Sécurité, respect de la vie privée et sûreté dans l'ensemble de l'écosystème mobile

Enjeux clés et implications politiques

La GSMA représente les intérêts des opérateurs de téléphonie mobile du monde entier, réunissant près de 800 opérateurs et plus de 250 entreprises dans l'écosystème mobile élargi, qui comprend des fabricants d'appareils mobiles, des éditeurs de logiciels, des fournisseurs d'équipements et des entreprises Internet, ainsi que des entreprises œuvrant dans des industries connexes. La GSMA organise également des événements phares du secteur, tels que les Mobile World Congress, Mobile World Congress Shanghai et les conférences de la série Mobile 360.

Pour plus d'informations, veuillez consulter le site web de la GSMA à **www.gsma.com**

Suivez la GSMA sur **Twitter: @GSMA**

Si vous souhaitez plus d'informations sur ce rapport ou si vous avez des questions, veuillez envoyer un e-mail à **publicpolicy@gsma.com**

A.T. Kearney est un cabinet de conseil en management de premier ordre sur le plan mondial, comptant des bureaux dans plus d'une quarantaine de pays. Depuis 1926, nous sommes les conseillers de confiance de quelques-unes des plus grandes organisations au monde. A.T. Kearney est un cabinet appartenant à un ensemble d'associés, engagé à aider ses clients à avoir un impact immédiat et à développer leur avantage sur les questions les plus critiques les concernant.

Pour en savoir plus, visiter **www.atkearney.com**

Sommaire

1 Synthèse

Ces trente dernières années, le marché des services de télécommunications mobiles a pris de l'ampleur et comptabilise actuellement plus de 7,6 milliards de connexions,[1] desservant 4,7 milliards de consommateurs uniques à l'échelle mondiale.[2] Cette croissance devrait se poursuivre, et on prévoit que d'ici 2020, près des trois quarts de la population mondiale bénéficieront d'un abonnement mobile.[3]

L'impact de cette croissance est visible tant dans les marchés développés que dans ceux en voie de développement. Les services mobiles ont permis aux particuliers, aux entreprises et aux États d'innover de manière inédite et souvent inattendue, avec des consommateurs dans le monde entier toujours prêts à adopter de nouvelles technologies. Grâce à l'omniprésence des services mobiles et des smartphones dans beaucoup de pays développés, des modèles d'affaires entièrement nouveaux se font jour, adoptant de nouveaux modes d'échanges personnels et commerciaux, qui permettent à l'écosystème mobile dans son ensemble de contribuer à hauteur de 3 100 milliards de dollars de valeur économique ajoutée.[4]

Devant l'importance économique et sociale croissante de l'Internet et de l'utilisation mobile d'Internet en particulier, il est nécessaire de protéger les consommateurs qui utilisent ces services et de veiller à ce qu'ils puissent continuer à les utiliser en toute sécurité et de manière sûre. Sans cette protection, les avantages des communications modernes risquent d'être compromis. Si les consommateurs ne peuvent pas avoir confiance dans l'intégrité d'un service de commerce électronique, ou craignent l'interception de leurs informations privées sensibles lorsqu'ils utilisent des services de communication, ils risquent d'être bien moins enclins à les utiliser et se sentir contraints d'avoir recours à des moyens de communication plus coûteux et moins efficaces. Dans les cas les plus extrêmes, un service qui dans les années 1990 était promu comme garant de sécurité (par example pour les automobilistes, ou les personnes vulnérables voyageant seules) et de respect de la vie privée (appels depuis un appareil personnel au lieu d'un téléphone fixe dans le salon familial), pourrait être utilisé de manière abusive et finir par nuire à ces besoins fondamentaux.

L'industrie du mobile a œuvré à l'éducation des consommateurs et a mis au point de nouvelles fonctionnalités qui ont renforcé la confiance dans ses services. Chaque nouvelle itération technologique introduit de nouvelles fonctionnalités, qu'il s'agisse de chiffrement ou de validation de l'identification de l'utilisateur, qui renforcent à chaque fois la sécurité des services mobiles tout en minimisant le risque de fraude, de vol d'identité ou d'autres menaces possibles.

Or il n'est pas possible de tenir pour acquise la confiance dans ces services et qui permet aux individus partout dans le monde de communiquer, d'échanger, de partager des idées et d'interagir. À mesure que des services plus évolués et plus complexes sont mis au point, la liste des menaces éventuelles, et du potentiel de nuire, ne fait que s'allonger. Des escroqueries et des attaques de plus en plus sophistiquées sont élaborées et perpétrées, et la capacité des criminels à intercepter des communications s'intensifie, que ce soit sous la forme de vol de données volumineuses ou de piratage suivi de la divulgation de communications privées au cours des élections américaines de 2016. Moins médiatisée mais tout aussi dommageable sur le plan individuel, il convient de mentionner la prévalence des attaques de phishing, de faux programmes (ransomware) et de fraude d'argent. Bien entendu, ces manœuvres ciblent les communications en général et pas seulement celles d'un appareil mobile, et par conséquent les solutions doivent envisager les services en question dans leur globalité.

Naturellement, les États et les décideurs politiques veulent agir pour empêcher ce type d'incidents et protéger les citoyens dans la plus large mesure possible. Néanmoins, dans un environnement d'une telle complexité, il est important que toute intervention soit correctement ciblée. Le potentiel pour qu'une action, aussi bien intentionnée soit-elle, finisse par avoir un coût disproportionné ou par réduire l'accès aux services qu'elle cherchait à protéger existera toujours. Par ailleurs, des compromis complexes sont à trouver entre la nécessité de protéger la sécurité des communications individuelles et celle pour les services de sûreté d'intercepter légalement certaines communications afin de protéger le grand public. Il ne faut pas perdre de vue la nature complexe et multipartite de bon nombre de ces services. Par exemple, deux personnes communiquant via un service de messagerie par « chat » utilisent en fait deux appareils différents, peut-être deux systèmes d'exploitation différents et deux applications d'interface, et une multitude de réseaux pour se connecter via une plateforme de messagerie souvent hébergée dans un ressort juridique différent de l'un des utilisateurs ou des deux. Chacun de ces maillons de la chaîne présente des faiblesses, des lacunes et des menaces potentielles qui lui sont propres, qu'il s'agisse d'écoutes ou d'abus, en passant par des risques de piratage ou de logiciels malveillants. Les efforts destinés à protéger les consommateurs peuvent être mal orientés s'ils se concentrent uniquement sur une faiblesse potentielle et ignorent les autres. Souvent les mesures visant à renforcer une partie déjà solide de la chaîne de services globale sont vaines pour combler les lacunes qui se trouvent dans une autre.

1. Connexions y compris machine-à-machine (M2M)
2. GSMA, 2016. « The Mobile Economy: 2016 »
3. Ibid.
4. Ibid.

1

Le secteur mobile a engagé des investissements considérables pour permettre une utilisation sûre et sécurisée de ses services, tout en cherchant aussi à protéger autant que possible la vie privée de ses clients. Ses efforts revêtent bien entendu une dimension technologique : amélioration continue des normes, déploiement de meilleures versions technologiques, tests des réseaux pour en déceler les faiblesses et renforcement des capacités afin de repérer les attaques malveillantes et de les empêcher. La GSMA joue un rôle essentiel en matière de coordination des activités et de lancement d'initiatives telles que le code IMEI (identifiant pour lutter contre le vol d'appareils mobiles) ou des régimes d'agrément de sécurité pour les éléments critiques d'infrastructures. Par ailleurs, de nombreux opérateurs mobiles et autres acteurs de l'écosystème sont extrêmement actifs sur leurs marchés et au sein des instances internationales afin d'optimiser l'efficacité des réponses technologiques.

Toutefois, la technologie à elle seule n'apporte pas toute la réponse à la multitude de menaces et de défis qui se présentent. Avec le soutien de la GSMA, l'industrie entière a été très active en participant à des programmes destinés à éduquer les consommateurs et les entreprises quant à la manière d'utiliser en toute sécurité les technologies mobiles et les applications qu'elles prennent en charge, afin de réduire au minimum les agissements illicites tels que les abus en ligne, la fraude et les violations de la vie privée. Une réponse globale s'impose à cet égard, sollicitant la participation des États, d'autres organismes et d'instances de soutien à but non lucratif, ainsi que celle des fournisseurs finaux de services livrés en ligne ou via des appareils mobiles, comme les services bancaires et les paiements en ligne.

Le problème bien plus répandu est celui du partage volontaire de données à caractère personnel afin d'avoir accès à des services commerciaux de bonne foi. Dans ce domaine, le secteur mobile est confronté à un défi différent : alors que huit consommateurs sur dix se disent inquiets de l'ampleur des données à caractère personnel qu'ils communiquent, il serait naturel de s'attendre à ce que les opérateurs de réseau cherchent à assouvir leurs craintes. Or en raison de questions technologiques et d'antitrust, il est extrêmement difficile (voire parfois impossible) pour un opérateur de réseau mobile d'intervenir dans les échanges qui se produisent entre un prestataire de service en ligne et l'utilisateur final. Par ailleurs, des critères de protection des données extrêmement disparates s'appliquent d'un pays à l'autre, et surtout entre le secteur des télécommunications et celui des prestataires de service en ligne. Le seul engagement qu'un opérateur puisse prendre est d'assurer la protection des données qu'il détient directement et de sensibiliser ses utilisateurs aux risques que ceux-ci encourent s'ils partagent leurs données avec d'autres organisations en dehors du contrôle de l'operateur. Les États et l'écosystème dans son ensemble devraient collaborer pour veiller à ce que les consommateurs fassent des choix éclairés et efficaces, en trouvant le juste équilibre entre le désir de chacun de protéger sa vie privée et son souhait d'accéder à partir d'un appareil mobile à du contenu et des applications intéressants financés par des publicités.

Parfois, ce sont les pouvoirs publics et les services de sûreté qui s'immiscent dans la prestation de services mobiles privés et sécurisés. Leur mandat à la fois légitime et de plus en plus sensible de protéger les citoyens les amène parfois à s'accorder des pouvoirs étendus pour accéder à des données à caractère personnel et les utiliser, ainsi qu'à intervenir pour bloquer ou limiter les services de communication dans des circonstances particulières. L'industrie reconnaît son obligation légale et morale d'appui à la sécurité publique et de respect des mandats légitimes des gouvernements dans le respect du droit, ainsi que son obligation légale et morale de respecter les droits de l'homme. Il arrive de plus en plus fréquemment que des opérateurs du monde entier aient à contester des interventions spécifiques qu'ils estiment disproportionnées, en décalage par rapport aux cadres internationaux relatifs aux droits de l'homme, voire potentiellement contre-productives par rapport à des objectifs de sécurité publique. Il s'agit là d'un domaine extrêmement complexe, qui revêt des différences considérables d'un pays à l'autre, d'où la démarche de la GSMA qui vise à poser des principes communs et à éduquer toutes les parties concernées sur les meilleures pratiques à adopter. Les opérateurs de réseaux mobiles sont confrontés à deux autres défis : ils se trouvent en première ligne quand les États cherchent à remettre en question les entreprises Internet mondiales vis-à-vis desquelles ils ont peu d'influence, voire aucune, et ils sont parfois tenus de garder le silence sur ce type d'activités, malgré leur souhait d'être transparents avec les consommateurs qui leur accordent leur confiance.

Action par les pouvoirs publics, le secteur mobile et d'autres parties prenantes

Le présent rapport s'arrête à tour de rôle sur chacune des grandes problématiques de la protection des consommateurs, du respect de la vie privée, de la sécurité publique et de la sûreté des infrastructures pour en souligner les problèmes potentiels, les mesures déjà prises en vue d'y remédier et les autres qui peuvent être nécessaires. L'importance de ces questions est telle que les opérateurs mobiles membres de la GSMA en sont venus à la conclusion qu'ils doivent travailler plus étroitement ensemble, tant à l'échelon mondial que national, pour que leur réponse ait le plus d'effet possible. Aucune de ces problématiques à facettes multiples ne peut être résolue d'un simple coup de baguette magique ou isolément par une organisation ou un secteur quelconque. Pour parvenir aux meilleurs résultats possibles pour les utilisateurs mobiles et la société dans son ensemble, il est nécessaire aussi d'obtenir l'engagement et l'action de la part des pouvoirs publics, des services de sûreté, d'organisations multilatérales et non gouvernementales et des entreprises de l'ensemble de l'écosystème numérique, sans oublier bien sûr les efforts individuels des consommateurs à proprement parler. Ces problématiques ne revêtent pas toutes le même ordre de priorité pour tous les pays et donc pour tous les opérateurs. En revanche, toutes ont en commun où que ce soit la nécessité d'une coopération plus étroite entre les multiples parties prenantes impliquées dans la prestation des services à l'utilisateur final, afin d'une part d'optimiser la sécurité et la confiance du consommateur, et d'autre part d'élaborer et de porter à exécution des solutions qui procurent le meilleur bénéfice global pour la société. Qu'il s'agisse de normes, d'équipements d'infrastructure, de services et d'opérateurs, la nature mondiale des systèmes de communication modernes fait que des mesures ponctuelles et unilatérales ne sont pas aussi efficaces qu'une approche coordonnée.

Le rapport présente un ensemble de principes auxquels adhèrent les opérateurs mobiles membres de la GSMA pour les orienter dans leurs actions visant à protéger le consommateur et à sécuriser les réseaux de communication mobile. Il lance aussi un appel aux décideurs politiques et aux régulateurs pour qu'ils se mettent à envisager les problématiques en jeu dans leur globalité, afin de contribuer à l'élaboration de solutions multipartites qui protègent au mieux l'intérêt général des consommateurs, des entreprises et de la société civile. En affichant clairement son engagement envers la sécurité, le respect de la vie privée et la sûreté des services de communications mobiles, le secteur cherche à veiller à ce que les avantages des communications mobiles continuent à se développer dans un avenir prévisible, à enrichir la vie et la société, en usant du plein potentiel de ces technologies aussi prometteuses que dynamiques.

1

Protection du consommateur

Des efforts multipartites doivent être déployés pour encourager l'utilisation sûre et responsable des services et appareils en ligne basés sur mobile. Il est particulièrement important que les pouvoirs publics et leurs services de sûreté veillent à la présence de cadres juridiques, de moyens et de processus appropriés pour empêcher, identifier et poursuivre des comportements criminels. Bien souvent, une telle démarche nécessite une coopération mondiale. Il incombe aussi à d'autres acteurs de l'écosystème du secteur, comme les fabricants d'appareils et les prestataires de services basés sur mobile par exemple, de participer à des initiatives visant à protéger les consommateurs lorsqu'ils utilisent des appareils et des services mobiles et à les éduquer sur l'adoption de comportements sécuritaires et de bonnes pratiques, pour qu'ils puissent continuer à bénéficier de ces services sans courir de danger. Les opérateurs de réseau mobile ont un rôle à jouer en sensibilisant les consommateurs aux dangers et en appelant à leur vigilance, et en les incitant à prendre l'ensemble complet des mesures de sécurité mises à leur disposition. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures proactives pour la protection des consommateurs en luttant contre les activités illicites et préjudiciables liées ou bien à l'utilisation du téléphone mobile ou bien aux activités que le mobile rend possibles, en adoptant les mesures suivantes :

- **Travailler en collaboration avec d'autres organismes pour offrir des solutions multilatérales**
- **Mettre en œuvre des solutions destinées à empêcher l'utilisation de réseaux à des fins d'activités frauduleuses et criminelles, et celle d'appareils en vue de nuire au consommateur**
- **Éduquer les consommateurs sur les comportements sécuritaires, dans le but de renforcer leur confiance, lors de l'utilisation des services et des applications mobiles**

Protection de la vie privée du consommateur

La protection de la vie privée vise essentiellement à renforcer la confiance en la protection adéquate des données à caractère privé, en conformité avec la réglementation et les exigences en matière de respect de la vie privée. Pour cela, toutes les parties concernées doivent adopter une approche cohérente, neutre sur le plan technologique, et constante entre l'ensemble des services, des secteurs et des territoires. Les pouvoirs publics peuvent y contribuer en accordant la souplesse nécessaire à l'innovation, en adoptant des cadres basés sur les risques de sauvegarde des données à caractère privé, et enfin en encourageant des pratiques responsables en matière de gouvernance numérique en accord avec la réglementation locale. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures proactives afin de protéger et de respecter la vie privée des consommateurs et de leur permettre de faire des choix éclairés sur le type de données recueillies et la manière dont leurs données à caractère personnel sont utilisées, en mettant en œuvre des politiques qui encouragent :

- **Le stockage et le traitement en toute sécurité des informations à caractère personnel et privé, en conformité avec les exigences légales le cas échéant**
- **Être transparent avec les consommateurs sur les données que nous partageons sous forme anonyme et en pleine conformité avec les exigences légales**
- **La mise à disposition aux consommateurs des informations et des outils nécessaires pour faire des choix simples et significatifs au sujet de leur vie privée**

Protection de la sécurité publique

Dans le cadre des lois et des règlements, y compris des obligations de licence, et conformément à la législation locale, les opérateurs de réseau mobile sont tenus dans l'obligation d'assumer des responsabilités supplémentaires pour aider les services de sûreté dans le respect de l'objectif global de protection de la sécurité publique. Il est important que les États aient en place un cadre juridique proportionnel qui précise clairement les pouvoirs à la disposition des services de sûreté. Le cadre juridique doit également veiller au caractère nécessaire et proportionné des demandes d'assistance, en s'assurant de les adresser au fournisseur du service de communication ou de technologie le plus approprié et compatible, et dans le respect des principes des droits de l'homme. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à se conformer à l'ensemble des obligations juridiques et de licence dans leurs réponses aux préoccupations de sûreté et de sécurité publique présentes dans les pays où ils opèrent, dans le plein respect des droits de l'homme. Nous nous engageons à coopérer avec les organes de sécurité en vue de protéger la sécurité publique en adoptant les mesures suivantes :

- **Dès lors que la situation l'exige, travailler avec les organismes compétents à l'élaboration et à la mise en œuvre de solutions appropriées en vue de parvenir à l'objectif final tout en faisant subir le minimum de perturbations aux consommateurs et aux services essentiels**
- **Renforcer les réseaux disposant de la fonctionnalité de remédier à des situations d'urgence et de sécurité, le cas échéant**
- **Stipuler clairement notre limite d'action vis-à-vis de la chaîne de valeur en soulignant les domaines qui relèvent de l'intervention de tiers**

Protection de la sécurité des réseaux et de l'intégrité des appareils

Les acteurs du secteur doivent travailler ensemble et être coordonnés avec les services de sûreté internationaux pour partager des renseignements sur les menaces potentielles, afin de contrer les attaques malveillantes perpétrées sur des réseaux et des appareils mobiles et aussi pour identifier ses auteurs. Il s'agit pour cela de solliciter la participation des équipes d'intervention existantes en cas d'incident de sécurité et au besoin d'en créer de nouvelles pour combler les lacunes éventuelles. Les règlements, si nécessaires, doivent s'appliquer de manière cohérente entre tous les prestataires de la chaîne de valeur, d'une manière neutre sur les plans du service et de la technologie, tout en préservant le modèle multipartite pour la gouvernance de l'Internet et lui permettant d'évoluer. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures pour protéger l'infrastructure sous-jacente et veiller à apporter aux consommateurs le service de communication le plus sûr et le plus fiable, et ce comme suit :

- **Prendre des mesures pour sécuriser l'infrastructure du réseau que nous exploitons et contrôlons**
- **Promouvoir le partenariat public-privé afin de minimiser les risques, soit de piratage, soit d'exploitation du réseau à des fins malveillantes par des approches mondiales et coordonnées**
- **Stipuler clairement la responsabilité qui incombe aux opérateurs vis-à-vis des infrastructures et la démarcation des limites avec d'autres infrastructures ou services**

2 Introduction

Dans toutes les régions du monde, les menaces tant réelles que perçues posées à la sécurité nationale, à la sécurité publique et au respect de la vie privée sont à la hausse. Les réseaux mobiles ont un rôle à jouer dans la protection de la sécurité publique, notamment quand les services de sûreté compétents usent de leur mandat pour mener des enquêtes criminelles à partir de données d'appels et d'interception des communications, pour prendre en charge les communications suite à des incidents majeurs ou pour assurer le suivi de la propagation de menaces sanitaires. Au niveau individuel, des cas de fraude, d'usurpation d'identité, de cyberintimidation et d'autres activités illégales sont commis sur les réseaux mobiles, ainsi que sur les services en ligne ou numériques dont l'accès se fait via des réseaux fixes. L'actualité récente, notamment avec les affaires très médiatisées de violations de données, ont également provoqué le malaise parmi beaucoup de consommateurs qui se posent des questions sur leur sécurité et la protection de leur vie privée, notamment en ce qui concerne les détails sur leur vie personnelle.

C'est dans ce contexte que les opérateurs de réseau mobile sont confrontés à la difficulté croissante d'assurer une expérience mobile à la fois sûre et sécurisée pour leurs consommateurs, tout en s'acquittant de leurs obligations de protéger la sécurité publique. La GSMA et les opérateurs qui en sont membres font déjà beaucoup pour s'attaquer aux problèmes du respect de la vie privée et de la sécurité et pour y remédier, ainsi que pour promouvoir l'utilisation sûre et bénéfique des services mobiles et du vaste éventail d'applications qu'ils prennent en charge.

