) Un accès aux bases de données de référence nationales où sont enregistrés les identifiants des dispositifs importés et acquis de manière légale, selon qu'il convient.

5) Un accès à une base de données mondiale relative aux dispositifs volés, ainsi que l'accès à une base de données contenant des informations propres à un dispositif donné, de façon à pouvoir confirmer l'authenticité des dispositifs. Ce dernier aspect serait particulièrement utile dans les cas où l'identifiant unique d'un dispositif volé aurait été altéré et où ce dispositif aurait été reprogrammé avec un identifiant correspondant à un autre dispositif.

Il est recommandé de recouper minutieusement l'identifiant complet avec la base de données nationale relative aux dispositifs, afin d'éviter d'inclure dans cette base un dispositif doté d'un identifiant appartenant à un autre dispositif qui est déjà en circulation dans le pays.

Il est recommandé de prendre des mesures juridiques à l'égard des points de vente proposant des dispositifs volés.

7.8 Autres éléments à prendre en compte pour lutter contre l'altération volontaire d'identifiants uniques de dispositifs mobiles volés

Les autres éléments à prendre en compte pour lutter contre l'altération volontaire de dispositifs mobiles volés sont notamment les suivants:

– Envisager l'élaboration de cadres de politique générale visant à prévenir l'utilisation ou la vente sur le marché de dispositifs mobiles volés qui ont subi une altération volontaire.

– Organiser des campagnes éducatives et des formations sur les aspects techniques liés au vol et à l'altération volontaire d'identifiants uniques de dispositifs mobiles.

– Envisager de mettre en place des mesures de contrôle concernant les éléments matériels ou logiciels utilisés pour altérer volontairement les identifiants des dispositifs mobiles.

Il est recommandé de disposer des fondements juridiques et de l'appui nécessaires pour permettre aux autorités chargées de l'application de la loi de poursuivre les personnes qui modifient, altèrent ou effacent les identifiants des dispositifs mobiles dans le but de contourner les mesures visant à prévenir l'utilisation des dispositifs volés sur le marché.

Il est recommandé que ce cadre juridique prévoie également des mesures à mettre en œuvre à l'égard des personnes qui offrent, possèdent, importent ou vendent des outils matériels ou logiciels utilisés pour altérer volontairement les identifiants des dispositifs mobiles.

Il est recommandé que les autorités chargées de l'application de la loi reçoivent un enseignement et une formation au sujet des aspects techniques liés au vol et à l'altération volontaire d'identifiants uniques de dispositifs mobiles, et au sujet du cadre juridique permettant d'engager des poursuites.

Il est recommandé que les fabricants de dispositifs mobiles prévoient des mécanismes garantissant la fiabilité et l'intégrité de l'identifiant unique de ces dispositifs.

8 Exigences du cadre

Lors de la mise en place de solutions visant à lutter contre le vol de dispositifs mobiles, il convient de tenir compte des exigences suivantes.

8.1 Base de données centralisée de référence

Il est recommandé d'utiliser une base de données centralisée de référence pour conserver les informations sur les dispositifs perdus ou volés. Tous les exploitants devraient donc l'utiliser pour empêcher que les dispositifs volés aient accès à tout réseau mobile. Cette base de données devrait contenir au moins l'identifiant unique du dispositif volé, la date à laquelle le vol s'est produit et le nom de l'entité qui a inséré ces informations dans la base de données.

Il est recommandé que cette base de données contienne aussi d'autres types d'identifiants et d'informations, afin de faciliter l'identification des dispositifs volés dont les identifiants ont subi une altération volontaire et de traiter le problème.

Il est recommandé de faire figurer dans cette base de données de référence des informations relatives aux dispositifs importés et/ou acquis légalement.

Il est recommandé que les entités autorisées aient accès à toutes les bases de données pertinentes.

Il est recommandé de mettre en œuvre une procédure d'enregistrement obligatoire des dispositifs. Lors de la mise en œuvre de cette procédure, il convient de porter une attention particulière au moment d'associer le dispositif à des informations PII, et de veiller aux conséquences indirectes sur le commerce des dispositifs mobiles légaux et sur la concurrence sur le marché du mobile.

Il est recommandé de mettre en œuvre des procédures d'audit pour vérifier que les dispositifs signalés comme ayant été volés ont été bloqués et que les procédures adéquates ont été adoptées par toutes les parties prenantes.