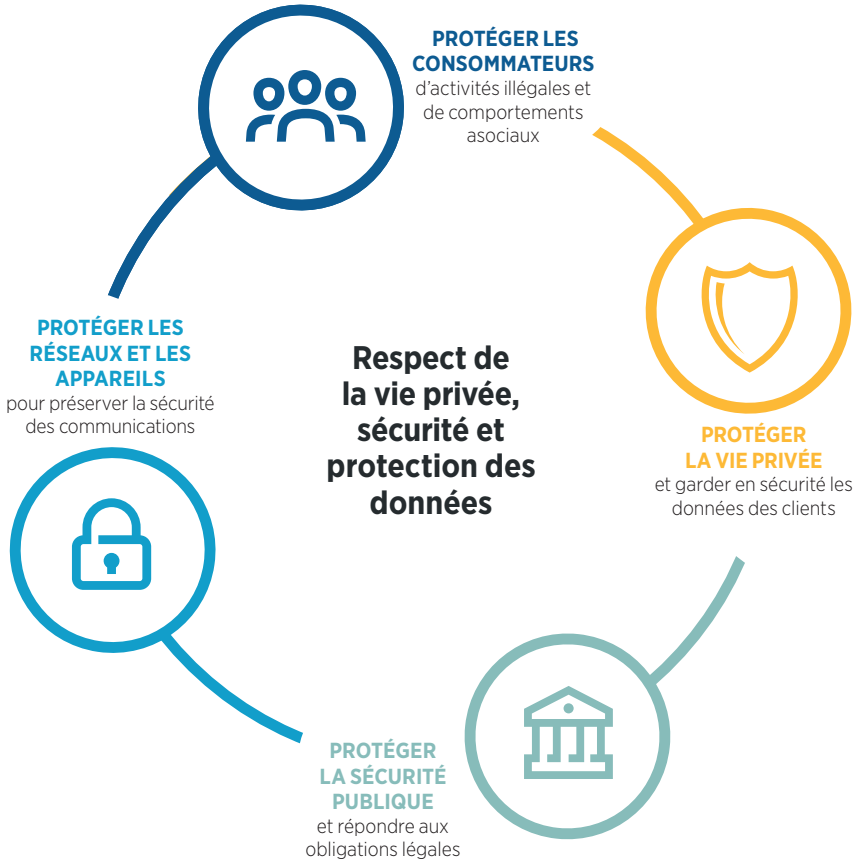
Le présent rapport cherche à expliquer les grands enjeux et défis portant sur la sécurité, le respect de la vie privée et la sécurité dans le monde mobile, en soulignant les complexités et les compromis qui existent et en faisant connaître les initiatives et les mesures déjà prises par le secteur. Lorsqu'il existe de la marge de manœuvre pour faire plus, le rapport en relève les domaines concernés et décrit les mesures à prendre pour mener à bien les interventions envisagées, qu'il s'agisse d'éduquer les consommateurs, d'établir des partenariats dans l'ensemble de l'écosystème, ou d'élaborer et de mettre en œuvre des solutions techniques multipartites. Le rapport aborde chaque problématique à tour de rôle, tout en reconnaissant les nombreuses interdépendances et les chevauchements qui existent entre elles.

Structure

Le thème général de la sécurité et du respect de la vie privée est vaste mais il peut être abordé sous quatre grandes rubriques, illustrées à la Figure 1.

Figure 1

Cadre du respect de la vie privée et de la sécurité



Les quatre sections suivantes du présent rapport s'arrêtent sur chaque domaine à tour de rôle, à savoir :

1. **Protection du consommateur** : encourager l'utilisation sécurisée des services mobiles
2. **Respect de la vie privée et protection des données** : protéger la vie privée des consommateurs ainsi que le stockage et le traitement sécurisés des données à caractère personnel des individus
3. **Protection de la sécurité publique** : définir le rôle et les responsabilités des opérateurs mobiles à l'appui des pouvoirs publics pour protéger le public
4. **Protection de l'infrastructure du réseau et des appareils** : assurer l'intégrité et la sécurité de l'infrastructure du réseau mobile et des appareils utilisés pour accéder à ces réseaux mobiles

La dernière section énonce les principes de haut niveau qui ont été approuvés par les opérateurs membres de la GSMA et elle décrit brièvement les plans visant à les intégrer dans les activités futures de la GSMA.

Comme le rapport le fera apparaître, la nature de ces problématiques nécessite une action coordonnée dans l'ensemble des pays ainsi qu'entre les segments du secteur. Bien que le secteur mobile soit le chef de file pour s'attaquer à ces problématiques, beaucoup de groupes sont actifs dans ce domaine, qu'il s'agisse d'organismes de normalisation, comme 3GPP, l'IETF et oneM2M, ou d'organismes mondiaux, comme l'UIT, Telecommunications Industry Dialogue (ID), la Global Network Initiative (GNI) et l'UNICEF. Ils ont tous autant les uns que les autres un rôle précieux et important à jouer pour façonner les discussions et élaborer des solutions. La GSMA est ouverte à toute autre initiative de collaboration et de participation provenant de l'ensemble de l'écosystème mobile et de l'industrie globale des TIC sur l'intégralité de ces sujets.

3 Protection du consommateur

Alors que les services mobiles continuent de croître rapidement en termes d'importance et de portée, ils changent fondamentalement la façon dont les gens se connectent et interagissent entre eux et avec les entreprises. Comme c'est souvent le cas avec un mouvement de fond comme celui-ci, il y en a toujours qui cherchent à profiter de la situation pour nuire à autrui.

Pour que les consommateurs du monde entier puissent continuer à bénéficier des nombreux avantages de la technologie mobile, il est important qu'ils puissent utiliser ces services en toute confiance et en toute sécurité. Cette section traite des enjeux qui touchent directement la sécurité et le bien-être des consommateurs de services mobiles, et plus particulièrement des utilisateurs d'appareils et de services mobiles qui sont exposés à des menaces de comportement illégal, criminel ou antisocial, et aborde donc les thèmes suivants :

- La protection des enfants et des personnes vulnérables
- Le vol et le commerce d'appareils volés et la vente et l'utilisation d'appareils de contrefaçon
- La fraude et la sécurité des appareils mobiles

Chacun de ces enjeux constitue une implication importante pour les pouvoirs publics, pour l'industrie ainsi que pour les autres parties prenantes. Ils sont également traités avec plus de détail plus loin dans ce chapitre.

Protection des consommateurs

Des efforts multipartites doivent être déployés pour encourager une utilisation sûre et responsable sur mobile des services en ligne et d'appareils connectés. Il est particulièrement important que les pouvoirs publics et leurs services de sûreté veillent à la présence de cadres juridiques, de moyens et de processus appropriés pour empêcher, identifier et poursuivre des comportements criminels. Bien souvent, une telle démarche nécessite une coopération globale. Il incombe aussi à d'autres acteurs de l'écosystème du secteur, comme les fabricants d'appareils et les prestataires de services basés sur mobile par exemple, de participer à des initiatives visant à protéger les consommateurs lorsqu'ils utilisent des appareils et des services mobiles et à les éduquer sur l'adoption de comportements sécuritaires et de bonnes pratiques, pour qu'ils puissent continuer à bénéficier de ces services sans courir de danger. Les opérateurs de réseau mobile ont un rôle à jouer en sensibilisant les consommateurs aux dangers et en appelant à leur vigilance, et en les incitant à prendre l'ensemble complet des mesures de sécurité mises à leur disposition. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures proactives pour la protection des consommateurs en luttant contre les activités illicites et préjudiciables liées ou bien à l'utilisation du téléphone mobile ou bien aux activités que le mobile rend possibles, en adoptant les mesures suivantes :

- **Travailler en collaboration avec d'autres organismes pour offrir des solutions multilatérales**
- **Mettre en œuvre des solutions destinées à empêcher l'utilisation de réseaux à des fins d'activités frauduleuses et criminelles, et celle d'appareils en vue de nuire au consommateur**
- **Éduquer les consommateurs à des comportements sécuritaires, afin de renforcer leur confiance, lors de l'utilisation des services et des applications mobiles**

Les enfants et les personnes vulnérables

Pour les groupes d'utilisateurs potentiellement vulnérables, notamment mais pas exclusivement les enfants et des femmes, les services mobiles offrent de nombreux avantages pour les aider à rester plus connectés, plus indépendants et plus en sécurité. Il n'empêche pas moins que les enfants et les personnes vulnérables sont aussi exposés au risque de comportements préjudiciables. Ainsi, une étude de la GSMA examinant l'écart entre les sexes en ce qui concerne la propriété et l'utilisation d'appareils mobiles a constaté que 68 % des femmes ont tendance à percevoir comme obstacles les dangers courus liés à la possession et à l'utilisation d'appareils mobiles ainsi que le harcèlement de la part d'inconnus.[5] La question de la « sécurité et du harcèlement » figure au rang des cinq principaux obstacles à la possession et à l'utilisation de téléphone mobile par les femmes.[6] Alors qu'il est important de noter que, à l'instar des hommes, les femmes pouvant être considérées vulnérables ne représentent qu'une partie de ce groupe, il convient de reconnaître ces préoccupations et d'y remédier pour garantir l'accès universel aux nombreux avantages de la connectivité, surtout quand il s'agit de groupes susceptibles d'avoir le plus à gagner de l'utilisation de services mobiles.

Les consommateurs doivent se familiariser avec la manière d'utiliser en toute sécurité les fonctions de leur appareil mobile (par ex., la caméra) et les services basés sur le mobile. Ce besoin est exacerbé par le fait que les appareils mobiles sont de plus en plus puissants et peuvent être utilisés pour réaliser toujours plus de tâches courantes, y compris accéder à l'éducation formelle et à l'apprentissage informel, à des services bancaires et à des applications d'e-santé. Alors que les consommateurs apprennent à tirer parti de ces nombreux avantages, l'occasion se présente d'élargir activement leurs compétences numériques en constante évolution en inscrivant la prise en compte de la sécurité sur Internet par le biais de programmes d'éducation et de sensibilisation. Les programmes conçus pour aider à renforcer cette « résilience numérique » vont nécessiter la contribution de tout un éventail de parties prenantes. Il est important que les opérateurs de réseau mobile participent à l'élaboration de ces programmes pour s'assurer qu'ils répondent aux besoins d'une industrie en mutation rapide et clarifient les rôles dévolus aux différents acteurs de l'écosystème des TIC. Les opérateurs de réseau mobile jouent déjà un rôle dans la promotion des avantages de la technologie mobile tout en éduquant les groupes potentiellement vulnérables à la manière de renforcer leur résilience numérique, d'utiliser les services en toute sécurité et de répondre et signaler tout abus qui se présente.

Soutien de l'inclusion et de la sécurité des femmes

En moyenne, les femmes sont 14 % moins susceptibles de posséder un appareil mobile que les hommes, cet écart entre les sexes pouvant atteindre 38 % dans certaines régions.[7] Cela équivaut à 200 millions de femmes en moins que les hommes à être propriétaires d'un appareil mobile.[8] Au total, plus de 1,7 milliard de femmes dans les pays à revenus faibles et intermédiaires ne possèdent pas d'appareil mobile.[9] Les raisons à cela sont variées et le programme Femmes Connectées de la GSMA s'attèle à les isoler et à y remédier. Les problèmes de sécurité et de harcèlement se sont révélés être des obstacles importants à l'adoption d'appareils mobiles par certaines femmes, surtout dans les pays à faible revenu.[10] La GSMA et ses organisations membres lancent actuellement une initiative qui renforce l'action de Femmes Connectées en accordant un accent particulier aux questions de sécurité et de harcèlement.

Les opérateurs de réseau mobile reconnaissent qu'en utilisant des services de sécurité mobile, les femmes peuvent continuer à bénéficier de la sécurité offerte par la connectivité tout en minimisant les risques de harcèlement dont elles font l'objet. Par exemple, dans de nombreux pays, des opérateurs de réseau mobile ont lancé des services de blocage automatique d'appels non désirés, qui peuvent être particulièrement attrayants pour les utilisatrices. Il existe aussi des services pour les propriétaires de téléphones portables grand public ou basiques, tels que « Urgence Banglalink » qui envoient automatiquement une alerte SMS à trois contacts préalablement enregistrés quand l'utilisateur compose un numéro abrégé. La position géographique de l'utilisateur est également envoyée à ces contacts,[11] ce qui accroît leur sécurité.

5. GSMA, 2015. "Connected Women – Bridging the Gender Gap: Mobile Access and Usage in low- and middle- income countries"
6. Ibid.
7. Ibid.
8. Ibid.
9. Ibid.
10. Ibid.
11. Banglalink Emergency: http://www.banglalink.com.bd/en/services/services/information-based-services/banglalink-emergency/

Protection des jeunes utilisateurs et protection en ligne des enfants

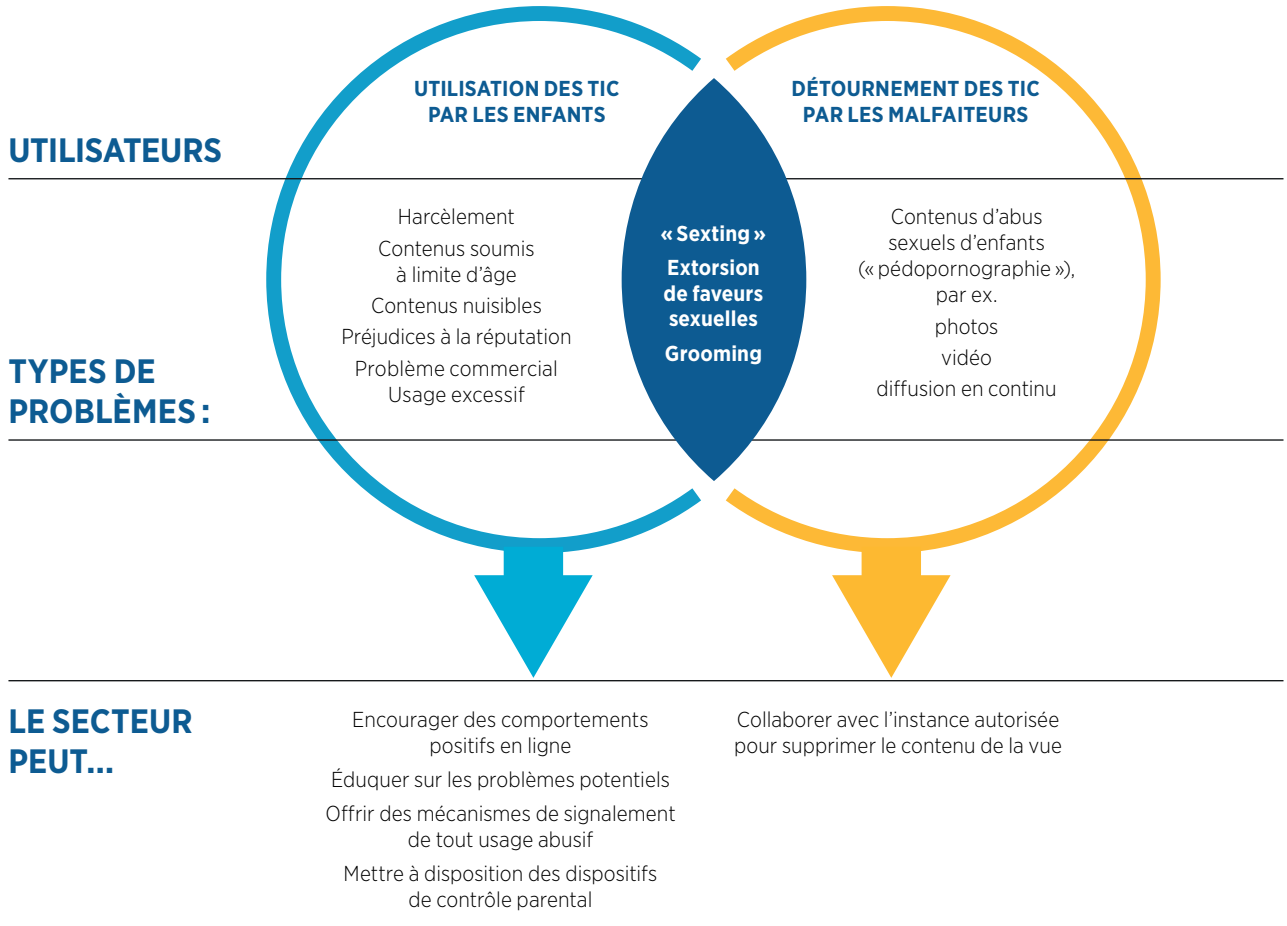
Les enfants constituent un deuxième groupe d'utilisateurs potentiellement vulnérables des services mobiles. Pour comprendre la problématique de la protection en ligne des enfants, il est important de bien faire la distinction entre deux axes d'action distinctes :

1. Encourager l'usage sûr et responsable des services mobiles par les enfants
2. Lutter contre l'usage abusif des services mobiles par des adultes/délinquants, par exemple en matière de contenus illicites d'abus sexuels d'enfants, qu'il s'agisse d'en produire, de les distribuer ou d'y accéder

Comme le montre la Figure 2, cette distinction est utile car les groupes touchés et les mécanismes d'intervention requis diffèrent grandement.

Figure 2

Protection en ligne des enfants – les enjeux et les utilisateurs



Un élément essentiel pour permettre aux enfants et aux jeunes de mener une vie numérique plus sûre consiste à les inciter à adopter des comportements positifs en ligne, tout en les éduquant sur les risques potentiels qui existent, pour qu'ainsi ils aient les moyens de naviguer sur Internet de manière plus sûre avec une confiance accrue. Le secteur mobile, aux côtés d'autres parties prenantes comme les éducateurs, les parents et les groupes représentant les enfants, y contribue par la mise en œuvre et l'application de politiques d'utilisation acceptables, l'instauration de mécanismes de signalement en cas d'usage abusif et la mise en place de dispositifs de contrôle parental.

Pour le deuxième enjeu qui consiste à lutter de manière robuste contre l'usage abusif des technologies pour accéder à des contenus d'abus sexuels d'enfants, en partager ou en profiter, un certain nombre d'actions se révèlent nécessaires de la part d'un éventail de parties prenantes. Les États doivent avoir en place une législation appropriée, les services de sûreté doivent être dotés des moyens nécessaires pour enquêter sur tous les aspects des abus sexuels commis contre des enfants en ligne (en partant du « grooming » jusqu'au partage de contenus pédopornographiques) et il est nécessaire de mettre en place des services nationaux pour le signalement d'abus sexuels d'enfants découverts en ligne. Les acteurs du secteur peuvent alors contribuer à cette réponse commune, par exemple, en travaillant en étroite collaboration avec le service de signalement national afin de supprimer de leurs services les contenus d'abus sexuels d'enfants dès qu'ils en prennent connaissance, et en travaillant avec les pouvoirs publics lorsque les circonstances s'y prêtent et dans le respect des procédures régulières.

Dans les domaines de chevauchement, illustrés à la Figure 2, ces deux types d'intervention s'imposent. Ainsi par exemple, pour atténuer les risques que des jeunes partagent des images sexuelles d'eux-mêmes qu'ils ont autoproduites (« sexting »), ces enfants doivent comprendre les conséquences potentielles de partager ces images et d'en perdre le contrôle. Lorsqu'un délinquant prend possession de contenu sexuel autoproduit et le partage, il est nécessaire alors de déclencher une procédure pour supprimer le contenu de la vue (comme on l'expliquera dans plus de détail à la rubrique concernant les contenus d'abus sexuels d'enfants), ainsi que pour enquêter sur l'auteur de l'infraction et le poursuivre en justice.

Encourager l'utilisation sûre et responsable des technologies et des services mobiles par les enfants

Aux côtés d'autres parties prenantes, le secteur mobile a pris des mesures actives afin d'encourager l'usage plus sûr des services mobiles par les enfants et les jeunes. En collaborant avec des parties prenantes issues de l'ensemble de l'écosystème mobile, ainsi que des ONG et des organisations gouvernementales, le programme mYouth[12] de la GSMA a pour vocation d'aider les jeunes à tirer le meilleur parti de leur expérience mobile. S'ajoutant à d'autres initiatives, le programme mYouth éclaire des approches visant à promouvoir l'utilisation sûre et responsable des appareils mobiles. Les approches adoptées par les opérateurs de réseau mobile sont multiples, qu'il s'agisse de programmes d'éducation et de sensibilisation des plus variés ou de mise à disposition de solutions techniques comme des services de contrôle parental. Dans le cadre de son partenariat avec Child Helpline International, la GSMA a élaboré des lignes directrices sur les questions de l'usage plus sûr de l'Internet pour la communauté des lignes d'assistance aux enfants, et faire en sorte que quand ils sont confrontés à des problèmes en ligne, les enfants puissent contacter une ligne d'assistance aux enfants où un conseiller formé se tient à leur disposition pour les soutenir.[13]

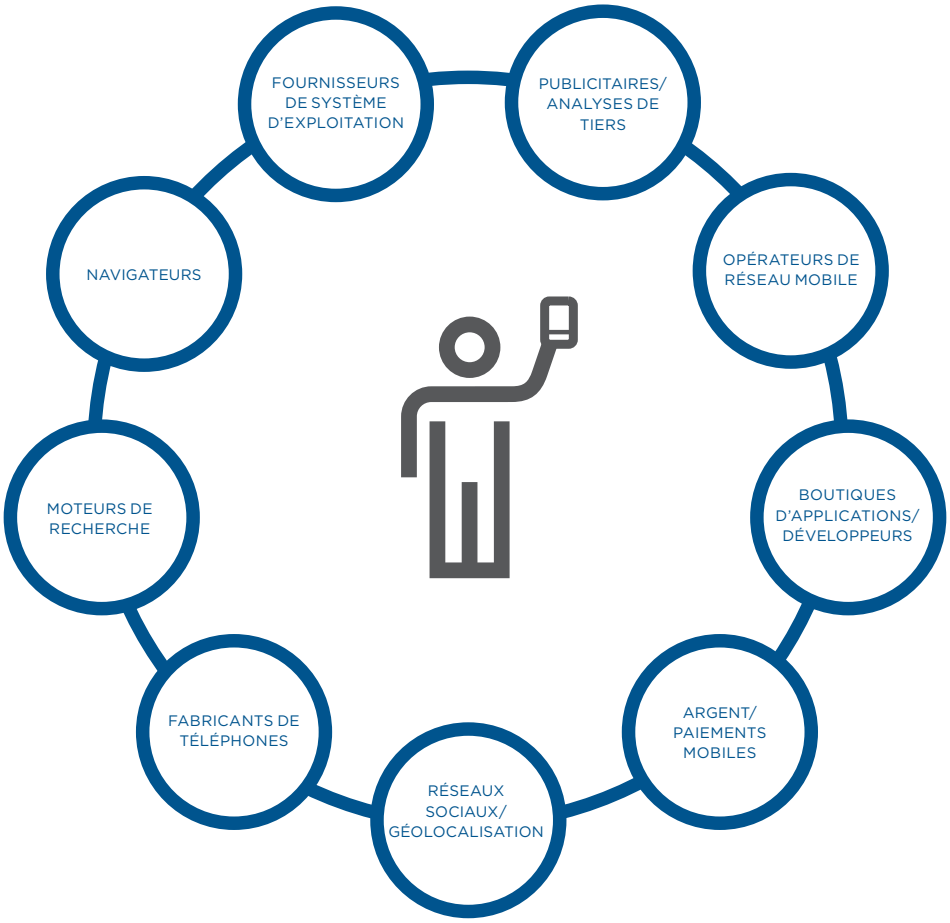
En ce qui concerne la protection des droits de l'enfant sur Internet, les entreprises et d'autres parties prenantes doivent trouver le juste équilibre entre le droit de l'enfant à la protection, son droit d'avoir accès à l'information et à la liberté d'expression. Il revient donc aux entreprises de veiller à cibler des mesures destinées à protéger les enfants sur Internet sans être indûment restrictives, pas plus pour l'enfant que pour d'autres utilisateurs. Les lignes directrices de l'UIT et d'UNICEF à l'usage des professionnels pour la protection en ligne des enfants soulignent les mesures qui peuvent être prises pour aider à protéger et à promouvoir les droits de l'enfant dans un monde numérique.[14]

L'évolution rapide de l'écosystème mobile ajoute de la complexité à ce domaine. Le modèle de services de contenu pris en charge par l'opérateur a évolué. Dans le paysage actuel, les utilisateurs disposent de multiples moyens d'accéder à toutes sortes de contenus numériques à partir de leurs appareils mobiles. Beaucoup d'acteurs ont un rôle à remplir pour les doter de ces moyens, y compris les opérateurs de réseau mobile, comme l'illustre la Figure 3.

12. Le programme mYouth de la GSMA a pour mission de promouvoir l'utilisation positive, sécurisée et responsable des services mobiles par les jeunes. Cette initiative multipartite comprend des partenariats conclus avec Child Helpline International et l'UNICEF. Pour en savoir plus, voir : http://www.gsma.com/publicpolicy/customer-affairs/children-mobile-technology/myouth
13. Pour prendre connaissance des lignes directrices, voir : http://www.childhelplineinternational.org/resources/manuals-toolkits/internet-safety-guides/
14. UIT et UNICEF, 2014. « Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants »

Figure 3

L'écosystème mobile



Les distinctions traditionnelles qui existent entre les différentes parties du secteur des télécommunications et entre les sociétés internet et les diffuseurs sont rapidement en train de tomber ou de perdre en pertinence. L'État, le secteur privé, les décideurs politiques, les éducateurs, la société civile et les parents ont chacun de leur côté un rôle vital à jouer en encourageant l'utilisation plus sûre des services mobiles par les enfants et les jeunes.[15] La coopération et le partenariat entre ces parties sont fondamentaux pour poser les bases à une utilisation plus sûre et sécurisée d'Internet et des technologies associées.

La GSMA remplit un rôle de chef de file dans le domaine des initiatives d'autoréglementation pour le secteur mobile et a apporté une contribution essentielle aux lignes directrices de l'UIT et de l'UNICEF à l'usage des professionnels pour la protection en ligne des enfants. La GSMA échange activement avec les États et les régulateurs, les décideurs politiques, les services de sûreté et le secteur afin de faciliter l'élaboration d'approches collaboratives prônant une utilisation sécurisée et responsable de l'Internet.

15. UIT et UNICEF, 2014. « Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants »

Pour approfondir

Lignes directrices de l'UIT et de l'UNICEF à l'usage des professionnels pour la protection en ligne des enfants

Les Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants sont destinées à poser les bases d'une utilisation plus sûre et plus sécurisée de services basés sur Internet et de technologies connexes pour les enfants d'aujourd'hui et les générations de demain.

Les Lignes directrices à l'usage des professionnels pour la protection en ligne des enfants sont nées des consultations qui ont eu lieu avec des membres de l'Initiative sur la Protection en ligne des enfants, ainsi que d'une plus large consultation ouverte qui a invité des membres de la société civile, d'entreprises, d'universités, des pouvoirs publics, des médias, d'organisations internationales et des jeunes pour qu'ils disent ce qu'ils pensent de ces lignes directrices.

La coopération et le partenariat sont fondamentaux pour poser les bases à une utilisation plus sûre et sécurisée d'Internet et des technologies associées. Les pouvoirs publics, le secteur privé, les décideurs politiques, les éducateurs, la société civile, les parents et les proches soignants ont chacun un rôle crucial à jouer pour parvenir à ce but. Les initiatives d'autoréglementation de l'industrie peuvent intervenir dans cinq domaines d'action :

1. **Inscrire les considérations des droits de l'enfant dans les stratégies d'entreprise et les processus de gestion**
2. **Élaborer des procédures normalisées pour gérer le matériel d'abus sexuels d'enfants**
3. **Créer un environnement en ligne plus sûr et adapté à l'âge**
4. **Éduquer les enfants, les parents et les enseignants sur la sécurité des enfants et leur utilisation responsable des technologies de l'information et des communications (TIC)**
5. **Promouvoir les technologies numériques en vue d'accroître la participation civique**

Combattre les contenus d'abus sexuels d'enfants en ligne

Même si les lois relatives aux contenus illégaux varient considérablement d'un pays à l'autre, il existe un consensus quasi-universel autour du caractère illégal des contenus d'abus sexuels d'enfants. Il ne fait pas de doute que l'exploitation sexuelle des enfants par des individus ou des organisations qui cherchent à consommer, partager ou profiter de contenus d'abus sexuels d'enfants relève d'une conduite qui est universellement reconnue comme étant inacceptable.

Comme on l'a vu plus haut, la lutte contre l'utilisation abusive des technologies en ce qui concerne les contenus d'abus sexuels d'enfants nécessite que les États aient en place une législation appropriée, des services de sûreté équipés et habilités à enquêter et des services de signalement nationaux opérationnels pour signaler des abus sexuels d'enfants. Les fournisseurs de services Internet et les opérateurs de réseau mobile sont en mesure de jouer un rôle essentiel dans la prévention de la revictimisation des enfants qui ont subi des abus sexuels en prenant des mesures pour limiter l'accès à des contenus d'abus sexuels d'enfants. Par exemple, les membres de l'Alliance Mobile contre les Contenus d'Abus Sexuels sur Mineurs de la GSMA (l'Alliance Mobile)[16] s'attellent à entraver l'utilisation des services mobiles par des individus ou des organisations qui souhaitent consommer ou profiter de contenus d'abus sexuels d'enfants. Ils y parviennent par une démarche de collaboration et de partage de l'information, en collaboration avec les services de signalement, en ayant en place des procédures de notification et de retrait et en restreignant l'accès aux URL ou aux sites web qu'une autorité compétente estime abriter des contenus d'abus sexuels d'enfants. Il est important de souligner que la décision quant aux URL ou aux domaines à bloquer relève d'une autorité compétente (comme INTERPOL, un service de signalement national ou un service de sûreté). Comme cela, les opérateurs de réseau mobile peuvent se reporter à cette liste et veiller à la mettre en application sans être mis dans une position où il leur est demandé de juger de la légalité de contenus spécifiques.

Les membres de l'Alliance Mobile GSMA se sont engagés à surveiller les tendances émergentes qui se répercutent dans ce domaine et de mettre en œuvre des réponses appropriées. Ainsi, l'Alliance Mobile de la GSMA a déjà commencé à travailler avec ses partenaires extérieurs pour comprendre et contrôler les impacts potentiels de chiffrement sur la restriction de l'accès à des contenus d'abus sexuels d'enfants connus, et pour y remédier s'il y a lieu.

16. Pour en savoir plus sur l'Alliance Mobile, voir : http://www.gsma.com/publicpolicy/consumer-affairs/children-mobile-technology/mobile-alliance

Pour approfondir

L'Alliance Mobile contre les Contenus d'Abus Sexuels sur Mineurs de la GSMA

L'Alliance Mobile contre les Contenus d'Abus Sexuels sur Mineurs (l'Alliance Mobile) a été fondée par un groupe international d'opérateurs mobiles regroupés au sein de la GSMA en vue de travailler collectivement afin de faire obstruction à l'utilisation de l'environnement mobile par des individus ou des organisations qui souhaitent consommer ou profiter de contenus d'abus sexuels d'enfants.

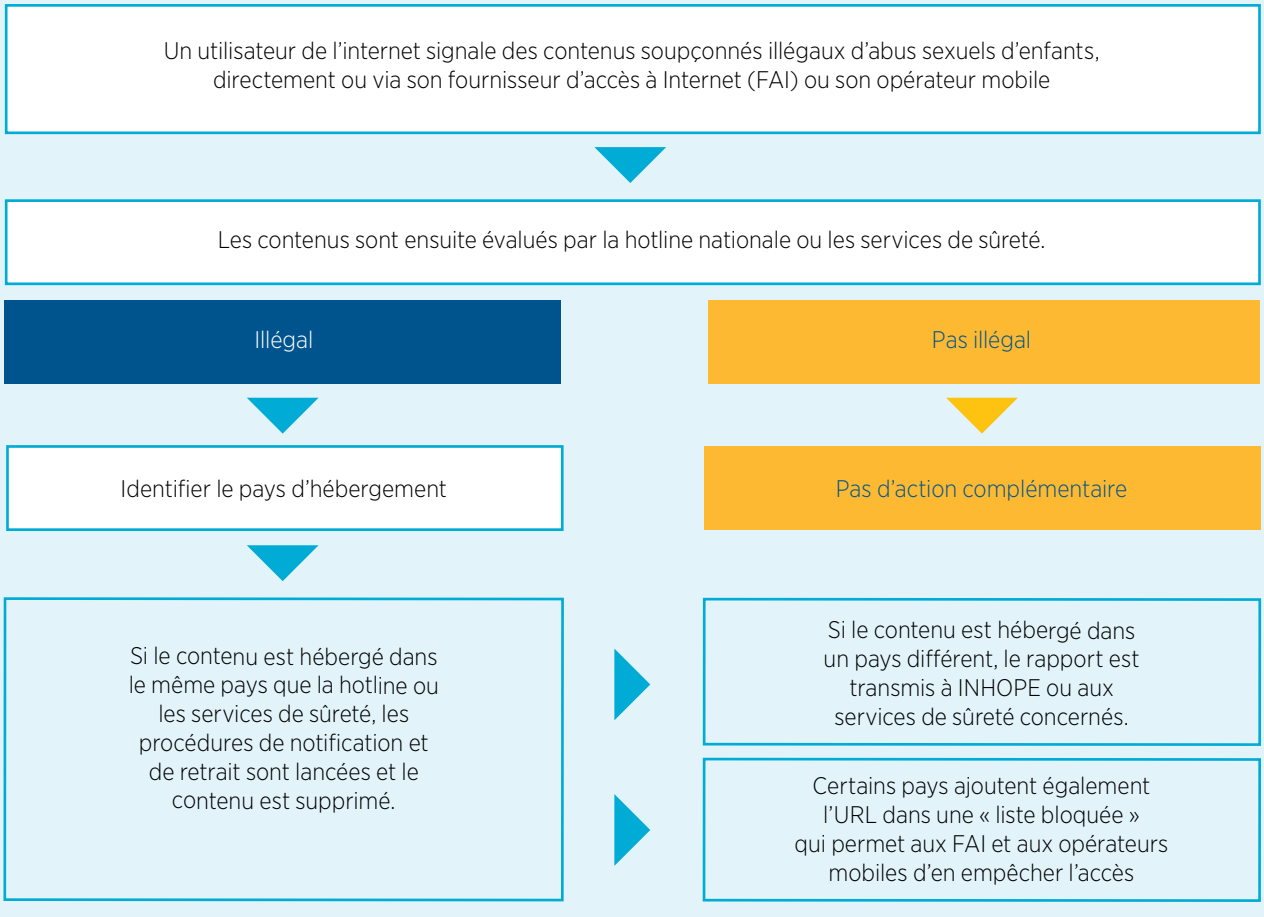
Les membres de l'alliance se sont engagés à :

- **Mettre en œuvre des mécanismes techniques visant à restreindre l'accès à des URL identifiés par un organisme approprié, reconnu au niveau international comme comportant des contenus d'abus sexuels d'enfants**
- **Appliquer les procédures de notification et de retrait pour permettre la suppression de tout contenu d'abus sexuels d'enfants posté sur leurs propres services**
- **Soutenir et promouvoir les lignes d'assistance ou les autres mécanismes à la disposition des consommateurs pour signaler des contenus d'abus sexuels d'enfants découverts sur Internet ou dans les services de contenu mobile**

Au moyen d'un ensemble de mesures techniques, de coopération et de partage d'informations, l'Alliance Mobile œuvre à juguler et au bout du compte à inverser la croissance des contenus d'abus sexuels d'enfants en ligne dans le monde entier.

L'Alliance Mobile contribue également aux efforts plus larges d'éradication des contenus d'abus sexuels d'enfants en ligne en publiant des conseils et des boîtes à outils pour le bénéfice de l'ensemble du secteur des communications mobiles. Elle a ainsi produit un guide pour établir et gérer une ligne d'assistance en collaboration avec INHOPE, l'organisation qui regroupe plusieurs hotlines, et un guide pour la mise en œuvre de procédures de notification et de retrait avec l'UNICEF. Elle collabore également avec la Coalition Financière Européenne (EFC) et la Coalition Financière contre la pédopornographie (FCACP).

Exemple de traitement de contenus d'abus sexuels d'enfants par les services de signalement et leurs partenaires



3

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Les appareils et les services mobiles enrichissent la vie des jeunes. Cette perspective doit être adoptée, encouragée et mieux comprise par toutes les parties prenantes afin que les jeunes tirent un maximum d'avantages de la technologie mobile. La meilleure approche à adopter pour veiller à la protection en ligne des enfants consiste à engager des efforts multipartites pour encourager l'utilisation sûre et responsable des services en ligne et des appareils Internet chez les enfants et les jeunes, et donner les moyens aux parents et tuteurs d'échanger avec leurs enfants, et de contribuer à leur protection, dans le monde numérique.[17]

D'autre part, l'éventail complet de réponses pour combattre les contenus d'abus sexuels d'enfants passe par la législation, des lignes de signalement, l'engagement des services de sûreté, le soutien aux victimes, avec les mesures et les procédures techniques nécessaires pour y venir à l'appui. Alors que les opérateurs de réseau mobile cherchent à jouer un rôle pour s'attaquer à ce problème, notamment à travers l'Alliance Mobile, pour avoir un impact réel, il leur faut le soutien, le leadership et la redevabilité d'autres organismes et instances compétents.

Le secteur mobile condamne le recours abusif à ses services pour partager des contenus d'abus sexuels d'enfants.

- L'Alliance Mobile contre les Contenus d'Abus Sexuels sur Mineurs de la GSMA assure un leadership dans ce domaine et travaille pro-activement pour combattre l'utilisation abusive des réseaux et des services mobiles par des criminels dans le but d'accéder à des contenus d'abus sexuels d'enfants ou de les partager.[18]
- Les opérateurs de réseau mobile utilisent les conditions générales d'utilisation, des procédures de notification et de retrait et des mécanismes de signalement pour faire en sorte que leurs services soient dépourvus de ce type de contenus.[19]
- Le secteur mobile a pris l'engagement de collaborer avec les services de sûreté et les autorités compétentes pour permettre la suppression ou la désactivation rapide des cas confirmés de contenus illégaux hébergés par leurs services,[20] y compris des contenus d'abus sexuels d'enfants

Il revient aux États de faire preuve d'ouverture et de transparence quant aux contenus qui sont illégaux dans leurs pays, avant d'en confier la responsabilité de l'application à des lignes de signalement, aux services de sûreté et au secteur, sous réserve du respect de la procédure légale.[21] En revanche, ces initiatives proactives ne doivent pas pour autant dégénérer en des mesures susceptibles d'enfreindre les conventions internationales sur les droits de l'homme ou la responsabilité du secteur privé, tels que définis par les Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme. Les États peuvent s'ils le souhaitent adhérer à des initiatives telles que WePROTECT Global Alliance et au modèle de cadre d'intervention nationale qui y est proposé comme outil utile pour orienter leur réponse à des contenus d'abus sexuels d'enfants.[22]

17. GSMA, 2016. « Manuel des politiques de communications mobiles : Les enfants et la technologie mobile »
18. GSMA, 2016. « Manuel des politiques de communications mobiles : Contenus illégaux »
19. Ibid.
20. Ibid.
21. Ibid.
22. Pour plus d'informations, voir : http://www.weprotect.org/the-model-national-response/

Les appareils volés et de contrefaçon

Vol et commerce d'appareils mobiles

Les atouts propres des appareils mobiles : compacité, portabilité et valeur marchande élevée, et comme support d'informations précieuses, en sont leur talon d'Achille, devenant la cible de prédilection des criminels. C'est ainsi qu'est apparu un marché noir international d'appareils mobiles volés. Dans de nombreux pays, les décideurs politiques s'inquiètent de plus en plus de l'incidence des vols d'appareils mobiles, ainsi que de l'implication du grand banditisme dans l'exportation et le négoce en gros d'appareils mobiles volés.

Dresser des obstacles au vol et au commerce d'appareils mobiles

La GSMA attribue des identifiants uniques, appelés IMEI (International Mobile Equipment Identifiers), aux fabricants d'appareils compatibles à 3GPP (3rd Generation Partnership Project)[23]. La base de données IMEI enregistre les plages allouées et les informations relatives aux modèles d'appareils pour lesquels elles ont été attribuées. Les informations enregistrées comprennent le nom du fabricant et du modèle de l'appareil et de ses principales capacités de réseau (par ex. bandes de fréquences, interfaces radio et types d'appareils).

En 1996, la GSMA a lancé une initiative consistant à bloquer les appareils mobiles volés au moyen d'une base de données partagée des identifiants uniques des appareils mobiles déclarés perdus ou volés par les consommateurs des opérateurs de réseau membres de la GSMA. Cette liste centralisée, surnommée la liste noire, est accessible à tous les membres de la GSMA qui ont une connexion à la base de données IMEI pour y partager des renseignements sur les appareils volés. Dès qu'un opérateur de réseau mobile détecte un appareil se connectant à son réseau qui figure sur la liste noire, il peut en bloquer l'utilisation. Quand les voleurs se rendront compte que les consommateurs sont peu susceptibles d'acheter des appareils volés s'ils risquent d'être désactivés peu de temps après, le vol d'appareils a toutes les chances de perdre de son attrait. C'est dans cette perspective que la GSMA encourage ses membres à déployer sur leurs réseaux un Registre d'Identification des Équipements (EIR en anglais) normalisé, pour bloquer la connexion d'appareils volés d'après leur identifiant IMEI. Le blocage IMEI, fondé sur la liste noire, a eu un impact positif dans de nombreux pays, mais pour qu'une campagne de lutte contre les vols ait véritablement des chances d'aboutir, d'autres mesures doivent être mises en place. Le vol et la vente d'appareils constituent un problème d'envergure internationale. Même si un IMEI est bloqué par tous les opérateurs de réseau mobile d'une région, l'appareil mobile peut toujours être utilisé dans une autre région où les opérateurs de réseau mobile ne sont pas connectés à la base de données IMEI de la GSMA.

La GSMA cherche à connecter le plus grand nombre d'opérateurs de réseau mobile que possible à la base de données IMEI. Fin 2016, la liste noire de la base de données de la GSMA comptait plus de 140 opérateurs de réseau mobile répartis dans plus d'une quarantaine de pays du monde entier, qui partagent des informations sur les appareils volés au jour le jour. En Amérique latine, où le problème du vol d'appareils est très répandu, 18 pays se sont joints à la base de données IMEI pour partager des données sur les vols et la plupart des opérateurs de réseau mobile de la région font de même. Pour habiliter plus encore les consommateurs et les revendeurs, un service public de contrôle d'appareil IMEI est disponible dans certains pays pour vérifier le statut des appareils en vente. Ce service a été déployé dans le cadre de la campagne menée par la GSMA baptisée « We Care »[24], qui fin 2016 avait déjà enregistré plus de 1,5 million de recherches.