8.2 Appui du réseau pour bloquer les dispositifs

Il est nécessaire que les réseaux mobiles comportent des éléments pouvant empêcher l'accès des dispositifs volés dont les identifiants valides ont été inscrits sur liste noire et des dispositifs transmettant des identifiants dans un format qui n'est pas conforme aux normes applicables aux identifiants uniques[1].

Il est recommandé que les solutions de blocage utilisées dans les réseaux mobiles prennent en charge des fonctionnalités permettant d'éviter l'utilisation de dispositifs ayant des identifiants uniques clonés, et donc de différencier les dispositifs authentiques des dispositifs clonés[2].

8.3 Identifiants uniques fiables

Il est recommandé que les bases de données de référence utilisées pour empêcher les dispositifs mobiles volés d'accéder aux réseaux mobiles s'appuient sur des identifiants uniques fiables (RUI), car l'altération des identifiants uniques des dispositifs peut avoir des incidences négatives sur l'efficacité des solutions visant à retirer les dispositifs volés du marché.

Il est recommandé que l'identifiant unique soit stocké[3] dans un élément sécurisé du dispositif mobile et que celui-ci applique des mesures de sécurité, pour autant que cela soit techniquement réalisable, afin de détecter toute altération volontaire de l'élément sécurisé ou des informations stockées à l'intérieur et, par conséquent, de rendre le dispositif inutilisable tant que les données d'origine ne sont pas restaurées.

Il est recommandé que l'entité responsable de la gestion des identifiants uniques applique un processus qui encourage les fabricants légitimes de dispositifs à utiliser de façon adéquate et sécurisée les identifiants uniques qui leur ont été attribués.

Il est recommandé que les identifiants uniques soient conformes aux principes d'intégrité (tous les fabricants doivent disposer de plages d'identifiants attribuées par l'entité désignée) et aux principes de sécurité définis par le secteur (toutes les mesures établies, ou une combinaison d'entre elles, visant à mettre en œuvre les identifiants de sorte qu'il soit impossible de les altérer)[4].

---

1 Voir les spécifications techniques [b-3GPP TS 122.016] et [b-3GPP TS 123.003] pour les dispositifs compatibles 3GPP/3GPP2.

2 Pour les dispositifs compatibles 3GPP/3GPP2, lorsque l'IMEI est utilisé en tant qu'identifiant unique, la prise en charge d'une fonction de vérification de l'IMEI ou de l'IMSI du réseau d'accès radioélectrique au réseau central peut permettre de satisfaire cette exigence.

3 Par exemple, il est défini dans la spécification technique [b-3GPP TS 122.016] que l'IMEI ne doit pas être modifiée.

4 Voir, par exemple, la spécification technique [b-IMEI-SEC] concernant les dispositifs mobiles compatibles 3GPP.

Il est recommandé que les processus que le secteur a mis en place pour faire respecter ces principes soient appuyés par les pouvoirs publics ou conformes aux cadres réglementaires nationaux.

Il est nécessaire que les identifiants uniques ne soient pas reprogrammables, même durant le service de maintenance. Si les identifiants uniques peuvent être modifiés après le processus de fabrication, alors ils risquent d'être moins sûrs, car ils pourront être altérés par un tiers non autorisé.

8.4 Collaboration étroite avec les autorités chargées de l'application de la loi et d'autres organismes nationaux

Afin de limiter efficacement la circulation de dispositifs volés sur le marché, il est nécessaire de mettre en place une collaboration étroite entre les autorités responsables de l'établissement et de la tenue à jour de bases de données de référence, les autorités douanières nationales, ainsi qu'entre ces autorités d'autres pays et les parties prenantes concernées. Il devrait donc être tenu compte des considérations suivantes:

– Étant donné que les autorités douanières et d'autres organismes autorisés nationaux compétents jouent un rôle essentiel dans la surveillance et l'interception de produits volés, perdus ou ayant subi une altération volontaire, il est important de mettre à leur disposition des outils permettant d'identifier ces dispositifs, et même les dispositifs légaux, grâce à une base de données centralisée de référence.

– Il convient d'établir et de mettre en œuvre des mesures coercitives ainsi que d'instaurer et d'entretenir la communication entre les différentes organisations concernées, notamment en échangeant les informations pertinentes, telles que les bases de données des dispositifs mobiles conformes aux normes nationales, régionales ou internationales.