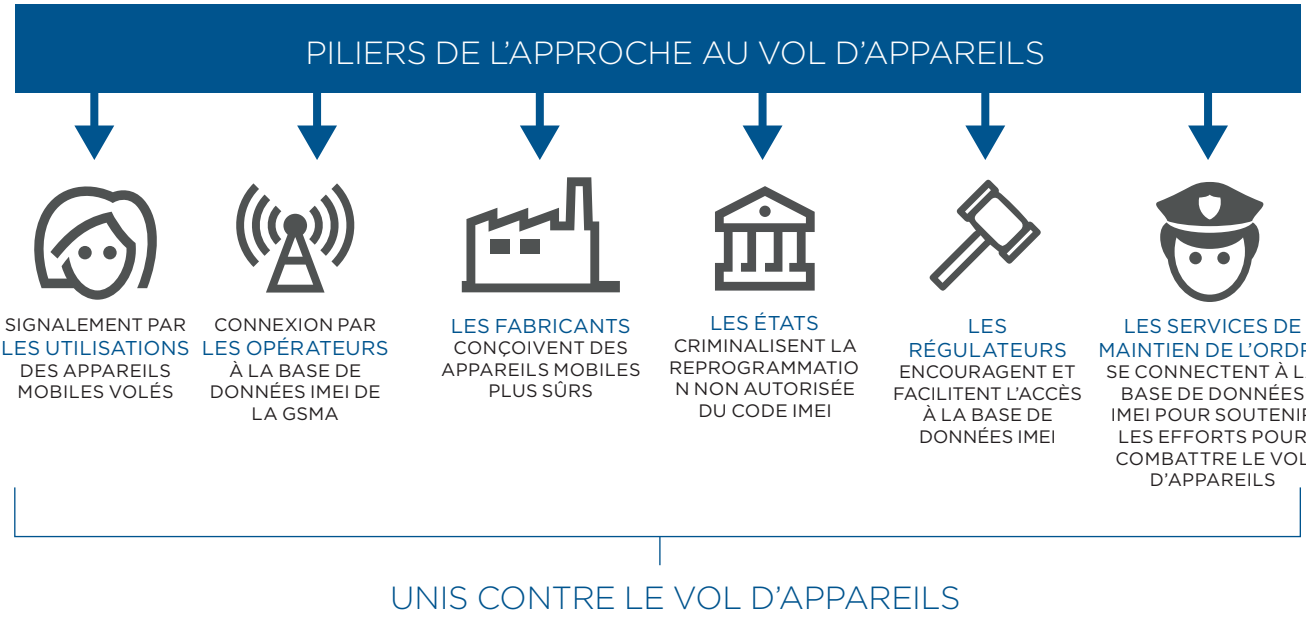
23. 3GPP réunit sept organisations de normalisation des télécommunications (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC). Les spécifications 3GPP sont publiées, gratuitement, jusqu'à quatre fois par an. Le terme « spécification 3GPP » couvre toutes les spécifications GSM (y compris GPRS et EDGE), W-CDMA (y compris HSPA) et LTE (y compris LTE-Advanced et Pro LTE-Advanced). Pour plus d'informations, voir : www.3gpp.org
24. Pour en savoir plus sur la campagne « We Care », voir : http://www.gsma.com/latinamerica/wecare

Le succès du blocage IMEI dépend de l'application sécurisée par les fabricants des identifiants IMEI sur tous les appareils mobiles. Les plus grands fabricants d'appareils mobiles au monde ont convenu de soutenir deux initiatives clés de la GSMA pour renforcer la sécurité IMEI, à savoir : (1) la définition des principes de conception technique pour l'application de la sécurité IMEI, et (2) la participation au processus de la GSMA de signalement et de correction des failles de la sécurité IMEI.[25] Certains fabricants d'appareils pourraient faire plus encore pour renforcer les niveaux de sécurité concernant l'intégrité IMEI, ce qui est essentiel pour assurer un blocage efficace des appareils. Les opérateurs de réseau mobile et d'autres grands fournisseurs et revendeurs d'appareils mobiles peuvent prendre des décisions d'achat éclairées quant au choix des appareils à vendre à leurs consommateurs : l'application de la sécurité IMEI sur ces appareils et leur respect des principes de conception technique peuvent potentiellement en devenir des considérations déterminantes. Il est important que toutes les parties prenantes, à savoir les fabricants, les opérateurs de réseau mobile et les consommateurs, travaillent ensemble pour assurer une complète intégrité IMEI et la résolution rapide des problèmes qui peuvent survenir. D'autre part, les États doivent reconnaître le rôle central que l'intégrité IMEI joue pour permettre le blocage d'appareils volés, en criminalisant toute modification non autorisée de l'identifiant IMEI d'appareils mobiles (qu'on appelle aussi reprogrammation ou falsification IMEI). Dans plusieurs pays, la modification de l'IMEI d'un appareil mobile après sa fabrication constitue une infraction pénale, et d'autres sont incités à faire de même en identifiant et poursuivant en justice les délinquants afin de décourager le contournement des contrôles de sécurité.

Le bouton de désactivation (le « kill switch ») constitue une autre forme de dissuasion pour lutter contre le vol d'appareils mobiles. Ce bouton est un moyen de désactiver les fonctions essentielles d'un appareil mobile. Il s'agit essentiellement d'une fonction au sein du système d'exploitation de l'appareil mobile, qui une fois déclenchée cesse de fonctionner comme prévu. Il ne peut être réactivé ou réutilisé que si le propriétaire légitime de l'appareil en autorise la réactivation. La GSMA a rédigé le document des Exigences de fonction d'un dispositif anti-vol à l'intention des fabricants d'appareils, des opérateurs de réseau mobile et des pouvoirs publics. Celui-ci définit un ensemble de fonctionnalités mises à la disposition d'un propriétaire d'appareil pour localiser, désactiver et réactiver son appareil si celui-ci est égaré, perdu ou volé.[26]

Figure 4

Piliers de l'approche au vol d'appareils



25. Pour en savoir plus sur le processus de signalement et de correction des failles de la sécurité IMEI, voir : http://www.gsma.com/publicpolicy/wp-content/uploads/2007/07/IMEI-Weakness-Reporting-and-Correction-Process-3.2.0.pdf
26. GSMA, 2016. « Exigences de fonctionnalité de lutte contre les vols, version 3.0 »

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

La GSMA cherche à aider les parties prenantes à restreindre la vente et l'utilisation d'appareils volés ou perdus. La GSMA et ses membres se tiennent à la disposition des pouvoirs publics et d'autres parties prenantes pour collaborer avec eux et leur offrir leur expertise et leurs ressources en vue d'élaborer des solutions pertinentes et axées sur le consommateur. C'est dans cette perspective que la GSMA formule les suggestions suivantes :

- Une approche de collaboration entre les principales parties prenantes est essentielle :[27]
  - L'utilisateur peut signaler à son opérateur de réseau que son appareil a été volé, en activer les fonctions anti-vol et, dans les pays où les opérateurs sont connectés à la base de données IMEI, il peut utiliser le code IMEI pour vérifier le statut de l'appareil qu'il envisage d'acheter
  - Les opérateurs de réseau mobile peuvent bloquer les appareils volés de leur réseau, se connecter à la base de données IMEI de la GSMA pour partager des données de la liste noire et encourager leurs fournisseurs d'appareils à protéger adéquatement l'intégrité des implémentations IMEI dans leurs produits
  - Les fabricants d'appareils peuvent concevoir des appareils plus sûrs (comme en rendant impossible la reprogrammation de l'IMEI) et déclencher le bouton de désactivation pour permettre aux utilisateurs de désactiver à distance leur appareil perdu ou volé
  - Les opérateurs de boutiques d'applications peuvent obtenir auprès de la GSMA le code IMEI d'appareils volés et s'en servir pour refuser l'accès par ces derniers à leur boutique d'applications
  - Les États peuvent adopter une loi visant à criminaliser la reprogrammation non autorisée de l'IMEI et soutenir les efforts déployés par le secteur et les services de sûreté de lutte contre le vol d'appareils
  - Les régulateurs peuvent encourager les réseaux locaux à se connecter à la base de données IMEI de la GSMA pour partager des données sur les appareils volés, fournir et/ou faciliter la fourniture de services de contrôle IMEI pour permettre aux utilisateurs de vérifier le statut de l'appareil qu'ils envisagent d'acheter, et plus généralement fournir un cadre réglementaire propice à des solutions efficaces et faciles d'utilisation par les consommateurs pour lutter contre le vol d'appareils
  - Les services de sûreté peuvent veiller à se doter des moyens de vérifier le statut des appareils en obtenant un accès gratuit aux données de la GSMA sur les appareils volés, et à concentrer leurs efforts et leurs ressources sur les vols d'appareils en s'assurant que les contrevenants sont identifiés et poursuivis en justice
- Il est important d'éviter des solutions qui peuvent être moins efficaces et/ou avoir même des conséquences préjudiciables inattendues :
  - La solution optimale pour empêcher l'utilisation d'appareils perdus ou volés au niveau d'un réseau consiste à utiliser des listes noires. L'utilisation de listes blanches à de telles fins est à éviter. Les listes blanches ont été conçues à d'autres fins, notamment pour contribuer à la lutte contre les dispositifs de contrefaçon, même si l'efficacité de cette approche n'a pas été prouvée
  - Il convient d'éviter le recours à des solutions non normalisées de lutte contre le vol des appareils mobiles, car celles-ci sont de nature exclusive et ont tendance à être techniquement difficiles et coûteuses à mettre en œuvre
  - Il s'agit d'éviter les approches contraires aux normes mobiles mondiales, comme le fait de lier des appareils spécifiques à des utilisateurs de mobile individuels : celles-ci ont tendance à être coûteuses, voire disproportionnées, et difficiles à respecter par les utilisateurs et les prestataires de services, tout en présentant le risque de soulever tout un nombre de problèmes juridiques complexes et de restriction de la concurrence
  - L'établissement de bases de données nationales d'identifiants d'appareils représente des efforts et des dépenses inutiles. La base de données existante de la GSMA est capable de répondre aux besoins de blocage d'appareils et de partage des données. En outre, il est préférable de tenir à jour un seul registre mondial des données sur les appareils, car il est garant de cohérence, de partage des données de plus large envergure, tout en évitant le risque de fragmentation qui finirait par nuire à l'efficacité de ces approches

27. GSMA, 2016. « The Mobile Economy: Latin America and the Caribbean 2016 »

Étude de cas

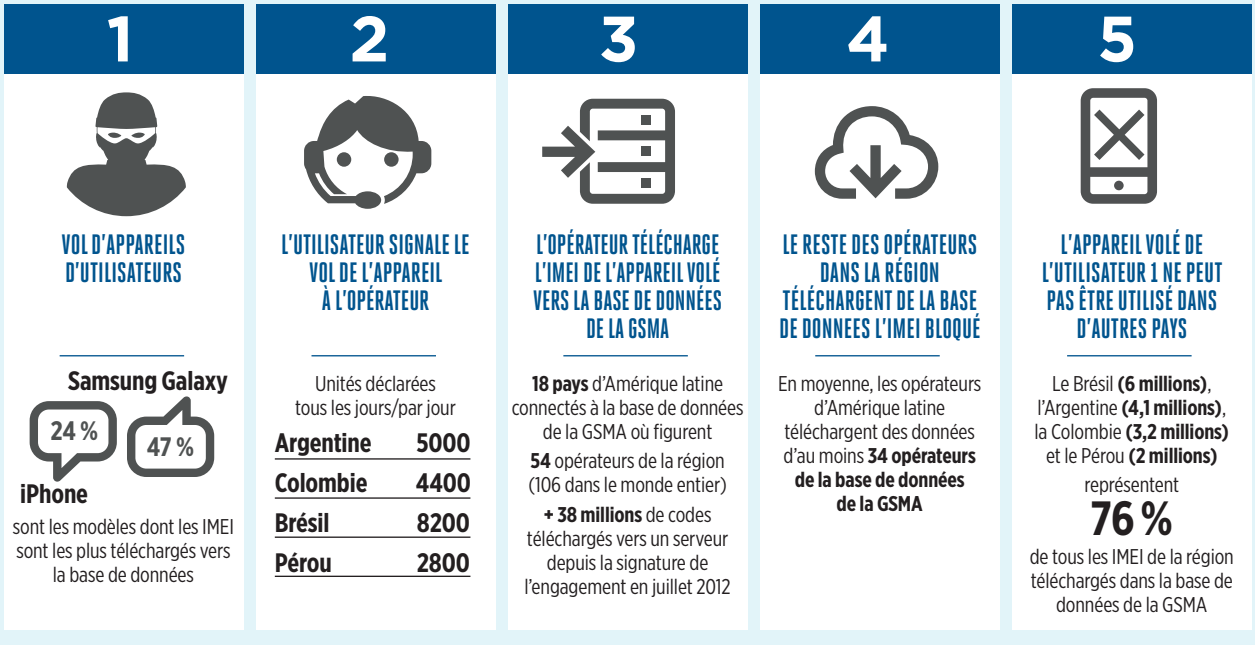
Contribution de l'industrie dans la lutte contre le vol d'appareils en Amérique latine

Le vol d'appareils est en forte hausse depuis quelques années en raison de l'adoption généralisée du téléphone mobile, du smartphone en particulier. Les délits liés au vol d'appareils augmentent à une allure très rapide en Amérique latine. Ainsi au Pérou, dans les trois premiers mois de 2014, 1,2 million de téléphones mobiles ont été déclarés volés. Cela représentait une augmentation de 34 % par rapport à la même période en 2013. Alors que tous les délits sont loin d'être signalés, la base de données IMEI a relevé le vol de 14 millions de téléphones mobiles enregistrés en 2014 rien que dans les pays andins de l'Équateur, de la Colombie, du Pérou et de la Bolivie.

Il est fréquent de faire franchir les frontières aux téléphones mobiles volés pour exploiter les possibilités d'arbitrage de prix et/ou contourner des initiatives propres à chaque pays de bloquer les appareils grâce à leur IMEI. Par conséquent, pour lutter réellement contre ce problème, il est essentiel d'assurer le partage des informations non seulement entre les opérateurs du même pays mais aussi avec ceux sur le plan régional et mondial.

En 2011, la Commission interaméricaine des télécommunications (CITEL) a approuvé une résolution qui, entre autres, recommandait : « La régulation au niveau régional de l'échange de bases de données d'appareils figurant sur la liste noire et le blocage de leurs identifiants uniques (IMEI) pour empêcher l'activation et l'utilisation de téléphones portables volés dans d'autres marchés et aider à contrôler le trafic illégal d'appareils entre les pays de la région ». En 2012, 13 opérateurs de réseau mobile latino-américains, membres de la GSMA, se sont engagés à travailler ensemble et à collaborer avec les instances régionales de la région entière en vue de bloquer l'utilisation d'appareils volés. Cette initiative volontaire prévoit le partage d'informations sur les appareils mobiles volés afin de les bloquer et de rendre plus difficiles leur trafic et leur réutilisation dans l'ensemble de la région.

La GSMA continue de promouvoir l'adoption de ces lignes directrices par l'ensemble des opérateurs qui en sont membres en Amérique latine par la ratification de protocoles d'entente entre les opérateurs sur une base pays par pays, mais dans l'objectif d'assurer le partage complet des données dans la région entière.



Vente et utilisation d'appareils de contrefaçon

Un appareil mobile de contrefaçon viole explicitement la marque ou la conception d'un produit original ou authentique « de marque », même en présence de légères variations par rapport à la marque établie. Du fait de leur caractère illicite, ces appareils mobiles sont généralement expédiés et vendus sur le marché noir partout dans le monde par des réseaux de grand banditisme. C'est ce qui explique le peu de prise de conscience parmi les consommateurs et les pouvoirs publics de la véritable envergure et de l'impact du commerce d'appareils mobiles de contrefaçon. On estime que 143 millions d'appareils mobiles illicites ont été vendus en 2013 au niveau mondial.[28]

Alors que la production et la distribution de produits de contrefaçon présentent un grave problème de violation de propriété intellectuelle et de règles commerciales légitimes, avec le manque à gagner qui en résulte tant en termes de chiffre d'affaires des fabricants que de recettes fiscales pour les États, les appareils de contrefaçon ont également un impact sur les consommateurs. Dans de nombreux pays, les appareils de contrefaçon sont à ce point répandus que les consommateurs ne s'en rendent pas compte et les achètent à leur insu. Indépendamment de la qualité médiocre du service souvent associée à la performance et l'utilisation d'appareils de contrefaçon, il a été signalé que beaucoup d'entre eux contiennent des matières dangereuses qui constituent une menace pour l'environnement. Plusieurs études ont démontré la présence de substances dangereuses, telles que du plomb dans les joints de soudure, dans certains appareils mobiles contrefaits à des niveaux qui dépassent les limites jugées acceptables dans le monde.[29] Ces limites sont définies dans les règlements que les fabricants légitimes d'appareils mobiles sont tenus de respecter. Les appareils mobiles de contrefaçon qui contiennent des matériaux dangereux constituent une menace pour l'environnement s'ils ne sont pas éliminés en adoptant des procédures respectueuses de l'environnement.

Les appareils mobiles de contrefaçon ne sont pas faciles à identifier et à bloquer du fait que beaucoup sont dotés d'un IMEI d'apparence légitime. Les contrefacteurs ont désormais l'habitude de s'emparer des plages de numéros IMEI allouées à des fabricants d'appareils légitimes pour les utiliser dans leurs produits, ce qui rend la distinction entre les produits légitimes et ceux qui sont contrefaits plus difficile à faire.

28. The Mobile Manufacturers Forum (MMF), 2014. "Counterfeit/Substandard Mobile Phones: A Resource Guide for Governments"
29. Ibid.

Restriction de la vente et de l'utilisation d'appareils de contrefaçon

Pour aider à résoudre ce problème, il est possible d'utiliser les données qui figurent sur la liste blanche (le registre des plages de numéros d'identification alloués à tous les fabricants légitimes d'appareils) de la base de données IMEI de la GSMA pour détecter les appareils aux identifiants IMEI non valides ou inexistants, et au besoin leur refuser l'accès au réseau. Cependant, dans le cas d'IMEI qui appartiennent à des appareils légitimes mais qui ont été utilisés par des contrefacteurs dans leurs produits, il est difficile de différencier et d'isoler les appareils légitimes des contrefaçons. Par ailleurs, il n'est possible de bloquer un appareil de contrefaçon qu'après que le consommateur l'a acheté, souvent à son insu, et tente de le connecter à un réseau mobile. Les perturbations provoquées par le blocage d'appareils qui ont déjà été vendus ont souvent pour effet de punir des parties innocentes, et non pas celles qui font le commerce de produits contrefaits. Les mesures prises doivent veiller à ne pas gêner les utilisateurs innocents et à ne pas perturber le marché légitime, pendant que ceux qui participent à des activités de contrefaçon et de commerce illicite continuent de profiter. Plus précisément, les autorités compétentes devraient concentrer leurs efforts sur la fabrication et la distribution d'appareils de contrefaçon pour les ôter de la circulation avant qu'ils finissent entre les mains de consommateurs qui ne se doutent de rien.

La GSMA et l'Organisation mondiale des douanes (OMD) ont conclu un partenariat en septembre 2016 pour collaborer dans la lutte contre la contrefaçon et le commerce frauduleux d'appareils mobiles. L'intégration de la base de données IMEI permettra le recoupement et le filtrage des appareils de contrefaçon identifiés par leur IMEI au point d'importation. Il n'est toutefois pas possible d'appliquer cette solution aux appareils mobiles qui font l'objet de trafic et sont importés en dehors du processus douanier comme produits de contrebande : pour cela, les services douaniers et les services de sûreté doivent renforcer leurs efforts de lutte contre le trafic illicite.

En raison de la complexité de cette question, les services de sûreté n'ont pas déployé suffisamment d'efforts dans la lutte contre la distribution et la vente d'appareils de contrefaçon pour endiguer le problème. Les dispositions législatives et réglementaires nationales actuelles n'ont qu'un effet limité en raison de l'envergure internationale de la distribution des appareils de contrefaçon qui n'ont pas de mal à échapper aux mesures de répression prises individuellement par les pays. Par ailleurs, l'établissement de listes blanches nationales d'appareils relève d'une approche non prouvée : aucune preuve n'existe quant à leur efficacité dans la lutte contre la vente et l'utilisation d'appareils de contrefaçon. Une telle approche peut avoir pour effet d'entraver la libre circulation des appareils mobiles dans le monde et être considérée illégale dans certains pays. Au lieu de cela, il est préférable d'élaborer des solutions mondiales et multipartites, comme le décrit la section suivante.

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

La GSMA reconnaît les problèmes que posent les appareils de contrefaçon tant pour les utilisateurs que pour les réseaux, les fabricants légitimes et les pouvoirs publics, et elle soutient la nécessité de maintenir l'intégrité du marché des appareils mobiles. La GSMA est désireuse de travailler avec ses membres, les États et d'autres parties prenantes à l'élaboration de solutions qui peuvent être efficaces dans la lutte contre la production et la distribution d'appareils de contrefaçon.

- Pour cela, la collaboration entre un éventail de parties prenantes est essentielle :
  - Les régulateurs peuvent travailler avec les fabricants d'appareils et les opérateurs de réseau à l'échelle nationale pour déterminer l'ampleur de l'utilisation d'appareils de contrefaçon sur le marché local. Il est important qu'ils travaillent avec les parties prenantes concernées pour élaborer et convenir des mesures à prendre qui ne pénalisent ni les fabricants d'appareils légitimes ni les utilisateurs innocents exploités par les contrefacteurs
  - Pour entraver le marché noir d'appareils, les pouvoirs publics peuvent décider d'abaisser les tarifs et les droits perçus sur les appareils légitimes importés, en diminuant ainsi le coût de possession des appareils légitimes. Ils peuvent aussi soutenir des programmes de sensibilisation et d'éducation des consommateurs pour mettre en évidence les risques posés par l'achat d'appareils de contrefaçon
  - Les services douaniers peuvent se doter des moyens nécessaires pour vérifier la légitimité des identifiants des appareils à leur point d'importation en obtenant l'accès gratuit à la base de données IMEI de la GSMA. Ils peuvent ainsi renforcer leurs efforts à identifier les délinquants et les poursuivre
  - Les fabricants d'appareils peuvent travailler avec les pouvoirs publics, les régulateurs et les services douaniers pour sensibiliser les parties prenantes aux appareils de contrefaçon et relayer des renseignements aux autorités compétentes sur les activités liées à la production, à la distribution et à la vente d'appareils de contrefaçon
  - Les opérateurs de réseau mobile peuvent se connecter à la base de données IMEI de la GSMA pour obtenir la liste définitive des identifiants d'appareils légitimes et si nécessaire ils peuvent refuser l'accès aux appareils désignés de contrefaçon
  - Les utilisateurs peuvent vérifier la légitimité des appareils qu'ils envisagent d'acheter en se reportant aux services de vérification fournis par d'autres parties prenantes, le cas échéant
- Il est important d'éviter des solutions qui peuvent être moins efficaces et/ou avoir même des conséquences préjudiciables inattendues :
  - Il convient d'éviter le recours à des solutions non normalisées de lutte contre le vol d'appareils mobiles de contrefaçon, car celles-ci sont de nature exclusive et ont tendance à être techniquement difficiles et coûteuses à mettre en œuvre.
  - Il s'agit d'éviter les approches contraires aux normes mobiles mondiales, comme le fait de lier des appareils spécifiques à des utilisateurs individuels. Celles-ci ont tendance en effet à être coûteuses, voire disproportionnées, et difficiles à respecter par les utilisateurs et les prestataires de services, tout en présentant le risque de soulever tout un nombre de problèmes juridiques complexes et de restriction de la concurrence

La fraude sur les appareils mobiles

Les manœuvres frauduleuses peuvent se présenter sous une multitude de formes et certaines se servent des appareils mobiles à leurs propres fins. On compte parmi elles des attaques telles que la fraude de service (par ex. l'usurpation d'identité ou la fraude d'argent mobile), le spam mobile[30] et, de plus en plus, la fraude par « ingénierie sociale » (par ex. les pratiques de Phishing, SMiShing ou Vishing),[31] qui incitent par la ruse les victimes à révéler des informations sensibles les concernant et les services qu'elles consomment, sans se rendre compte qu'elles mettent leur propre sécurité en danger

La fraude par ingénierie sociale se sert de moyens de manipulation pour pousser quelqu'un à prendre des mesures qui lui sont préjudiciables, comme révéler ses détails personnels ou ses mots de passe. Une fois qu'ils ont accès à ces détails personnels, les criminels peuvent enregistrer ces informations et les utiliser pour commettre d'autres délits, par exemple d'usurpation d'identité et de fraude bancaire. Il est fréquent que les fraudeurs qui se mettent en contact avec leurs victimes cibles nouent des liens avec elles et gagnent leur confiance, souvent en s'aidant d'informations accessibles au public.

La fraude par ingénierie sociale est en plein essor et INTERPOL, l'agence internationale de police, y voit là l'une des nouvelles tendances de fraude dans le monde. Ainsi au Royaume-Uni, le bureau national de lutte contre la fraude a fait part d'une augmentation des incidents de 21 % au cours des 12 mois entre octobre 2014 et octobre à 2015.

Prendre la mesure de la fraude et la minimiser

Les fraudeurs arrivent à leurs fins lorsqu'ils parviennent à convaincre leur victime de leur légitimité, que ce soit en personne ou par le biais d'un service ou d'un site web.

Les solutions technologiques offrent un certain degré de défense : par exemple, les opérateurs de réseau mobile ont adopté les techniques recommandées par la GSMA pour détecter la transmission internationale de spams mobiles frauduleux et y remédier.

Quoique peu fréquemment, les systèmes de messagerie vocale ont été ciblés par le passé comme moyen de compromettre la sécurité des utilisateurs mobiles en permettant à des parties non autorisées d'écouter des messages vocaux ou de passer des appels frauduleux. Les systèmes de messagerie vocale peuvent servir d'outil de fraude et la GSMA a fourni des conseils aux opérateurs et aux consommateurs pour veiller au déploiement robuste de l'authentification des consommateurs afin de protéger les comptes de messagerie vocale des utilisateurs en veillant à ce que seuls les consommateurs légitimes aient accès aux services de messagerie vocale en trouvant le juste équilibre entre la facilité d'utilisation et la sécurité.

Néanmoins, le comportement humain est également au cœur de la question de la fraude mobile, et par conséquent l'un des principaux vecteurs de minimisation des risques passe par l'éducation à la protection des données personnelles et par la sensibilisation aux menaces potentielles. Les opérateurs de réseau mobile sont bien placés pour aider à éduquer les consommateurs sur la nécessité de faire preuve de méfiance et de vigilance. Toutefois il revient aux prestataires de services ultimes de renforcer cette démarche par des messages plus spécifiques : par exemple, les banques et les revendeurs sont les mieux placés pour fournir et appliquer les mesures de sécurité technique qui correspondent précisément à leur service.

Terminologie

Fraude par ingénierie sociale : exemples

- **Phishing :** méthode utilisée pour infecter des ordinateurs ou des appareils mobiles afin d'accéder à des détails personnels de valeur. Les fraudeurs de « Phishing » utilisent généralement les e-mails comme moyen de communication, pour inciter les gens à se connecter à des sites ou services d'apparence authentique afin de leur soutirer leurs détails personnels.
- **SMiShing :** ou « SMS phishing », cette méthode utilise des messages texte SMS pour servir d'« appât » qui induit ensuite les victimes à divulguer leurs renseignements personnels.
- **Vishing :** méthode par laquelle les fraudeurs persuadent leurs victimes de leur communiquer des détails personnels ou de leur virer de l'argent, par téléphone, en se faisant passer pour un service légitime, une banque par exemple

30. Le terme « spam mobile » se réfère à des messages mobiles en masse non sollicités. La plupart des spams sont destinés à frauder ou à arnaquer la victime et reposent sur l'existence d'un modèle de facturation (par ex. barrière faible à l'expéditeur si le destinataire est la partie facturée)
31. Voir l'encadré sur l'ingénierie sociale

Pour aider les opérateurs de réseau mobile à cet égard, la GSMA recommande trois principes directeurs[32] à observer lors de l'élaboration de messages adressés aux consommateurs sur cette question :

1. Le message doit être pertinent et spécifique
2. Le message doit être simple et facile à comprendre
3. Le message doit être renforcé lors des échanges avec le client

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

La fraude sous toutes ses formes relève d'une question complexe et elle est presque toujours illégale dans la plupart des pays. Les opérateurs de réseau mobile ont beau se mobiliser, seule la prévention leur permettra d'influer sur le comportement des consommateurs dans le but d'atténuer le risque de fraude. Il revient aux dispositions législatives et réglementaires de se concentrer sur les fraudeurs. Quant aux consommateurs, le principal moyen de développer leur aptitude à se protéger passe forcément par une démarche d'éducation et de sensibilisation. Sur les marchés ayant un faible niveau de compréhension technologique, il est fréquent que les consommateurs n'usent pas du plein potentiel des fonctions technologiques mises à leur disposition pour se protéger.

- Il est important que les prestataires de services finaux, (par ex. les banques dans le cas des services monétaires) mettent en œuvre les plus hauts niveaux possible de sécurité, qui sont appropriés à leur marché
- Il convient d'employer et de promouvoir des contrôles préventifs, comme des campagnes de sensibilisation des consommateurs, pour renforcer leur éducation et accroître leur protection tout en minimisant le risque de devenir victimes de fraude
- Il revient aux opérateurs de réseau mobile d'élaborer des stratégies robustes de gestion des risques afin d'atténuer les risques de fraude. Le type de mesures prises et le niveau de mise en œuvre seront déterminés par chaque opérateur en fonction de l'évaluation des menaces et doivent être spécifiques aux services qu'ils offrent et aux consommateurs sur leur marché

Étude de cas

Gestion des risques de l'argent mobile : communication avec le consommateur

M-PESA de Safaricom est un exemple de la communication comme outil pour aider à prévenir la fraude liée à l'argent mobile. L'une des priorités essentielles pour le service M-PESA de Safaricom est d'atténuer les risques que des escroqueries soient perpétrées contre les consommateurs. En plus de mesures réactives, et plutôt que de tenter d'utiliser uniquement des contrôles de détection (c.-à-d., la surveillance et le signalement des tendances a posteriori), Safaricom s'en remet lourdement à un contrôle préventif pour réduire les risques d'escroqueries contre les consommateurs. Safaricom a constaté que le contrôle préventif le plus efficace consiste à sensibiliser le client par des messages clairs. Pour atteindre les consommateurs de M-PESA, Safaricom a adopté une approche à plusieurs volets. Des SMS répétés, des annonces à la radio en dialecte local et des annonces dans les journaux sont autant de moyens utilisés dans ses campagnes de sensibilisation auprès des consommateurs. Safaricom doit essentiellement son succès à gérer la fraude contre les consommateurs de M-PESA aux messages clairs de sa campagne de sensibilisation des consommateurs.

La communication auprès des consommateurs est un outil à utiliser dans le cadre d'une stratégie plus large de gestion des risques et elle doit s'accompagner de données et de tableaux de bord pertinents et de procédures internes clairement définies. La GSMA met ainsi à la disposition des opérateurs son cadre complet accompagné d'une boîte à outils consacrés à la gestion des risques de l'argent mobile.

32. L. Gilman, 2012. « Mitigating the risk of fraud through consumer communication », GSMA

4 Protection de la vie privée du consommateur

Ces dix dernières années, nous avons observé un extraordinaire enrichissement des services de communication. Par leur nature même, les sociétés basées sur les services Internet, ont accès à des quantités d'informations considérables sur les utilisateurs, en commençant par leur identité, avec qui ils communiquent, où ils se trouvent, jusqu'à connaître leurs intérêts personnels en se reportant aux sites et aux services qu'ils consultent. Les prestataires peuvent analyser le contenu des communications, comme les mots tapés dans les moteurs de recherche ou les emplacements saisis dans les applications de cartographie, et combiner cet ensemble de données pour se faire une idée des intérêts et de l'intention d'un utilisateur donné.

Pour fournir leurs services de communications, les opérateurs de réseau mobile utilisent un ensemble limité de données à caractère personnel. Ce sont surtout les sociétés tierces de l'écosystème Internet qui utilisent le plus les informations à caractère personnel.[33] Bien que les utilisateurs ne s'en rendent pas toujours compte, bon nombre de ces services en ligne sont offerts gratuitement en échange de l'utilisation par le fournisseur de leurs données personnelles pour vendre de la publicité ou pour commercialiser des services payants à l'utilisateur. La présente section traite le type de données qui sont collectées auprès des utilisateurs dans l'écosystème Internet, leur lieu de stockage, leur utilisation, qui y a accès ainsi que les implications qui en découlent en matière de respect de la vie privée.

Les problématiques qui sont traitées sont les suivantes :

- La collecte et l'utilisation de données, en mettant l'accent sur le soutien à l'innovation
- Le choix du consommateur, en mettant l'accent sur l'intégration de ce choix dans les applications et les services en ligne
- Les flux transfrontaliers de données et la nécessité de tenir compte des questions de sécurité nationale

Chacun de ces enjeux constitue une implication importante pour les pouvoirs publics, pour l'industrie ainsi que pour les autres parties prenantes. Ils sont également traités avec plus de détail plus loin dans ce chapitre.

Protection de la vie privée du consommateur

La protection de la vie privée vise essentiellement à renforcer la confiance en la protection adéquate des données à caractère privé, en conformité avec la réglementation et les exigences en matière de respect de la vie privée. Pour cela, toutes les parties concernées doivent adopter une approche cohérente, neutre sur le plan technologique, et constante entre l'ensemble des services, des secteurs et des territoires. Les pouvoirs publics peuvent y contribuer en accordant la souplesse nécessaire à l'innovation, en adoptant des cadres basés sur les risques de sauvegarde des données à caractère privé, et enfin en encourageant des pratiques responsables en matière de gouvernance numérique en accord avec la réglementation locale. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures proactives afin de protéger et de respecter la vie privée des consommateurs et de leur permettre de faire des choix éclairés sur le type de données recueillies et la manière dont leurs données à caractère personnel sont utilisées, en mettant en œuvre des politiques qui encouragent :

- **Le stockage et le traitement en toute sécurité des informations à caractère personnel et privé, en conformité avec les exigences légales le cas échéant**
- **Être transparent avec les consommateurs sur les données que nous partageons sous forme anonyme et en pleine conformité avec les exigences légales**
- **La mise à disposition aux consommateurs des informations et des outils nécessaires pour faire des choix simples et significatifs au sujet de leur vie privée**

33. Pour une discussion plus détaillée sur ces services, se reporter au document de la GSMA publié en 2016 par A.T.Kearney, intitulé « The Internet Value Chain: A study on the economics of the internet", pg. 11

Collecte et utilisation des données

La GSMA prévoit que le nombre de smartphones va passer de 2,6 milliards d'unités fin 2015 à 5,8 milliards à l'horizon 2020. Parallèlement, il est prévu que le TCAM du trafic de données augmente de 49 % au cours de la même période.[34] Cette prolifération des appareils et des données permet aux particuliers, aux entreprises et aux États d'innover de manières aussi inédites qu'inattendues.[35]

Toutefois, les recherches montrent que, malgré l'augmentation constante de leur utilisation de ces services, les consommateurs se révèlent aussi de plus en plus inquiets du respect de leur vie privée et ils cherchent à se faire rassurer qu'ils peuvent faire confiance aux entreprises auxquelles ils confient leurs données. Une étude de la GSMA a constaté que huit utilisateurs de mobile sur dix se disent inquiets de communiquer leurs informations personnelles quand ils utilisent Internet sur leur mobile ; il en résulte aussi que près de la moitié des utilisateurs soucieux du respect de leur vie privée seraient disposés à limiter leur utilisation de ces applications s'ils ont des doutes sur la protection de leurs informations personnelles.[36]

Lorsqu'il s'agit d'envisager les questions portant sur la collecte et l'utilisation de données à caractère personnel, il est important de noter les deux distinctions suivantes :

- Les lois sur le respect de la vie privée, là où elles existent, varient d'un pays à l'autre : il n'existe pas de cadre universel. Il est fréquent que les organisations régies par ces lois ont une implantation internationale. Tout cela crée des incertitudes quant à la base juridique appropriée à adopter et soulève la question de savoir les lois de quel pays il convient d'appliquer en matière d'utilisation des données : celui de l'utilisateur ou celui du prestataire de service. La situation peut être encore plus compliquée si le prestataire de service stocke et traite les données dans un pays tiers
- Une deuxième distinction se situe entre l'opérateur de réseau mobile et les services et les applications en ligne fournies par un tiers auxquels les utilisateurs peuvent accéder via le réseau. La plupart des opérateurs de réseau mobile sont soumis à des lois et des obligations de licence en ce qui concerne la protection de la vie privée qui ne s'appliquent pas à d'autres services en ligne dans l'écosystème d'Internet.

En raison de l'actuel décalage qui existe entre les lois relatives au respect de la vie privée sur le plan national et/ou du secteur du marché, combiné aux flux de données internationaux, il est pratiquement impossible que l'ensemble des parties répondent de manière cohérente aux attentes de respect de la vie privée des consommateurs. Cette disparité dans l'applicabilité des règles risque d'être exacerbée à mesure que davantage d'appareils et de capteurs vont devenir interconnectés par le biais de « l'Internet des objets » (IoT)[37], compte tenu de la dimension souvent internationale des services IoT qui regroupent une multitude de types de prestataires de services issus de différents secteurs.

4

Terminologie

Données à caractère personnel

Données à caractère personnel : ce terme peut signifier beaucoup de choses pour beaucoup de gens dans le monde en ligne et s'accompagne de diverses significations définies en droit. Le présent document ne vise pas à réinterpréter la loi. Néanmoins, quand nous utilisons le terme « données à caractère personnel », nous entendons par là (notamment mais pas uniquement) les informations relatives à une personne vivante et qui :

- **sont recueillies directement auprès de l'utilisateur (par ex., des informations saisies par l'utilisateur sur l'interface d'une application, comme son nom, son adresse et les détails de sa carte bancaire)**
- **sont recueillies indirectement (par exemple, numéro de téléphone mobile, adresse e-mail, nom, sexe, données de naissance, données de localisation, adresse IP, IMEI, identifiant unique du téléphone)**
- **concernent le comportement de l'utilisateur (par ex. données de localisation, données sur l'utilisation de service ou de produit, consultations de sites)**
- **sont générées par un utilisateur et sont conservées sur l'appareil de l'utilisateur (par ex., journaux d'appels, messages, images générées par l'utilisateur, listes de contacts ou carnets d'adresses, notes et informations d'identification de sécurité)**

Utilisateur : Toute référence à l'utilisateur porte généralement sur l'utilisateur final de l'appareil qui initie l'utilisation d'une application ou d'un service, et qui peut être ou ne pas être le « client » d'une application ou d'un prestataire de service.

34. GSMA, 2016. « The Mobile Economy: 2016 »
35. Ibid.
36. GSMA, 2014. Le document intitulé « Protection de la vie privée sur mobile : Connaissances approfondies issues des études sur les consommateurs et considérations pour les décideurs »
37. L'Internet des objets est abordé dans plus de détails au chapitre intitulé « Protection de la sécurité des réseaux et de l'intégrité des appareils ».

Ces disparités quant aux exigences de respect de la vie privée entre différents services et différentes applications peuvent conduire à une expérience où les utilisateurs se trouvent à accorder à leur insu un accès facile à leurs données à caractère personnel, s'exposant ainsi à des situations inattendues ou indésirables. D'autre part, il existe des services et des applications en ligne qui sollicitent le « consentement » des consommateurs à des conditions générales relatives au respect de la vie privée sans que ceux-ci ne lisent l'avis concerné ni ne comprennent les implications de leur décision. Une étude commandée par la GSMA montre que 82 % des utilisateurs donnent leur accord à des avis de respect de la vie privée sans en prendre connaissance, car elles ont tendance à être trop longues ou de nature trop juridique.[38] En raison de la distinction souvent mal comprise entre les opérateurs de réseau mobile et les autres services auxquels les utilisateurs ont accès sur leur appareil mobile, il existe aussi le risque que les consommateurs ne sachent pas qui traite leurs données, et en viennent parfois à croire que leur vie privée est mieux respectée qu'elle ne l'est dans la réalité.

Pour approfondir

Big Data

Grâce aux augmentations de la puissance de calcul, à la baisse des coûts et aux avancées réalisées dans le domaine analytique, en matière de Machine Learning et dans des disciplines connexes, il est possible de traiter et d'analyser d'énormes volumes de données. Plutôt que de devoir identifier des connexions causales, de simples corrélations de données permettent de tirer de précieux enseignements. On parle souvent dans ce cas-là de techniques analytiques des Big Data. Ces fonctionnalités représentent un changement radical dans la capacité de la société non seulement à créer de nouveaux produits et services, mais aussi à résoudre certains des besoins les plus pressants de notre temps en matière de politiques publiques : qu'il s'agisse de gestion routière en milieu urbain encombré ou de comprendre et de prévenir la propagation des maladies.

De plus en plus, les opérateurs de réseau mobile vont avoir recours aux données qu'ils recueillent et vont accéder à des données contextuelles provenant d'autres sources pour les services des big data. Ils ont donc un rôle important à jouer comme responsables de ces données et potentiellement comme facilitateurs dans un marché futur de l'accès à ce type de données.

À titre d'exemple, pour aider à lutter contre l'épidémie d'Ebola, Orange Telecom (Afrique de l'Ouest) a travaillé avec la Harvard School of Public Health (HSPH) et Flowminder pour prédire la propagation de la maladie à l'aide de données de téléphones mobiles. Les données obtenues de téléphones cellulaires en Côte d'Ivoire (en 2011) et au Sénégal (en 2013) ont été anonymisées et agrégées par Orange Telecom, qui en a ensuite autorisé la remise à Flowminder. Elles ont ainsi servi à élaborer un modèle qui offrait un aperçu des mouvements de population dans la région, qui est venu éclairer les recommandations sur les endroits où concentrer les efforts de soins de santé (MIT Review, 2014. « Cell-Phone Data Might Help Predict Ebola's Spread »).