– Il est possible de lutter contre le commerce illégal de dispositifs mobiles volés, au moyen de mécanismes d'authentification de l'identité d'un dispositif particulier, visant à vérifier que le dispositif est authentique et que son utilisation est permise par les lois et les règlements du pays concerné.

– Les autorités chargées de l'application de la loi, qui se basent sur les cadres juridiques nationaux, peuvent choisir de ne pas bloquer immédiatement les dispositifs à des fins d'enquête pour identifier l'origine des dispositifs volés mis en vente sur le marché, bien qu'il soit préférable de bloquer tous les dispositifs le plus rapidement possible, sauf si des motifs valables et exceptionnels les obligent à agir autrement dans des cas particuliers.

Il est recommandé qu'une stratégie de haut niveau venant du sommet de l'État soit mise en place pour favoriser la coopération et appliquer un ensemble complet de mesures, afin de faciliter les engagements et la réalisation des activités de différents acteurs et autorités distincts du secteur (par exemple, application de la loi, douanes, commerce, etc.).

8.5 Outils de vérification du statut des dispositifs mobiles

Il est nécessaire de mettre à disposition un outil public pour les consommateurs et d'autres parties prenantes, afin de vérifier le statut des dispositifs mobiles. Les consommateurs et d'autres parties prenantes devraient pouvoir vérifier, de préférence en utilisant l'Internet, si certains dispositifs sont signalés comme étant volés ou perdus.

Il est recommandé que l'entité responsable du blocage d'un dispositif soit mentionnée dans la réponse à une recherche effectuée avec l'outil de vérification des dispositifs (y compris le pays dans lequel le blocage a été effectué), pour que le consommateur puisse éviter d'acheter ou d'acquérir des dispositifs volés, et aussi pour traiter les plaintes en cas de blocage erroné ou de blocage effectué par un tiers à cause d'un dispositif cloné ayant le même identifiant. De plus, il s'agit d'un outil de vérification préalable à l'achat important pour le consommateur.

Il est recommandé que les commerçants et les entités qui font le commerce de ces dispositifs effectuent des vérifications concernant les dispositifs qu'ils acquièrent, afin de s'assurer qu'il n'a pas été signalé qu'ils étaient perdus ou volés, ou qu'ils disposaient d'un identifiant unique dupliqué. Des registres devraient être tenus, afin de prouver que le principe de diligence due a été respecté pour réduire la possibilité de faire le commerce de dispositifs dont il a été signalé qu'ils étaient perdus ou volés, ou qu'ils disposaient d'un identifiant unique dupliqué.

8.6 Appui des cadres réglementaires et juridiques nationaux applicables

Il est recommandé d'élaborer des mécanismes permettant d'identifier et de bloquer les dispositifs perdus ou volés, ainsi que les dispositifs dont l'identifiant unique a subi une altération volontaire dans le réseau mobile, dans la mesure du possible d'un point de vue technique. Une vérification devrait être effectuée auprès des opérateurs des réseaux mobiles locaux.

Avant de mettre en œuvre des mesures restrictives à l'encontre des dispositifs volés dont l'identifiant unique a subi une altération volontaire ou a été dupliqué, il est recommandé de s'assurer de la conformité au cadre réglementaire et juridique national applicable, notamment en ce qui concerne:

– La restriction de l'accès aux réseaux de télécommunication pour les dispositifs dont le vol a été signalé au niveau national ou dans un autre pays.
– La restriction de l'accès aux réseaux de télécommunication pour les dispositifs dont les identifiants ont subi une altération volontaire.
– La restriction de l'altération des identifiants uniques des dispositifs mobiles, et les conséquences de l'altération.
– La mise au point des solutions nécessaires en vue de permettre aux autorités, aux consommateurs et aux acteurs des circuits de vente de distinguer les dispositifs authentiques des dispositifs volés ayant subi une altération volontaire.
– L'existence d'une autorité chargée d'appliquer les points ci-dessus.

En ce qui concerne cette exigence, il convient de tenir dûment compte de la législation et des cadres réglementaires nationaux existants qui couvrent peut-être déjà les aspects considérés.

9 Cadre de référence

Compte tenu des exigences du cadre décrites au § 8, une proposition de cadre de référence visant à lutter contre le vol de dispositifs mobiles et l'utilisation de dispositifs mobiles volés est illustrée dans la Figure 1. Il convient de noter que tous les éléments fonctionnels décrits dans la Figure 1 n'ont pas nécessairement un caractère obligatoire. Chaque pays pourra mettre en œuvre les éléments voulus en fonction de ses besoins.