À côté de cela, Telenor Group, Telenor Pakistan et HSPH ont engagé la toute première initiative à l'échelle nationale au Pakistan visant à comprendre et à modéliser la propagation de la fièvre dengue, en utilisant des données anonymisées sur la mobilité. Il s'agissait là non seulement du plus grand projet de son genre à avoir jamais été réalisé, en termes du nombre d'abonnés analysés, mais il constitue aussi la première tentative d'analyser des épidémies de la fièvre dengue au moyen d'analyses CDR (enregistrement détaillé des appels). L'objectif recherché était de concevoir des stratégies de prévention ancrées dans des méthodes guidées par les données, où Telenor s'appuie sur les compétences fondamentales qui existent en interne en matière d'analyses et d'ensembles de données exclusifs pour créer de la valeur partagée, tant pour Telenor que pour la société. Cette étude a attesté d'une méthode soucieuse du respect de la vie privée en termes d'utilisation des données sur les consommateurs collectées par les opérateurs mobiles pour résoudre des problèmes sociétaux et y venir à l'appui. Cette approche dresse des cartes des risques de la fièvre dengue qui peuvent s'avérer des outils utiles pour les agents de santé et les pouvoirs publics au Pakistan, en leur apportant des éléments précieux pour concevoir de meilleures stratégies de prévention. (Telenor, 2017).

Le secteur mobile est bien déterminé à concrétiser les avantages économiques et sociétaux que l'analyse des Big Data peut apporter en adoptant de bonnes pratiques de responsabilité numérique pour donner les moyens à la société de débloquer le potentiel énorme de l'analyse des Big Data tout en adhérant aux principes établis de respect de la vie privée et en favorisant un climat de confiance.

En collaboration avec des représentants de l'écosystème mobile, la GSMA travaille aussi sur les aspects de la vie privée de l'analyse des Big Data, qui reposent sur les Principes de Protection de la vie privée sur mobile de la GSMA.

38. GSMA, 2014. Le document intitulé « Protection de la vie privée sur mobile : Connaissances approfondies issues des études sur les consommateurs et considérations pour les décideurs »

Respect de la vie privée des consommateurs lors de la collecte et de l'utilisation des données

La GSMA a élaboré un ensemble de principes de Protection de la vie privée sur mobile, qui décrivent la manière de respecter et de protéger la vie privée des consommateurs mobiles lors de leur utilisation d'applications et de services mobiles qui accèdent à leurs données à caractère personnel, les utilisent ou les collectent. Ces principes ne remplacent pas les lois en vigueur, mais ils reposent sur des principes reconnus et acceptés au niveau international en matière de respect de la vie privée et de protection des données.[39] Ils cherchent à trouver le juste équilibre entre la nécessité de protéger la vie privée d'un individu et de le traiter de manière équitable, tout en permettant aux organisations d'atteindre leurs objectifs sur le plan commercial, en matière de politique publique et sur le plan sociétal. De manière générale, ils sont suffisamment souples pour tenir compte des nouvelles technologies et des nouveaux modes commerciaux à mesure qu'ils apparaissent. Sur les neuf principes retenus, six sont particulièrement pertinents pour la collecte et l'utilisation des données à caractère personnel :

- Ouverture, transparence et notification
- Sécurité
- Finalité et utilisation
- Enfants et adolescents
- Minimisation des données et conservation
- Responsabilisation et application

Figure 5

Principes de Protection de la vie privée sur mobile de la GSMA[40]

OUVERTURE, TRANSPARENCE ET NOTIFICATION

Les personnes responsables doivent être ouvertes et honnêtes avec l'utilisateur et veiller à lui communiquer des informations claires, mises en évidence et en temps utile concernant leurs pratiques liées à l'identité et la confidentialité des données. Il convient d'informer l'utilisateur quant aux personnes qui recueillent des informations personnelles le concernant, de la finalité d'une application ou d'un service, ainsi que de l'accès, de la collecte, du partage et de toute autre utilisation de ses informations personnelles, y compris à qui celles-ci peuvent être divulguées, pour qu'il puisse prendre des décisions éclairées sur son choix d'utiliser ou non une application ou un service mobile.

SÉCURITÉ

Les informations personnelles doivent être protégées, en utilisant des protections raisonnables appropriées au degré de confidentialité des informations.

RESPONSABILISATION ET APPLICATION

Toutes les personnes responsables sont tenues de s'assurer que ces principes sont respectés

OBJECTIFS ET UTILISATION

L'accès, la collecte, le partage, la communication et toute autre utilisation des informations personnelles des utilisateurs doivent se limiter à des fins commerciales légitimes, comme la fourniture des applications ou services demandés par les utilisateurs, ou pour répondre autrement aux obligations légales.

LES ENFANTS ET LES ADOLESCENTS

Une application ou un service qui s'adresse à des enfants et adolescents doit garantir que la collecte, l'accès et l'utilisation des informations personnelles sont adéquats en toutes circonstances et compatibles avec les lois nationales.

MINIMISATION ET CONSERVATION DES DONNÉES

La collecte, l'accès et l'utilisation des informations personnelles doivent se limiter au minimum nécessaire pour répondre à des fins commerciales légitimes et pour fournir, maintenir ou développer des applications et des services. Les informations personnelles ne doivent pas être conservées plus longtemps que nécessaire à ces fins commerciales légitimes ou pour satisfaire aux obligations légales et elles doivent par la suite être supprimés ou rendues anonymes.

RESPECT DES DROITS DE L'UTILISATEUR

Les utilisateurs doivent recevoir des informations sur leurs droits quant à l'utilisation de leurs informations personnelles et des moyens simples pour exercer ces droits.

CHOIX ET CONTRÔLE DE L'UTILISATEUR

OPT IN OPT OUT

Participation ou exemption : les utilisateurs doivent pouvoir exercer un choix et un contrôle pertinents vis-à-vis de leurs informations personnelles.

ÉDUCATION

Les utilisateurs doivent recevoir des informations sur les questions de confidentialité et de sécurité et les façons de gérer et protéger leur confidentialité.

39. Principes de Protection de la vie privée sur mobile de la GSMA (2016), voir : http://www.gsma.com/publicpolicy/mobile-privacy-principles
40. http://www.gsma.com/publicpolicy/mobile-privacy-principles

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

La GSMA et ses membres estiment que le respect de la vie privée et la sécurité sont essentiels pour obtenir la confiance des consommateurs dans les services mobiles et c'est dans cette perspective qu'ils s'engagent à travailler avec les parties prenantes de l'ensemble du secteur mobile en vue d'élaborer une approche cohérente à la protection de la vie privée et de promouvoir la confiance dans les services mobiles. En ce qui concerne les services qu'ils fournissent eux-mêmes à leurs consommateurs, les opérateurs de réseau mobile vont s'efforcer de protéger l'identité numérique et de sécuriser les communications et les données à caractère personnel. La multiplicité des services tiers disponibles sur les appareils mobiles offre des degrés différents de protection de la vie privée. Par conséquent :

- Pour garantir aux consommateurs que leurs données personnelles soient correctement protégées, quel que soit le service ou l'appareil, un niveau cohérent de protection doit être fourni
- Les protections nécessaires doivent provenir d'une combinaison d'approches convenues internationalement, de législations nationales et d'actions du secteur

Dans une démarche de transparence et d'information des consommateurs, le secteur mobile, les autorités de protection des données et les autres régulateurs doivent :

- Indiquer clairement aux consommateurs les données qu'ils protègent et les attentes que les consommateurs sont en droit d'avoir en termes de respect de la vie privée
- Expliquer clairement qu'ils ne disposent d'aucun moyen de contrôle vis-à-vis d'applications et de services fournis par des tiers. Pour les consommateurs avisés, cela peut couler de source, mais ce n'est pas le cas pour de nombreux segments de consommateurs

Lors de la formulation ou de la révision de dispositions législatives ou réglementaires :

- Les États doivent veiller à la neutralité de la législation en termes de service et de technologie, en vue de l'application uniforme des règles à toutes les instances qui collectent, traitent et conservent des données à caractère personnel
- En raison du niveau élevé d'innovation dans les services mobiles, la législation devrait être axée sur le risque pour la vie privée d'un individu, plutôt que de tenter de légiférer pour certains types de données. Par exemple, le même élément de données peut être utilisé pour en extraire de la valeur commerciale (par ex. en étant vendu à des tiers), opérationnelle (par ex. pour éclairer la prise de décisions internes et d'affectation des ressources), ou publique (par ex. éclairer les efforts de reprise après sinistre)

Choix du consommateur

Donner au consommateur les moyens de choisir

De nombreux services en ligne sont offerts gratuitement aux consommateurs, auquel cas, la source de revenus du prestataire provient des annonces publicitaires qu'il vend. Afin d'optimiser ces recettes, la plupart des services en ligne, qu'il s'agisse aussi bien de sites Internet que d'applications sur mesure, utilisent les informations sur l'utilisateur pour permettre aux annonceurs qui sont intéressés par ce type de profil de faire une offre pour présenter son annonce (dans divers formats) à l'utilisateur en question. Ce type de ventes aux enchères de micro-segments à la milliseconde près devient de plus en plus répandu et il revient au prestataire de service d'utiliser les informations propres à l'utilisateur qu'il a obtenues directement ou qu'il a achetées. Bien qu'il y ait certes un équilibre à trouver entre les utilisateurs qui partagent des informations en échange d'utiliser des services gratuits, il est important qu'il leur soit donné les moyens de faire des choix éclairés sur ce type de contrepartie.

L'étude réalisée pour le compte de la GSMA[41] révèle que les utilisateurs de mobiles veulent avoir des choix simples et clairs à faire pour contrôler l'utilisation des informations qui les concernent. L'étude a révélé que plus de 80 % des internautes mobiles dans le monde entier s'inquiètent de partager leurs données à caractère personnel lorsqu'ils accèdent à des applications et des services. Par ailleurs, avant d'installer une application, la majorité (65 %) des utilisateurs de l'app cherchent à connaître le type de renseignements auxquels l'application veut accéder sur leur appareil, ce qui atteste bien de leur souhait de comprendre comment le respect de leur vie privée pourrait être atteint. La plupart des utilisateurs mobiles (81 %) souhaitent aussi qu'on leur demande leur permission avant que des tiers aient accès à leurs données à caractère personnel sur leurs appareils mobiles, et désirent avoir plus de contrôle quant aux types de données auxquelles différentes entreprises peuvent avoir accès.

41. La GSMA a travaillé en étroite collaboration avec ses membres pour relever les grands défis de la Protection de la vie privée sur mobile et, dans le cadre de ces efforts, elle a commandé une étude mondiale portant sur plus de 11 500 utilisateurs mobiles (Brésil, Colombie, Indonésie, Malaisie, Singapour, Espagne et Royaume-Uni). Les constats révèlent que les utilisateurs mobiles de tous les pays partagent les mêmes attitudes et les mêmes préoccupations au sujet de leur vie privée. Le document « Protection de la vie privée sur mobile : Connaissances approfondies issues des études sur les consommateurs et considérations pour les décideurs » en présente les grands constats et envisage les implications pour les décideurs politiques. Pour consulter le rapport détaillé, voir http://www.gsma.com/publicpolicy/mobile-privacy-consumer-research-insights-and-considerations-for-policymakers

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Sur les neuf principes de Protection de la vie privée sur mobile relevés par la GSMA, trois sont particulièrement pertinents pour le choix du client en ce qui concerne ses renseignements personnels :

- Le choix et le contrôle de l'utilisateur : les utilisateurs doivent avoir l'opportunité d'exercer un choix et un contrôle réels de leurs informations personnelles[42]
- Respect des droits de l'utilisateur : les utilisateurs doivent recevoir des informations sur leurs droits quant à l'utilisation de leurs informations personnelles et des moyens simples pour les faire valoir
- Éducation : les utilisateurs doivent recevoir des informations sur les questions de respect de la vie privée et de sécurité et les façons de gérer et protéger leur vie privée

Guidée par ces principes, la GSMA a également élaboré un ensemble de lignes directrices de conception du respect de la vie privée pour le développement d'applications mobiles en collaboration avec des représentants de l'écosystème mobile. Ces lignes directrices visent à aider les développeurs d'applications à incorporer le respect de la vie privée dans les nouvelles applications et les nouveaux services.

Cependant, ces principes, même s'ils sont pleinement adoptés, sont forcément limités pour offrir aux consommateurs le niveau de choix qu'ils requièrent. Les opérateurs de réseau mobile n'ont guère d'influence quant aux conditions générales de respect de la vie privée utilisées par les prestataires de services en ligne. L'adoption de dispositions législatives et réglementaires nouvelles pourrait avoir l'effet malencontreux d'imposer une charge excessive sur l'utilisateur mobile et d'exacerber un sentiment de « lassitude en matière de respect de la vie privée », ayant pour conséquence qu'il consente à des conditions qu'il n'a en fait ni lues ni comprises.

Pour les services qu'ils fournissent, les opérateurs de réseau mobile vont devoir s'efforcer d'observer des politiques claires en matière de respect de la vie privée et de faire en sorte qu'il soit facile de comprendre et contrôler la manière dont les données à caractère personnel sont utilisées.

La GSMA s'engage à collaborer avec les parties prenantes de l'ensemble du secteur mobile pour développer une approche cohérente à la protection de la vie privée et promouvoir la confiance dans les services mobiles. Cet engagement a donné lieu à diverses initiatives, notamment à l'adoption d'une position de leadership à cet égard au moyen des lignes directrices de la GSMA en matière de conception de la vie privée pour le développement d'applications mobiles, qui soulignent que :

- Il revient aux opérateurs de réseau mobile de s'assurer que les risques liés à la vie privée sont pris en considération lors de la conception de nouvelles applications et de nouveaux services et de développer des solutions qui fournissent aux clients des façons simples de comprendre leurs choix en matière de confidentialité et de contrôler leurs données
- Les développeurs d'applications pour appareils mobiles doivent incorporer les principes de respect de la vie privée élaborés par le secteur et leurs lignes directrices associées en matière de conception, comme les principes de Protection de la vie privée sur mobile de la GSMA
- La protection doit être conçue comme faisant partie intégrante des nouvelles applications et des nouveaux services (on parle de « vie privée dès la conception ») pour apporter transparence, choix et contrôle à l'utilisateur individuel et gagner sa confiance

42. Les Principes protection de la vie privée de la GSMA parlent de « informations personnelles » en référence aux données à caractère personnel

Flux transfrontalier de données à caractère personnel

Le troisième aspect du respect de la vie privée des consommateurs a trait au(x) pays où les données à caractère personnel sont conservées et/ou auxquelles il y est fait accès, et les implications des flux transfrontaliers des données. Il est fréquent que le stockage et le traitement des données d'une manière centralisée permettent aux opérateurs de réseau mobile d'améliorer les performances et la rentabilité de leur prestation de services qui pourrait sinon ne pas être viable dans le cadre d'une opération dans un seul pays. Les consommateurs bénéficient de la multitude de services, d'innovations et de support qu'une telle démarche permet. Or le transfert de données d'un pays à un autre peut soulever des questions quant à la compétence juridique concernée. L'existence de cadres et de mécanismes de responsabilisation interopérables peut aider les États à faire face aux contestations de compétence juridique et faciliter les flux transfrontaliers de données.

Les cadres émergents tels que les règles transfrontalières de protection de la vie privée de l'APEC et les règles d'entreprise contraignantes de l'Union européenne posent des principes internationaux communs, notamment des mécanismes de responsabilisation qui régissent la manière de traiter les données lors de leur transfert d'un pays à l'autre. Leur adoption est toutefois entravée par l'adoption par des États de règles de « localisation des données » (appelées aussi « souveraineté des données »), qui imposent des exigences de stockage local ou d'utilisation de technologies locales.[43] Ce type d'exigences de localisation se retrouvent dans toutes sortes de règles propres à des secteurs ou des domaines, notamment pour les prestataires de services financiers, la confidentialité professionnelle ou pour le secteur public et elles sont parfois imposées par des pays convaincus qu'il est plus facile pour les autorités de contrôle de vérifier des données qui sont conservées localement.[44] Bien que certaines de ces règles puissent chercher à protéger la vie privée des particuliers, elles en viennent à fragmenter les dispositions législatives et réglementaires existantes, ce qui présente le double risque de confusion et de restriction des avantages offerts par une infrastructure de réseau ouverte. Il est possible aussi que ces mêmes règles relatives à la localisation des données nuisent au commerce numérique et à la croissance économique mondiale.

Répondre aux questions de respect de la vie privée et de sécurité des flux transfrontaliers de données

L'exploitation d'un réseau mobile produit, jour après jour, de grandes quantités de données. Chaque appel et chaque transfert de données doivent être enregistrés pour être ensuite traités en fonction du tarif en vigueur et des donnéess du solde du compte pour pouvoir facturer les utilisateurs les services qu'ils utilisent. Des quantités volumineuses de données opérationnelles sont générées et stockées, telles les données de trafic, les registres d'erreurs ou les demandes des clients (par ex., changement de tarif, changement d'adresse). Face à toutes ces exigences, les opérateurs de réseau mobile sont de gros utilisateurs de services mondiaux de stockage et de traitement centralisés de données. Les consommateurs bénéficient du large éventail de services d'innovations et de solutions de pointe que les opérateurs sont en mesure d'offrir, directement ou par un tiers, en ayant accès à ces services mondiaux et en les utilisant, que ce soit directement auprès de l'opérateur ou par un tiers.

Assurer l'intégrité et la sécurité de ces données relève d'une entreprise majeure et nécessite des solutions complexes. De nombreux opérateurs de réseau mobile, surtout s'il s'agit de filiales de groupes internationaux ou qui choisissent d'utiliser des fournisseurs tiers, peuvent conclure que la meilleure solution est d'héberger et de traiter les données dans plusieurs pays. Cela leur permet de renforcer les économies d'échelle et leur expertise en regroupant les besoins de plusieurs pays pour bâtir une solution globale et plus robuste, d'une fonctionnalité et d'une sécurité renforcées et d'une redondance accrue, qui ne seraient pas possible s'ils adoptaient une approche fragmentée à pays unique. En adoptant une approche centralisée, les opérateurs peuvent acquérir une expertise plus approfondie et mettre en œuvre des solutions de sauvegarde et de redondance qui pourraient autrement ne pas être viables économiquement, voire possibles, pour une opération simple dans un seul pays. Bien entendu, de telles solutions nécessitent le transfert des données des consommateurs dans des centres de données multinationaux qui, bien souvent, sont implantés dans des pays autres que celui de l'opérateur de réseau d'origine.

Bien que les avantages techniques soient indubitables, les implications juridiques sont complexes : les règles de protection des données de quel pays convient-il d'appliquer ? Celles du pays où les données sont traitées, du pays de l'utilisateur final ou du pays où se trouve le responsable du traitement des données (par exemple, l'opérateur de réseau mobile) ?

Plusieurs raisons expliquent la décision par des pays d'imposer des règles de localisation des données, notamment la conviction qu'il s'agit là d'un moyen pour les autorités de contrôler plus facilement les données stockées localement. Une autre raison courante vient du désir de protéger la vie privée de l'individu et de veiller au respect des attentes et des normes en vigueur dans le pays en question : un moyen évident à cela consiste à imposer que les données demeurent dans le pays. Or il existe des solutions et des principes qui permettent d'atténuer ces risques sans restreindre les flux de données et les avantages qui en découlent.

43. Anupam Chander et Uyen Le, 2015. « Data Nationalism », Emory Law Journal; et Jonah Force Hill, 2014. « The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders », Hague Institute for Global Justice

44. Commission européenne, « La création d'une économie européenne fondée sur les données », pg.5

Les restrictions imposées aux données à caractère personnel n'impliquent pas forcément une meilleure protection. Une approche fragmentée entraîne une protection disparate (par ex. des différences entre les pays et les secteurs quant au type de données qu'il est possible de stocker et pendant combien de temps) et est source de confusion qui nuit à la gestion sécurisée des données à caractère personnel. La fragmentation par la localisation peut aussi dresser des obstacles qui rendent les investissements dans la protection de la sécurité d'un coût prohibitif. Collectivement, une telle démarche peut aller à contre-courant des efforts déployés par les opérateurs de réseau mobile visant à développer des technologies et des services de renforcement du respect de la vie privée destinés à protéger les consommateurs.

Il est important de réitérer la distinction qui existe entre les données à caractère personnel auxquelles les opérateurs de réseau mobile ont accès et qu'ils traitent, par rapport aux données à caractère personnel collectées et stockées par les prestataires de services en ligne et les intermédiaires sur Internet. Comme on l'a vu à la section consacrée au choix du consommateur, il s'agit là de services très différents et le fait qu'ils soient opérés depuis l'extérieur du pays d'utilisation a pour effet dans de nombreux cas d'augmenter les complexités juridiques. Les préoccupations et les enjeux relatifs au respect de la vie privée sont tout aussi pertinents à cet égard, mais ils échappent au contrôle des opérateurs de réseau mobile, tant en ce qui concerne le type des données transférées par les utilisateurs que de la manière dont il y est fait accès.

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Le flux international des données joue un rôle important en matière d'innovation, de concurrence et de développement économique et social. Par conséquent :

- Il convient de limiter au strict minimum les restrictions et les conditions imposées aux flux internationaux de données, et de les appliquer exclusivement dans des circonstances exceptionnelles
- Les règles relatives au flux transfrontalier des données doivent être fondées sur les risques et soutenir des mesures qui visent à assurer le traitement des données en adoptant des mesures de sauvegarde appropriées et proportionnées tout en contribuant à la réalisation des avantages socio-économiques potentiels
- Aussi, dans la mesure où les États doivent contrôler les données à des fins officielles, ils devraient pouvoir y parvenir en usant des moyens légaux existants et des mécanismes intergouvernementaux appropriés qui ne restreignent pas le flux de données

Les opérateurs de réseau mobile reconnaissent les préoccupations concernant la conservation sûre et sécurisée des données et les souhaits des particuliers à ce qu'il ne soit pas porté atteinte à leurs droits. Ils reconnaissent aussi les défis plus globaux de surveillance nationale et internationale. Toutefois :

- Les États ne devraient imposer des mesures de restriction des flux transfrontaliers de données que si elles sont absolument indispensables pour atteindre un objectif légitime de politique publique
- L'application de ces mesures devrait être proportionnée et non pas arbitraire ou discriminatoire à l'égard de fournisseurs ou de services étrangers

Une préoccupation centrale porte sur l'actuelle fragmentation de la régulation des flux transfrontaliers de données par un mélange de lois et d'instruments en vigueur sur le plan international, régional et national. Bien qu'ils adoptent des principes communs, ils ne créent pas un cadre réglementaire interopérable qui reflète les réalités, les défis et le potentiel d'un monde globalement connecté. Les règles de protection des données devraient être rendues interopérables entre pays et régions dans la plus large mesure possible. L'interopérabilité est source de sécurité et de prévisibilité accrues, qui permet à une entreprise de bâtir un cadre évolutif et responsable de protection des données et de respect de la vie privée.

L'existence de cadres interopérables de protection des données permettrait de renforcer et d'encourager des mécanismes appropriés et efficaces pour s'assurer que les données sont gérées dans un souci de sauvegarde des droits et des intérêts des consommateurs et des citoyens. Des cadres interopérables de protection des données dotés de mécanismes efficaces de responsabilisation peuvent contribuer à renforcer et à protéger des droits importants qui contribuent à la prospérité des particuliers et des économies. Par exemple, les efforts visant à assurer l'interopérabilité des règles transfrontalières de protection de la vie privée de l'APEC et des règles d'entreprise contraignantes de l'Union européenne peuvent potentiellement profiter à la défense des intérêts et des droits du secteur, du commerce numérique et des consommateurs.

La GSMA et ses membres demeurent résolus à travailler avec les parties prenantes pour veiller à une gestion des flux transfrontaliers des données d'une manière qui sauvegarde les données à caractère personnel et la vie privée des particuliers. La GSMA et ses membres reconnaissent également l'importance de s'attaquer aux questions difficiles qui découlent des flux transfrontaliers de données, notamment en matière de compétence juridique.

5 Protection de la sécurité publique

En tant que fournisseurs d'infrastructures nationales essentielles, les réseaux mobiles jouent un rôle important dans la protection du grand public et de la société dans son ensemble. Par exemple, les réseaux mobiles sont utilisés comme moyen de communication pour les services d'urgence, surtout dans les interventions suite à des incidents majeurs, et beaucoup d'incidents sont signalés par le public via leur appareil mobile.

En vertu des dispositions législatives et réglementaires en vigueur, y compris des obligations de licence, et conformément à la législation locale, les opérateurs de réseau mobile sont tenus dans l'obligation d'aider les services de la sûreté dans un objectif global de la protection de la sécurité publique. Ainsi, il est possible que dans le cadre d'enquêtes criminelles, les services de sûreté obtiennent des ordonnances judiciaires en vue de surveiller les communications faites, reçues ou échangées entre des suspects. Par conséquent, à titre d'exigence standard de l'octroi de la plupart des licences, les opérateurs de réseau mobile sont tenus de fournir les moyens techniques pour s'acquitter de leurs obligations juridiques d'aider les services de sûreté. Dans la plupart des pays, ces interventions sont limitées et sujettes au respect du droit.

La Déclaration universelle des droits de l'homme (DUDH)[45] et le Pacte international relatif aux droits civils et politiques (PIDCP)[46] reconnaissent que les individus partout dans le monde ont le droit de communiquer entre eux en privé et aussi le droit à la liberté d'expression, dans les limites

45. La Déclaration universelle des droits de l'homme (DUDH) a été proclamée par l'Assemblée générale des Nations Unies à Paris le 10 décembre 1948 comme un idéal commun à atteindre pour tous les peuples et toutes les nations. Elle stipule, pour la première fois, la protection universelle des droits de l'homme fondamentaux. Le droit à la vie privée est énoncé à l'article 12 et le droit à la liberté d'expression à l'article 19. Pour consulter le texte de la DUDH, voir : http://www.un.org/fr/universal-declaration-human-rights/

46 Le Pacte international relatif aux droits civils et politiques (PIRDCP) est un traité multilatéral adopté par l'Assemblée générale des Nations Unies le 16 décembre 1966 et est en vigueur depuis le 23 mars 1976. Le droit à la vie privée est énoncé à l'article 17 et le droit à la liberté d'expression à l'article 19. Pour consulter le traité, voir : https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_fr

des confins, des frontières et de la moralité publique d'un État-nation donné. Les instruments internationaux relatifs aux droits de l'homme définissent également que ces droits ne peuvent être restreints que dans des circonstances préalablement décrites très limitées et que toute limitation doit toujours être nécessaire et proportionnée à la menace perçue.

Il peut exister des tensions entre les objectifs de sécurité nationale et de mise en application de loi pour protéger la sécurité publique et les droits à la vie privée, la liberté d'expression et l'accès à l'information. Dans la plupart des pays, ces besoins potentiellement conflictuels se traduisent par l'adoption d'une position par défaut qui fait valoir que chacun devrait pouvoir communiquer librement et en privé et que toutes interventions et interruptions devraient se limiter à des exceptions nécessaires et proportionnées, soumises au respect du droit. La plupart des pays ont des garde-fous visant à empêcher les abus et l'utilisation excessive de pouvoirs qui sont susceptibles de porter atteinte à la vie privée de communication.

La présente section souligne trois exemples types d'interventions portant sur la sécurité publique et les enjeux qui se posent lorsque les diverses parties cherchent à y répondre dans la pratique, et plus précisément :

- Les demandes d'assistance des services de sûreté, en mettant l'accent sur la nécessité de transparence et de garde-fous
- La restriction du service, en mettant un accent particulier sur l'utilisation de brouilleurs mobiles
- L'enregistrement des utilisateurs, en mettant l'accent sur l'enregistrement des utilisateurs de cartes SIM prépayée

Chacun de ces enjeux présente des implications importantes pour les pouvoirs publics, l'industrie et d'autres parties prenantes, et ils sont également abordés dans plus de détail plus loin dans ce chapitre.

Protection de la sécurité publique

Dans le cadre des lois et des règlements, y compris des obligations de licence, et conformément à la législation locale, les opérateurs de réseau mobile sont tenus dans l'obligation d'assumer des responsabilités supplémentaires pour aider les services de sûreté dans le respect de l'objectif global de protection de la sécurité publique. Il est important que les États aient en place un cadre juridique proportionnel qui précise clairement les pouvoirs à la disposition des services de sûreté. Le cadre juridique doit également veiller au caractère nécessaire et proportionné des demandes d'assistance, en s'assurant de les adresser au fournisseur du service de communication ou de technologie le plus approprié et compatible, et dans le respect des principes des droits de l'homme. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à se conformer à l'ensemble des obligations juridiques et de licence dans leurs réponses aux préoccupations de sûreté et de sécurité publique présentes dans les pays où ils opèrent, dans le plein respect des droits de l'homme. Nous nous engageons à coopérer avec les organes de sécurité en vue de protéger la sécurité publique en adoptant les mesures suivantes :

- **Dès lors que la situation l'exige, travailler avec les organismes compétents à l'élaboration et à la mise en œuvre de solutions appropriées en vue de parvenir à l'objectif final tout en faisant subir le minimum de perturbations aux consommateurs et aux services essentiels**
- **Renforcer les réseaux disposant de la fonctionnalité de remédier à des situations d'urgence et de sécurité, le cas échéant**
- **Stipuler clairement notre limite d'action vis-à-vis de la chaîne de valeur en soulignant les domaines qui relèvent de l'intervention de tiers**

Demandes d'assistance des services de sûreté

Obtempérer aux demandes d'assistance des services de sûreté

En règle générale, les licences des opérateurs de réseau mobile stipulent les obligations des opérateurs de réseau de donner leur appui aux services de sûreté et aux activités de sécurité nationale du pays émetteur. Là où elles existent, ces lois et obligations de licence exigent généralement des opérateurs de réseau mobile d'une part de conserver les données[47] concernant l'utilisation des services mobiles par leurs consommateurs et de les relayer aux services de sûreté quand ils en font la demande légitime, et d'autre part de se doter des moyens nécessaires pour intercepter les communications des consommateurs en direct sur demande légitime.

Les lois définissent généralement les conditions, et parfois les procédures, en vertu desquelles les services de sûreté peuvent exiger des opérateurs de réseau mobile de fournir l'accès ou des informations sur les communications échangées sur leur réseau et de fournir le point de référence juridique qui guide les opérateurs de réseau mobile dans leur réponse à ces demandes. En novembre 2016, le Royaume-Uni (R-U) a adopté une nouvelle législation[48] qui clarifie ces limites. Bien qu'il existe des divergences de vue sur l'acceptabilité des pouvoirs que la nouvelle loi accorde aux services de sûreté britanniques, il est important de relever que les règles ont fait l'objet de débats et ont été promulguées publiquement. Dans certains pays, il arrive que le cadre légal manque de clarté pour réguler la divulgation des données ou l'interception légale des communications des consommateurs. Cette lacune pose des problèmes pour le secteur qui cherche à protéger la confidentialité des informations des clients, tout en s'acquittant des obligations stipulées par leur licence d'assistance aux services de sûreté.

Ces dernières années ont été témoins d'un important débat public mondial sur la portée, la nécessité et la légitimité des pouvoirs juridiques dont les autorités gouvernementales usent pour accéder aux communications de particuliers. Des questions ont également été soulevées quant au rôle que jouent les fournisseurs de réseau et les prestataires de services de télécommunications à l'égard d'un tel accès. C'est dans ce contexte qu'en 2011, un groupe d'opérateurs et de fournisseurs de réseau mobile a formé le Telecommunications Industry Dialogue (ID) (voir ci-dessous) dans le but de travailler ensemble sur les enjeux du respect de la vie privée et de la liberté d'expression, et a posé les principes décrivant la responsabilité des entreprises de télécommunications dans leur sauvegarde. Parmi les résultats des travaux de l'ID, un certain nombre de ses entreprises membres ont pris l'initiative de divulguer, dans la mesure du possible, des informations sur la nature et le volume des demandes d'accès reçues des pouvoirs publics dans chaque pays où elles opèrent.[49]

Il est fréquent que la législation soit en décalage sur les développements technologiques[50] et des malentendus peuvent survenir quant au niveau de capacité technique des opérateurs de réseau mobile en matière d'interception des communications. Il est techniquement possible d'intercepter des appels téléphoniques ou des messages SMS standard entre des utilisateurs spécifiques et cela fait des dizaines d'années que les normes mobiles mondiales stipulent les exigences et les capacités d'interception licite. En revanche, les communications entre utilisateurs échangées sur une plateforme basée sur Internet sont généralement hors de portée des opérateurs de réseau mobile, même si le trafic emprunte leur réseau. Certains services prisés, tels que WhatsApp, WeChat et Signal, sont chiffrés, les messages n'étant pas stockés par les opérateurs de réseau mobile, ni les clés de déchiffrement mises à leur disposition. Cela signifie que, même s'ils en reçoivent la demande légitime, les opérateurs de réseau ne sont pas en mesure d'accéder au contenu des messages, et par conséquent sont incapables de les fournir (voir l'exemple de restriction de service de WhatsApp au Brésil à la section suivante).

Les opérateurs de réseau mobile reconnaissent l'importance de la souveraineté et de la légitimité des gouvernements dans la défense de la sécurité de leurs citoyens. C'est dans la poursuite de cet objectif que toute interception des communications à des fins de répression ou de sécurité ne devrait survenir que dans un cadre légal clair, compatible avec les principes des droits de l'homme de nécessité et de proportionnalité, et dans le respect de la procédure et des exigences d'autorisation adéquats qui y sont précisées.

Enfin, ce sont les opérateurs de réseau mobile qui au final doivent assumer la responsabilité et souvent aussi le coût des activités qu'ils déploient à l'appui des besoins en matière de sécurité publique. Le Salvador présente un exemple extrême à cet égard, où une taxe de 5 % sur les services de télécommunications a été approuvée en novembre 2015 pour financer les plans de sécurité d'ordre général du gouvernement.[51] Bien que la politique budgétaire relève du champ de décision de tout gouvernement, imposer une taxe aux opérateurs de l'infrastructure de réseau mobile, celle-là même qui prend en charge la sécurité, traduit une démarche contreproductive puisqu'elle détourne des fonds de l'une des parties qui investit déjà dans la sécurité publique.

47. Annulant la directive en 2014, la Cour de justice européenne (CJUE) a jugé que « la rétention générale des données personnelles », telle qu'ordonnée par la directive européenne sur la conservation des données a violé le droit à la vie privée stipulé dans la Charte des droits fondamentaux de l'Union européenne. En décembre 2016, la CJUE a confirmé sa position et a statué que les lois nationales qui portent application de la directive sur la conservation des données sont en violation de l'acquis de l'Union européenne
48. Pour en savoir plus, voir : http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
49. Néanmoins, de nombreux pays interdisent expressément aux opérateurs de réseau mobile de rendre publics les détails de haut niveau sur la nature ou le volume des demandes d'interception qu'ils ont reçues.
50. GSMA, 2016. « Manuel des politiques de communications mobiles : Accès par l'État »
51. Telecompaper, 2016. « El Salvador introduces 5% telecoms tax »

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Il incombe aux opérateurs de réseau mobile de veiller à ne répondre qu'aux demandes légales (c.-à-d. sur mandat judiciaire) des services de sûreté qui sont légalement autorisés et ont agi dans le respect du droit, moyennant des mécanismes de sauvegarde appropriés.

Par conséquent, il revient aux États de s'assurer de mettre en place un cadre légal proportionnel qui précise clairement les pouvoirs de surveillance dont les services de sûreté peuvent se prévaloir[52]

- Toute ingérence dans le droit à la vie privée doit se faire dans le respect du droit : la conservation et la communication de données et l'interception de communications à des fins de répression ou de sécurité doivent intervenir uniquement en conformité avec les procédures et les autorisations prévues par ce cadre[53]
- Une procédure légale devrait être prévue pour que les fournisseurs de télécommunications puissent contester les demandes qui, d'après eux, sortent du champ d'application des lois concernées
- Le cadre devrait être transparent, proportionnel, justifié et compatible avec les principes des droits de l'homme, y compris les obligations en vertu des conventions internationales en vigueur relatives aux droits de l'homme, comme la Convention internationale sur les droits civils et politiques
- Étant donné l'élargissement de la palette de services de communication, le cadre légal devrait être technologiquement neutre.[54]
- Les États devraient prévoir des limitations de responsabilité appropriées ou indemniser les fournisseurs de services de télécommunications contre les demandes introduites portant sur l'exécution des demandes d'assistance et des obligations de conservation, de divulgation et d'interception des communications et des données et le retrait de l'accès au réseau et de services[55]
- Par ailleurs, c'est aux États qu'il devrait revenir de supporter les coûts induits par le respect de l'ensemble des lois couvrant l'interception des communications, la conservation et la divulgation des données, ou la restriction de l'accès à des réseaux ou services, comme c'est déjà le cas dans certains pays aujourd'hui. De tels coûts et la base de leur calcul devraient être convenus d'avance.[56]

La GSMA et ses membres soutiennent les initiatives qui cherchent à accroître la transparence des États et la publication par l'État de statistiques liées aux demandes d'accès aux données sur les clients[57] dans la mesure du possible.

52. GSMA, 2016. « Manuel des politiques de communications mobiles : Accès par l'État »
53. Ibid.
54. Ibid
55. Ibid.
56. Ibid
57. Ibid.

Étude de cas

Telecommunications Industry Dialogue — Rapports de transparence (divulgation des demandes reçues par les autorités)

Justification de la publication de rapports...

Le Telecommunications Industry Dialogue (ID), créé officiellement en 2013, est un groupe d'opérateurs et de fournisseurs en télécommunications qui, ensemble, se penchent sur les enjeux de la liberté d'expression et des droits à la vie privée dans le secteur des télécommunications tels que définis par les Principes directeurs des Nations Unies sur les entreprises et les droits de l'homme. Avec leur présence mondiale, ces entreprises fournissent des services et des équipements de télécommunications à des consommateurs, des entreprises et des services publics dans près d'une centaine de pays à travers le monde.

L'un des principaux axes d'activité d'ID porte sur le partage des enseignements. Par ailleurs, dans une démarche de transparence, les opérateurs d'ID AT&T, Millicom, Orange, Telenor Group, Telia Company et Vodafone Group, publient régulièrement des rapports qui donnent des renseignements sur les demandes d'assistance qu'ils ont reçues des services de sûreté. Ils espèrent que ces rapports aideront le public à comprendre le contexte dans lequel ils opèrent et les échanges qu'ils ont avec les services de sûreté.

La teneur des rapports...

En règle générale, les rapports visent à :

- **Expliquer les cadres juridiques et les capacités des services de sûreté en vigueur dans les marchés où ils opèrent**
- **Expliquer les politiques et les procédures adoptées dans leurs réponses aux demandes des organismes et des autorités**
- **Lorsque cela est possible, rendre compte des statistiques sur le nombre de demandes d'assistance reçues des services de sûreté pour obtenir des données sur des consommateurs dans des pays ou régions spécifiques**

La nature des limitations...

Il est fréquent que les services de sûreté et la législation sur la sécurité nationale imposent des restrictions strictes qui empêchent les opérateurs de divulguer toute information relative aux demandes qu'ils reçoivent de la part des services répressifs ou des autorités, y compris des statistiques globales. Dans de nombreux pays, il est interdit aussi aux opérateurs de fournir au public toute indication quant aux moyens employés pour donner suite à ces demandes. Face à ces restrictions, il peut être très difficile pour les opérateurs de répondre au public qui leur demande plus de transparence

Ces opérateurs restent toutefois convaincus que, bien que la responsabilité de la transparence incombe principalement aux États, le fait de relever les demandes reçues des autorités, avec toutes les faiblesses que cela présente, constitue la mesure la plus sensée à être disponible, en évitant d'être trop complexe. Ils soulignent également que seuls les pouvoirs publics qui formulent ces demandes aux fournisseurs de communications sont en mesure de donner une image complète de l'étendue des demandes.

(Telecommunications Industry Dialogue, voir : https://www.telecomindustrydialogue.org/)

Ordonnances de restriction de service et brouilleurs

Ordonnances de restriction de service

En dehors des demandes d'interception de communications, il arrive que des autorités gouvernementales donnent l'ordre aux opérateurs de réseau mobile (ORM) de limiter les services qu'ils fournissent sur leur réseau : on parle alors d'ordonnances de restriction de service. Ces ordonnances exigent des opérateurs qu'ils ferment ou restreignent l'accès à leur réseau mobile, à un service du réseau ou à un service tiers auquel leur réseau donne accès. Les ordonnances peuvent imposer le blocage de certains services ou contenus mobiles ou sur Internet, la restriction de la bande de fréquence ou l'abaissement de la qualité des services SMS ou vocaux. En plus d'être obligés par la loi de se plier à ces demandes, dans certains cas, les opérateurs de réseau mobile peuvent être passibles de sanctions pénales (allant jusqu'à l'emprisonnement des cadres supérieurs) ou risquer de perdre leur licence s'ils venaient à divulguer qu'ils ont reçu une ordonnance de restriction de service ou à refuser d'y donner suite.

Ces ordonnances peuvent avoir un certain nombre de conséquences graves. Ainsi, la sécurité nationale peut être compromise en cas de détournement des pouvoirs (c.-à-d. s'en remettre à des restrictions de réseau pour prévenir les attaques terroristes prive autant les citoyens que les forces de l'ordre de la possibilité d'utiliser d'outils de communication dans la lutte contre le terrorisme). La sécurité publique, quant à elle, peut être mise en danger si les services d'urgence et les citoyens ne sont pas en mesure de communiquer. La liberté d'expression, la liberté de réunion, la liberté d'entreprise et d'autres droits humains peuvent s'en trouver atteints. Les opérateurs de réseau mobile en souffrent également. Non seulement ils subissent des pertes financières en raison de la suspension des services, ainsi que des atteintes à leur réputation, mais leurs agents locaux peuvent faire l'objet de pressions de la part des autorités, voire de représailles émanant du public.

C'est justement ce qui s'est passé au Brésil, quand il a été reproché au service de messagerie WhatsApp son manque d'empressement à appuyer diverses enquêtes criminelles.[58] En réponse, le gouvernement a exigé des opérateurs de réseau mobile au Brésil de restreindre l'accès aux services de WhatsApp à trois reprises depuis décembre 2015.[59] Le principal impact de cette mesure a été d'empêcher les 100 millions d'utilisateurs au Brésil d'utiliser l'application de messagerie mobile la plus populaire du pays. Chacune des décisions a été annulée sur appel devant les tribunaux supérieurs en raison de leur impact disproportionné. WhatsApp et sa société mère, Facebook, fait valoir l'impossibilité technique de toute coopération éventuelle en l'absence de stockage des communications, et même si elles venaient à l'être, elles resteraient inaccessibles en raison de l'utilisation du chiffrement de bout en bout. Pourtant, plusieurs des utilisateurs pénalisés font souvent porter le blâme de la perturbation du service aux opérateurs de réseau mobile.