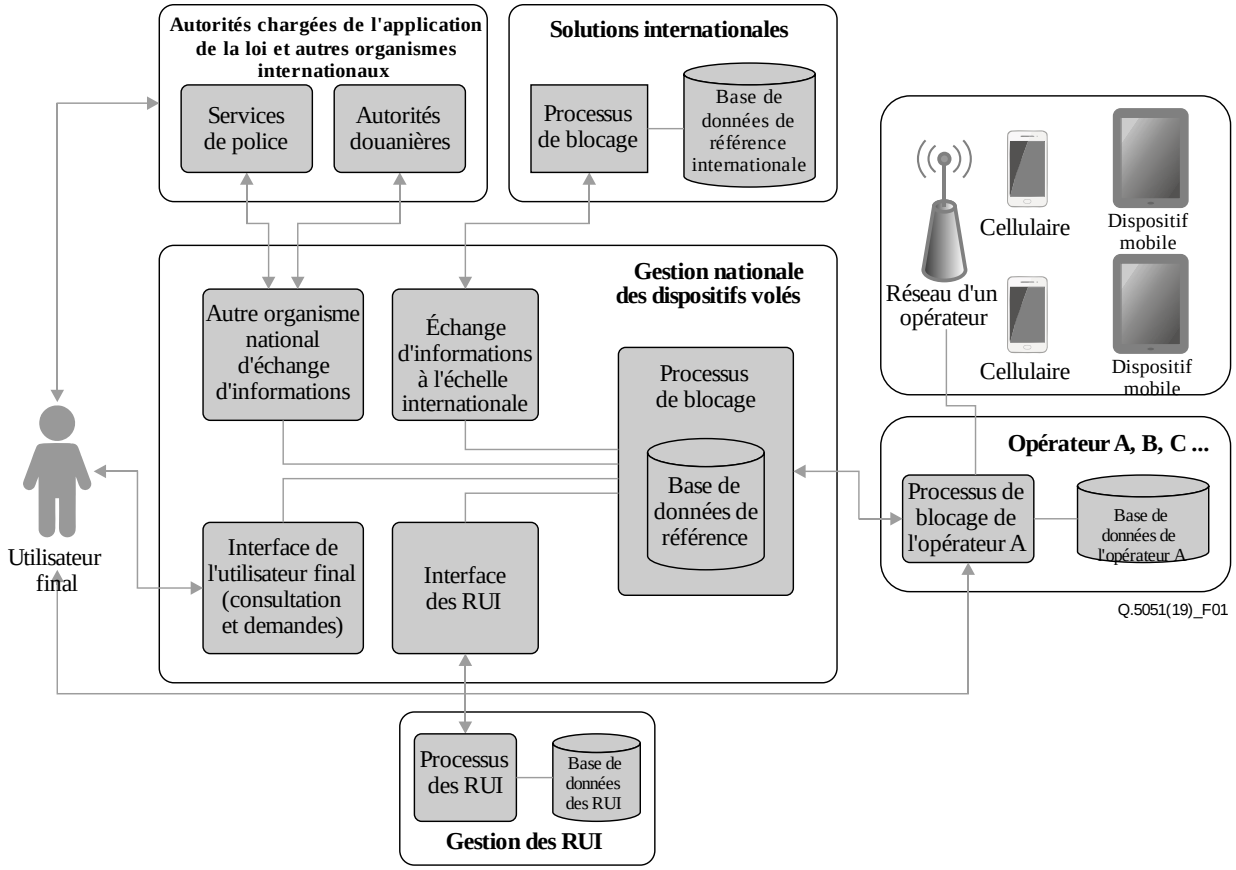

Figure 1 – Proposition de cadre général

Toute une gamme d'activités et de systèmes d'information, opérés par différentes organisations, doivent fonctionner conjointement pour permettre le contrôle et la production d'informations essentielles visant à identifier les dispositifs mobiles perdus ou volés ou dont les identifiants sont non valides, et à lutter contre leur utilisation.

Les consommateurs et d'autres parties prenantes devraient pouvoir vérifier si un dispositif particulier est signalé comme étant perdu ou volé, ou s'il est signalé que l'identifiant de ce dispositif est non valide.

La demande de blocage d'un dispositif volé pourrait être soumise par l'intermédiaire de différentes parties prenantes (consommateur, autorité chargée de l'application de la loi, opérateur mobile, ou demande présentée directement au système central). Quel que soit le lieu où la demande de blocage des dispositifs utilisés est soumise, des mesures devraient être prises pour valider l'identité de l'utilisateur ainsi que des informations relatives à la propriété du dispositif. S'agissant des dispositifs n'ayant pas été vendus aux consommateurs, par exemple ceux qui ont été volés en transit, en point de vente, etc., une plainte doit accompagner la demande de blocage du dispositif.

Afin de limiter la circulation des dispositifs volés sur le marché, d'autres organismes nationaux compétents (par exemple, les autorités chargées de l'application de la loi et les autorités douanières) devraient pouvoir vérifier le statut du dispositif en utilisant toutes les sources et bases de données de référence mises à disposition.

Les échanges avec les organismes internationaux sont aussi essentiels et peuvent être effectués sur une base bilatérale ou avec une base de données de référence mondiale.

Afin de garantir le blocage effectif des dispositifs volés sur les réseaux mobiles du pays concerné, tous les opérateurs devraient être synchronisés à l'aide d'une base de données de référence nationale et d'une base de données de référence mondiale.

Il est nécessaire qu'un système de gestion des identifiants uniques fiables (RUI) soit intégré au processus de blocage des dispositifs mobiles volés, car il est possible d'altérer les identifiants uniques de certains dispositifs pour contourner ce processus.

Il est nécessaire de mettre en œuvre un processus visant à identifier et à contrôler les dispositifs mobiles dont les identifiants sont non valides sur les réseaux, possiblement en raison de l'altération d'un dispositif volé après avoir été bloqué.

10 Caractéristiques souhaitables

Lors de la mise en place d'une solution visant à lutter contre l'utilisation des dispositifs mobiles volés, les pays doivent tenir compte des caractéristiques souhaitables énoncées aux paragraphes suivants.

10.1 Base de données de référence mondiale des dispositifs perdus ou volés

Étant donné que les dispositifs bloqués peuvent être transportés voire vendus à des consommateurs dans différents pays, il est recommandé d'utiliser une base de données de référence mondiale pour échanger des informations sur les identifiants des dispositifs perdus ou volés et bloquer ceux-ci, afin d'inscrire les dispositifs volés sur liste noire dans un point d'information unique qui facilite les échanges et réduit les délais de blocage.

Il est recommandé, quelle que soit la taille de l'opérateur, d'empêcher tous les dispositifs dont les identifiants figurent dans cette base de données de référence mondiale de se connecter au réseau local. Toutefois, d'autres approches sont envisageables selon le contexte propre à chaque mise en œuvre (par exemple, on peut privilégier le traitement par lots des identifiants uniques actifs par rapport à la base de données de référence mondiale).

Il est nécessaire que les autorités chargées de l'application de la loi et d'autres organismes gouvernementaux aient accès à la base de données de référence mondiale pour faire rapport et enquêter sur des groupes d'identifiants, afin que leurs mesures juridiques en matière de lutte contre le vol de dispositifs mobiles soient facilitées.

Il est recommandé de vérifier l'exactitude des informations à inclure dans la base de données mondiale qui concernent les dispositifs signalés comme étant volés. Seulement après cette vérification, les listes des dispositifs volés établies par les parties susmentionnées devraient être fournies en vue de leur inclusion dans la base de données mondiale répertoriant les dispositifs volés.

Cette base de données mondiale devrait être à disposition de toutes les parties prenantes du monde entier, pour leur permettre de vérifier si un dispositif est signalé comme étant volé. La base de données devrait être accessible à la fois au niveau du système, c'est-à-dire aux parties qui peuvent bloquer les dispositifs volés, et au niveau du consommateur, afin que les consommateurs de tous les pays puissent vérifier si un dispositif particulier a été signalé comme étant volé.

La base de données mondiale devrait fournir des informations adéquates, si elles sont disponibles (par exemple, les caractéristiques du dispositif, le pays dans lequel le dispositif a été volé, la date à laquelle le vol s'est produit, etc.). Si les identifiants du dispositif volé ont été trouvés dans plusieurs pays, cette information devrait figurer dans les résultats présentés par la base de données mondiale.

Des procédures devraient être appliquées pour que les personnes utilisant la base de données mondiale puissent remédier à des blocages involontaires (par exemple un blocage erroné, un blocage lié à des identifiants de dispositifs dupliqués ou clonés).

10.2 Mesures concernant les établissements qui vendent des dispositifs perdus, volés ou ayant subi une altération volontaire

Il est recommandé que les pays envisagent d'adopter un cadre établissant la responsabilité, pour les points de vente, de commercialiser uniquement des dispositifs homologués pour la vente, et les conséquences de la commercialisation de dispositifs volés ou de dispositifs dont les identifiants ont subi une altération volontaire. Cet appui juridique permettra aux autorités chargées de l'application de la loi de mieux lutter contre la vente et la demande de ces dispositifs.

Il est possible d'inclure dans la base de données de référence nationale les identifiants des dispositifs importés et vendus légalement. Cette base de données pourrait être utile dans le cadre de diverses mesures coercitives et activités nationales, comme les importations, la vente, l'utilisation dans les réseaux, les mesures des autorités chargées de l'application de la loi, etc.

Par conséquent, en ayant accès à cette base de données répertoriant les dispositifs autorisés, les autorités chargées de l'application de la loi pourraient prendre des mesures contre les établissements proposant au public des dispositifs volés, clonés ou ayant subi une altération volontaire, voire identifier et intercepter les produits importés illégalement.

Appendice I

Approche de la GSMA pour lutter contre le vol de dispositifs mobiles

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Dans un nombre croissant de pays, les opérateurs permettent aux consommateurs de signaler la perte ou le vol d'un dispositif mobile. L'opérateur peut alors établir l'identifiant unique du dispositif, à savoir l'identité internationale d'équipement mobile (IMEI), et l'opérateur du réseau mobile peut alors empêcher le téléphone d'avoir accès au réseau mobile. Cela consiste à inscrire l'IMEI sur une liste noire[5].

Une base de données mondiale peut être utilisée, par exemple, dans la communauté de l'opérateur mobile, où les IMEI inscrites sur liste noire sont indiquées dans la base de données mondiale des IMEI de la GSM Association (GSMA), permettant ainsi aux opérateurs d'échanger des données et de bloquer des dispositifs sur de multiples réseaux à l'échelle nationale et internationale.

La base de données des IMEI de la GSMA contient une liste noire mondiale établie à partir des données fournies par les opérateurs qui apportent leur contribution. La GSMA fournit les informations relatives aux IMEI inscrites sur liste noire 24 heures sur 24, 7 jours sur 7, aux opérateurs qui ont établi des connexions avec la base de données des IMEI, afin qu'ils téléchargent et utilisent ces informations dans leurs propres réseaux à des fins de blocage des dispositifs. L'extraction des données inscrites sur la liste noire d'un opérateur par les autres opérateurs contribuant à l'établissement de la base de données détermine la mesure dans laquelle les données sont échangées.

Souvent, l'abonné qui signale à son fournisseur de services qu'il n'est plus en possession d'un dispositif ne sait pas s'il l'a perdu ou s'il a été volé. Par conséquent, en règle générale, aucune distinction n'est faite entre la perte et le vol. Si le propriétaire retrouve le dispositif et en informe son fournisseur de services, le dispositif peut être débloqué et l'IMEI peut être retirée de la liste noire de la base de données des IMEI. La GSMA demande alors aux opérateurs utilisant la base de données des IMEI et qui ont téléchargé les données du dispositif inscrites initialement sur liste noire de retirer ces données de leur liste noire.

Compte tenu des caractéristiques de cette base de données mondiale, et de l'engagement des différentes parties prenantes sur le marché pour lutter contre les vols de dispositifs, la GSMA a créé un système permettant de vérifier le statut des IMEI. Il s'agit d'un système de vérification des dispositifs qui permet d'échanger des données et des informations sur le statut d'un dispositif avec des partenaires agréés, comme les commerçants, les assureurs, les recycleurs et les autorités chargées de l'application de la loi.

Grâce à ce système, les parties prenantes intéressées peuvent voir si un dispositif a été signalé comme étant perdu ou volé, consulter l'historique d'un dispositif en remontant à plusieurs années, ainsi que les informations et les capacités d'un modèle de dispositif. Ce type de système de vérification comporte plusieurs avantages: a) il aide les revendeurs à identifier et à détruire les dispositifs volés avant qu'ils puissent entrer dans la chaîne d'approvisionnement; b) il permet de confirmer l'authenticité d'un modèle de dispositif et aide à calculer la valeur du dispositif; c) il permet de décourager le vol de dispositifs moyennant une réduction de la valeur d'un dispositif volé; d) il permet de vérifier quel opérateur de réseau a signalé la perte ou le vol du dispositif, ce qui facilite le renvoi du dispositif au propriétaire légitime.

---

5 Voir la spécification [b-GSMA-IMEI-Blklst].

Outre les opérateurs de réseau, de nombreuses autres organisations de l'écosystème des dispositifs mobiles peuvent utiliser le système de vérification des dispositifs, notamment a) les recycleurs, les commerçants et les distributeurs de dispositifs qui utilisent les données pour réduire la probabilité que les dispositifs signalés comme étant volés ou perdus soient recyclés ou revendus; b) les compagnies d'assurance qui s'appuient sur la base de données pour réduire le nombre de demandes d'indemnisation fausses ou exagérées présentées suite à la perte ou au vol d'un dispositif; c) les autorités chargées de l'application de la loi, qui utilisent le système de vérification pour identifier les biens volés ou perdus et contribuer aux enquêtes concernant ces biens et/ou au renvoi de ces biens au propriétaire[6].

L'accès à la base de données mondiale des IMEI en vue de chercher un identifiant unique peut être accordé à diverses parties prenantes supplémentaires, notamment les consommateurs, grâce à des services fournis par des organismes comme les autorités nationales, qui proposent des portails en langue locale hébergés en ligne permettant de chercher des IMEI. L'accès en vue d'inscrire des identifiants sur liste noire ou d'en désinscrire de la liste noire est actuellement accordé uniquement aux opérateurs de réseau qui peuvent identifier et attester de manière univoque les données IMEI pour leurs clients, préservant ainsi l'intégrité de la liste noire. Il est envisagé d'élargir l'accès en écriture à la liste noire à d'autres parties, comme les fabricants des dispositifs, les commerçants, etc. qui peuvent attester et garantir que les IMEI sont bloquées.

Les systèmes susmentionnés (base de données des IMEI et système de vérification des IMEI de la GSMA) offrent aux parties prenantes divers avantages par rapport aux bases de données nationales qui aboutissent à une fragmentation mais qui pourraient être établies sur la base d'efforts bilatéraux ou multilatéraux visant à échanger et bloquer les identifiants de dispositifs signalés comme étant perdus ou volés. Ces avantages pourraient être les suivants: a) temps de mise en œuvre et d'ajustement réduit; b) des dépenses d'investissement (CAPEX) et dépenses opérationnelles (OPEX) réduites; c) moins de complexité et plus d'efficacité (un point d'échange commun au lieu de plusieurs origines et destinations); d) moins de reproduction d'informations. Ces éléments sont fondés sur les caractéristiques suivantes des systèmes susmentionnés: a) modularité, b) aucun frais de connexion pour les opérateurs/pouvoirs publics; c) la base de données des IMEI est une plate-forme technologique bien développée et stable qui existe depuis 1996.

6 Voir la spécification [b-GSMA-IMEI-DevChk].

Bibliographie

[b-UIT-T X-Sup.19] Recommandations UIT-T de la série X – Supplément 19 (2013), Supplément sur les aspects relatifs à la sécurité des smartphones.

[b-IMEI-SEC] GSMA (2016), *IMEI Security Design Principles. Enabling stolen mobile device blocking. V4.0*. <https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf>

[b-3GPP TS 122.016] ETSI TS 122 016 V3.1.0 (2000-01), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); International Mobile station Equipment Identities (IMEI) (3G TS 22.016 v3.1.0 Version de 1999).*

[b-3GPP TS 23.003] ETSI TS 123 003 V10.5.0 (2012-04), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 v10.5.0 Version 10).*

[b-GSMA] GSM Association, document officiel SG.24 (2016), *Anti-Theft Device Feature Requirements v3.0*.

[b-GSMA-IMEI-Blklst] GSMA Services, *IMEI Blacklisting*. <https://www.gsma.com/services/gsma-imei/imei-blacklisting/> (consulté pour la dernière fois le 13 avril 2020)

[b-GSMA-IMEI-DevChk] GSMA Services, *Device Check*. <https://www.gsma.com/services/gsma-imei/about-device-check/> (consulté pour la dernière fois le 13 avril 2020)

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	**Commutation et signalisation et mesures et tests associés**
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2020