Des exemples plus extrêmes d'interruptions de réseau se sont produits dans certains pays, parfois dans le but d'empêcher des opposants politiques au gouvernement de s'organiser.[60] Avant toute chose, les opérateurs de réseau mobile exhortent les gouvernements à faire preuve de transparence avec leurs citoyens quant à leur rôle dans l'interruption ou la restriction des réseaux et des services, et quant aux justifications légales de toute restriction. Il est important que les ordonnances d'interruption autorisent les entreprises à relayer sans délai à leurs clients la restriction imposée à leurs services sur ordonnance gouvernementale.[61]

58. The Financial Times, 2016. « WhatsApp ban ignites Brazil censorship fears »
59. The Guardian, 2016. « WhatsApp officially un-banned in Brazil after third block in eight months »
60. Des exemples d'interruption de réseau figurent dans la base de données « Internet & Jurisdiction Retrospective ». Voir : http://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTYtMTEifQ
61. Pour en savoir plus sur la déclaration commune de Telecommunications Industry Dialogue et Global Network Initiative, voir : http://www.telecomindustrydialogue.org/global-network-initiative-telecommunications-industry-dialogue-joint-statement-network-service-shutdowns/

Utilisation de brouilleurs

Le recours à des brouilleurs constitue une autre forme de restriction aux communications mobiles. Il s'agit de dispositifs qui produisent des interférences afin de perturber délibérément des services de communication par radio en agissant sur la communication qui se produit entre le terminal mobile et la station de base. En règle générale, ces outils rudimentaires sont utilisés pour empêcher les communications dans les centres pénitentiaires, ou entre des terroristes ou des groupes considérés politiquement subversifs, souvent là où il se produit des rassemblements publics de masse. Il arrive aussi que des brouilleurs soient utilisés comme outil pour empêcher l'utilisation d'appareils mobiles dans des zones interdites. En Amérique latine notamment, des brouilleurs sont utilisés pour empêcher l'utilisation illégale de téléphones mobiles dans des milieux sensibles, comme dans les prisons par exemple. Toutefois, le blocage du signal ne s'attaque pas à la cause à l'origine du problème : à savoir la possession illégale d'appareils mobiles par des détenus. Par ailleurs, de par la nature-même des signaux radio, il est quasiment impossible de garantir que les effets du brouillage se limitent à l'intérieur de l'enceinte d'un bâtiment. Par conséquent, les brouilleurs causent des interférences qui se répercutent sur les citoyens, les services et les instances de protection de la sécurité publique. De nombreux autres utilisateurs se trouvent impactés, notamment ceux qui vivent et travaillent à proximité des prisons, qui se trouvent incapables d'utiliser les services mobiles. Ces dispositifs nuisent aux opérateurs mobiles en raison du coût des brouilleurs, de la perte de revenus légitimes, et, assez souvent, du préjudice à la réputation causé par des interruptions de service.

Toute perturbation apportée aux réseaux de communication, aux services de réseau ou aux services Internet (qu'il s'agisse de médias sociaux, de moteurs de recherche ou de sites d'actualités) peut potentiellement nuire à la sécurité publique et restreindre l'accès à des services d'urgence, de paiement et de santé qui sont vitaux. Ainsi par exemple, les restrictions de service peuvent limiter la capacité des utilisateurs de mobiles à contacter les services d'urgence en composant des numéros tels que le 112 ou le 911, et elles peuvent perturber le fonctionnement d'alarmes ou de services médicaux personnels connectés à des mobiles. Pour ces raisons, il convient de limiter au minimum les restrictions de service et d'envisager sérieusement toutes les répercussions négatives qu'elles pourraient avoir sur l'ensemble des utilisateurs.

5

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Alors qu'elle comprend et soutient le recours approprié à des interceptions licites pour renforcer la sécurité publique, la GSMA décourage le recours à des ordonnances de restriction de service et à des brouilleurs.

Les États ne devraient recourir à ces ordonnances que dans des circonstances exceptionnelles et prédéfinies, et seulement si elles sont absolument nécessaires et proportionnelles pour atteindre un but spécifique et légitime qui est conforme aux droits humains reconnus sur le plan international et aux lois applicables.[62] D'autres arguments méritent d'être avancés :

- Dans un souci de transparence, les États ne devraient imposer aux opérateurs des ordonnances de restriction de service que par écrit, en se référant à la base juridique et en indiquant clairement la piste de vérification qui remonte à la personne l'autorisant. Ils devraient informer les citoyens que la restriction de service relève d'une ordonnance gouvernementale et a été approuvée par une instance judiciaire ou toute autre autorité, en conformité avec les procédures administratives prévues par la loi. Ils devraient autoriser les opérateurs de réseau mobile à en étudier les impacts sur leur réseau et leurs clients et à communiquer librement avec leurs clients au sujet de l'ordonnance. Si au moment de la restriction du service, cette communication risque de compromettre la sécurité nationale, les citoyens devraient en être informés le plus tôt possible après sa survenance[63]
- Les États devraient chercher à éviter ou à atténuer les effets potentiellement néfastes des ordonnances de restriction de service en minimisant le nombre de demandes, leur portée géographique, le nombre de particuliers et d'entreprises susceptibles d'être concernés, la portée fonctionnelle et la durée de la restriction. Par exemple, plutôt que de bloquer un réseau entier ou toute une plateforme de médias sociaux, il pourrait peut-être être possible de restreindre l'ordonnance à des contenus ou des utilisateurs particuliers. En tout état de cause, l'ordonnance devrait toujours spécifier une date de fin. Des mécanismes de contrôle indépendants devraient être établis pour veiller au respect de ces principes[64]
- Les opérateurs de réseau mobile peuvent jouer un rôle important à sensibiliser les représentants du gouvernement quant à l'impact potentiel des ordonnances de restriction de service. Ils peuvent aussi s'y préparer, de sorte que s'ils reçoivent une telle ordonnance, ils ont les moyens d'en déterminer rapidement et efficacement la légitimité, si elle a été approuvée par une instance judiciaire, si elle est valide et exécutoire, s'il existe une possibilité de recours et s'ils peuvent envisager de travailler avec le gouvernement pour en limiter la portée et ses impacts. Les procédures peuvent prévoir des indications quant à la suite que le personnel local doit donner aux ordonnances de restriction de service (par exemple, les faire remonter aux cadres supérieurs de l'entreprise)[65]
- Toutes les décisions doivent d'abord et avant tout être prises en ayant à l'esprit la sécurité des clients, des réseaux et du personnel des opérateurs de réseau mobile, et dans le but de pouvoir restaurer les services le plus vite possible[66]

La GSMA et ses membres se sont engagés à travailler avec les pouvoirs publics en vue d'utiliser cette technologie comme moyen d'empêcher l'utilisation des téléphones mobiles en milieu sensible, et de coopérer aux efforts visant à détecter, suivre et empêcher l'utilisation d'appareils infiltrés clandestinement. Il est néanmoins vital de trouver une solution pratique à long terme qui ne porte atteinte ni aux utilisateurs légitimes, ni aux investissements importants que les opérateurs mobiles ont déployés pour améliorer leur couverture.[67]

- Les brouilleurs ne devraient être utilisés qu'en dernier recours, et déployés seulement en coordination avec les opérateurs de réseau mobile titulaires d'une licence locale. Cette coordination doit se poursuivre pendant toute la durée de leur déploiement pour veiller à ce que les interférences soient réduites au minimum dans les zones limitrophes et à ce que les utilisateurs légitimes de téléphones mobiles n'en souffrent pas[68]
- En outre, les autorités réglementaires devraient interdire l'utilisation de brouilleurs par des organisations privées et imposer des sanctions à toutes celles qui les utilisent ou les commercialisent sans l'autorisation des autorités compétentes[69]
- Il est impératif de limiter l'importation et la vente de brouilleurs aux autorités jugées compétentes et autorisées à le faire, et c'est au régulateur national des télécommunications qu'il revient d'en autoriser le fonctionnement
- D'autre part, le renforcement des mesures de sécurité visant à empêcher l'infiltration clandestine d'appareils sans fil en milieu sensible, carcéral par exemple, constitue le moyen le plus efficace de lutter contre l'utilisation illégale d'appareils mobiles, puisqu'ils ne portent pas atteinte aux droits des utilisateurs légitimes de services mobiles qui se trouvent dans le voisinage[70]

62. GSMA, 2016. « Manuel des politiques de communications mobiles : Ordonnances de restriction de service »
63. GSMA, 2016. « Manuel des politiques de communications mobiles : Ordonnances de restriction de service
64. Ibid.
65. Ibid.
66. Ibid.
67. GSMA, 2016. « Manuel des politiques de communications mobiles : Brouilleurs »
68. Ibid.
69. Ibid.
70. Ibid.

Pour approfondir

Atténuer l'impact des ordonnances de restriction de service

Dans des situations d'urgence, les autorités gouvernementales de certains pays peuvent, dans la limite de leurs attributions, exiger des interventions drastiques de la part des opérateurs de réseau, allant jusqu'à l'interruption complète ou partielle du réseau et/ou des services pendant toute période donnée. Dès lors que la sécurité nationale est invoquée en justification à ces demandes, il y a de forte chance que des sanctions sévères soient infligées en cas de non-respect. Certains opérateurs de réseau répondent cependant avec diligence aux demandes du gouvernement en vue de minimiser l'impact potentiel que ces demandes peuvent avoir sur la liberté d'expression et le respect de la vie privée. Trois exemples peuvent être cités à cet égard :

1) Le 1er juin 2014, les autorités gouvernementales ont contacté Orange par téléphone dans l'un de ses marchés africains en lui demandant la suspension de ses services SMS dans l'ensemble du pays. Soucieux de vérifier le fondement juridique de cette demande, Orange a demandé à ce que l'ordonnance lui soit communiquée sous forme écrite. Le lendemain, les quatre opérateurs de télécommunications du pays ont reçu une ordonnance écrite, invoquant la loi concernée, signée par l'autorité compétente, et qui énonçait les sanctions en cas de non-respect. L'ordonnance a plus tard été publiée dans un journal panafricain. Les opérateurs se sont pliés à l'ordonnance par la suspension des services SMS jusqu'au 24 juillet. Orange a tiré plusieurs leçons de cet événement, notamment l'importance de la coopération entre des entreprises homologues dans leur réponse aux exigences gouvernementales qui présentent des irrégularités et que la transparence peut aider une entreprise à répondre à ces exigences. (Telecommunications Industry Dialogue, 2016. « Input to UN Rapporteur David Kaye »)

2) Chez AT&T, ces demandes sont évaluées par des employés (y compris des juristes d'AT&T et, si nécessaire, des avocats sur place familiers du droit applicable), qui ont reçu la formation nécessaire pour confirmer que les demandes émanent d'une instance compétente, placée sous autorité légale valable, et sont autrement conformes aux exigences applicables. L'entreprise rejette les demandes du gouvernement qui ne remplissent pas ces conditions. S'il y a lieu, elle cherche à faire clarifier ou à faire modifier une demande ou l'objet d'une demande du gouvernement ou d'une ordonnance du tribunal en s'adressant aux instances compétentes. Ces efforts permettent de réduire au minimum l'impact potentiel que les demandes gouvernementales pourraient avoir sur le respect de la vie privée des clients d'AT&T et leur capacité à communiquer et à accéder aux informations de leur choix. (Telecommunications Industry Dialogue, 2016. « Input to UN Rapporteur David Kaye »)

3) Les opérations d'Amérique centrale de Millicom connaissaient des conditions difficiles en matière de sécurité en 2015. Depuis l'année précédente, les autorités au Guatemala, au Salvador et au Honduras avaient promulgué des lois obligeant tous les opérateurs de télécommunications à suspendre les services ou à réduire la capacité des signaux dans les prisons et aux alentours, soupçonnant que des gangs organisés continuaient à opérer depuis l'intérieur des prisons en utilisant des appareils mobiles introduits clandestinement dans les lieux. Pour commencer, il a été demandé aux opérateurs télécom de mettre hors service les stations de base qui desservent des secteurs de grande superficie, affectant dans le même temps les populations vivant à proximité des établissements pénitentiaires tout en perturbant des activités de tous les jours, telles que l'utilisation des distributeurs automatiques de billets.

   L'entreprise a engagé un dialogue intense auprès des autorités et de ses homologues du secteur, en cherchant à trouver des solutions alternatives qui permettraient de remédier au problème sans pour autant que la population avoisinante n'en pâtisse. Ces solutions étaient des plus variées, partant de la conception d'une nouvelle couverture du réseau autour des prisons, en passant par des solutions de tiers qui fonctionnent à la manière de brouilleurs pour restreindre les signaux dans des endroits donnés, pour aller jusqu'à la réimplantation des prisons à l'écart de secteurs à forte densité de population.

   C'est à la suite de ces efforts que fin 2015, au Guatemala et au Honduras, toutes les restrictions imposées aux signaux d'appareils mobiles à l'intérieur des établissements pénitentiaires ont été appliquées de manière plus ciblée, en restreignant les effets à l'intérieur des bâtiments de la prison. (Millicom, 2016. « Law Enforcement Disclosure Report 2016 »)

Enregistrement obligatoire des cartes SIM prépayées

Le troisième domaine de la sécurité publique qui fait l'objet de nombreux débats depuis quelques années porte sur l'enregistrement obligatoire des cartes SIM prépayées. Il s'agit d'exiger des utilisateurs de présenter une pièce d'identité à l'achat d'une carte SIM prépayée (« paiement à l'utilisation ») en vue d'utiliser des services mobiles.

Il était pratique courante que les opérateurs de réseau mobile,[71] en particulier les nouveaux venus sur un marché, distribuent des cartes SIM gratuitement à tout venant. Les clients se procuraient du crédit par l'achat d'un coupon prépayé pour leur permettre d'utiliser la carte SIM et son numéro de téléphone.

Des pays ont fait valoir que cet arrangement permet aux criminels de tirer parti de l'anonymat qu'il confère pour se livrer à toute une variété d'activités illégales, par exemple en exigeant une rançon suite à un enlèvement ou pour planifier des attaques terroristes. Un tel anonymat est perçu comme offrant un moindre risque de remonter l'utilisation d'une carte SIM mobile jusqu'à son utilisateur réel. En réponse à cela, un certain nombre de pays exigent des opérateurs de réseau mobile d'enregistrer à la fois leurs clients existants et tous les clients futurs.

Lorsqu'elle a été appliquée, cette exigence a eu un certain nombre de conséquences inattendues, et notamment :

- L'exclusion d'utilisateurs dépourvus de la pièce d'identité exigée, qui souvent sont les plus pauvres et les plus vulnérables de la société, en les privant de l'accès aux services mobiles. Selon le pays et la disponibilité des pièces d'identité, il peut s'agir là d'un obstacle majeur[72]
- L'augmentation des vols d'appareils mobiles et l'émergence d'un marché noir pour les cartes SIM enregistrées frauduleusement ou volées,[73] nées du désir de certains consommateurs, notamment des criminels, de rester anonymes
- Les inquiétudes croissantes des consommateurs liées à l'accès, à la sécurité, à l'utilisation et à la conservation de leurs données personnelles, en particulier en absence de lois nationales sur la confidentialité et la liberté d'expression[74]

Étude de cas

Collaboration sectorielle

En 2012, la Commission chargée des communications d'Ouganda a annoncé que les opérateurs de réseau mobile allaient devoir bloquer toutes les cartes SIM qui n'étaient toujours pas enregistrées d'ici la date butoir du 31 août 2013.

Désireux de respecter ces délais, les opérateurs de réseau mobile Airtel et Warid ont lancé des campagnes innovantes pour inciter leurs utilisateurs à enregistrer leur carte SIM : en plus d'envoyer à leurs clients des rappels SMS de la date butoir pour l'enregistrement, ils ont également offert des minutes et des SMS gratuits à ceux qui s'enregistraient avant la date butoir. Ils ont aussi donné aux consommateurs l'option d'un enregistrement partiel, par l'envoi de leur numéro de mobile non enregistré à un numéro gratuit afin d'éviter la désactivation de leur carte SIM une fois le délai passé. Grâce à cette option, les consommateurs ont pu indiquer que leurs cartes SIM étaient actives et ont obtenu en retour plus de temps pour s'enregistrer en personne, même s'ils avaient manqué la date butoir.
(GSMA, 2013. « Enregistrement obligatoire des utilisateurs de cartes SIM prépayées : Livre blanc »)

71. Par « Enregistrement de l'utilisateur », les opérateurs de réseau mobile incluent les autres opérateurs qui fournissent des services de communication sans fil sans pour autant être propriétaires du réseau, tels que les opérateurs de réseaux virtuels mobiles (ORVM) et les opérateurs mobiles sous licence autre (MOLO)
72. GSMA, 2016. « Enregistrement obligatoire des utilisateurs de cartes SIM prépayées : Répondre aux défis par les bonnes pratiques »
73. GSMA, 2013. « Enregistrement obligatoire des utilisateurs de cartes SIM prépayées »
74. Ibid.

Un nombre croissant de pays ont introduit l'enregistrement obligatoire des utilisateurs de cartes SIM prépayées, essentiellement dans le but de lutter contre le terrorisme et d'améliorer la répression.[75] Or à ce jour, il n'existe aucune preuve empirique ni lien direct entre l'enregistrement obligatoire de la carte SIM et la baisse de la criminalité.[76] Malgré cette absence de toute preuve empirique, de nombreux pays restent convaincus que l'enregistrement obligatoire des cartes SIM contribue à la lutte contre la criminalité et le terrorisme. En règle générale, lorsque l'obligation d'enregistrer les utilisateurs de carte SIM prépayée est en place, c'est aux opérateurs de réseau mobile qu'il revient d'en assumer les coûts. Ceux-ci peuvent se révéler élevés et entraver la capacité des opérateurs de réseau mobile d'investir dans des services destinés aux clients qui dépensent moins. Plusieurs pays, y compris le Royaume-Uni, ont étudié[77] ces programmes dans le détail et en ont conclu que les coûts pour la société (en termes de fardeau bureaucratique et sous la forme de bases de données d'enregistrement) l'emportent sur les avantages et ont décidé de ne pas adopter cette politique. Il s'agit là de décisions nationales qui dépendent certes des circonstances propres à chaque pays, mais aussi parfois des problèmes auxquels l'enregistrement cherche à remédier.[78]

L'enregistrement de la carte SIM peut avoir comme effet positif d'offrir à de nombreux consommateurs un moyen d'accéder à des services mobiles et numériques à valeur ajoutée qui leur seraient autrement inaccessibles en tant qu'utilisateurs non enregistrés (tels que des services d'argent mobile, d'identité numérique et d'e-gouvernement). Afin de faciliter ces avantages et de créer des résultats positifs pour les consommateurs, les opérateurs de réseau mobile et les pouvoirs publics doivent en échange offrir des services qui incitent les clients à s'enregistrer volontairement.

Il est important de ne pas confondre les effets préjudiciables involontaires d'une politique d'enregistrement obligatoire dans un pays donné avec les avantages potentiels que l'enregistrement volontaire de la carte SIM peut offrir à des particuliers. Aucun de ces avantages et de ces résultats positifs ne découle d'une obligation imposée par l'État d'enregistrer la carte SIM. Au lieu de cela, ils peuvent être atteints par l'enregistrement volontaire des clients qui choisissent d'enregistrer leur carte SIM prépayée afin d'accéder à des services qu'ils jugent utiles, qu'il s'agisse d'argent mobile, de commerce mobile ou de services d'e-gouvernement. Ceci dit, l'enregistrement volontaire nécessite toujours que ces consommateurs soient munis d'une pièce d'identité.

Étude de cas

Des solutions de rechange à l'enregistrement : le Mexique

En 2009, le Mexique a institué la règle de l'enregistrement obligatoire des cartes SIM (« RENAUT ») dans l'objectif principal de lutter contre les activités criminelles.

Lorsque les règles « RENAUT » sont entrées en vigueur, plusieurs préoccupations subsistaient quant au respect de la vie privée et à la sécurité des données, et au problème posé par l'enregistrement d'une grande partie de la population dépourvue de pièces d'identité officielles. La solution avait aussi pour effet de ne pas s'attaquer à la cause des activités criminelles et a entraîné une augmentation des vols d'appareils.

Après consultation avec l'industrie, des universitaires et des ONG, le programme d'enregistrement RENAUT a été suspendu en 2012. La base de données a été mise hors service et les investissements financiers importants engagés par tous les opérateurs de réseau mobile et par les autorités ont été passés par pertes et profits. La loi sur les télécommunications et la radiodiffusion, en vigueur depuis 2014, prévoit un autre type de programme afin de s'attaquer à la situation unique du marché mexicain.

Cette nouvelle loi, aux côtés d'autres dispositions réglementaires, n'exige pas la fourniture de la part de l'utilisateur de détails d'enregistrement pour utiliser des services prépayés. La loi s'attache plutôt à tirer parti de la série d'obligations imposées aux opérateurs de réseau mobile (par ex. interceptions licites) pour aider les pouvoirs publics et les services de sécurité à lutter contre les activités criminelles. (GSMA, 2016. « Enregistrement obligatoire des utilisateurs de cartes SIM prépayées : Répondre aux défis par les bonnes pratiques »)

5

75. GSMA, 2016. « Manuel des politiques de communications mobiles : Enregistrement obligatoire des cartes SIM prépayées »
76. GSMA, 2016. « Enregistrement obligatoire des utilisateurs de cartes SIM prépayées : Répondre aux défis par les bonnes pratiques »
77. Lord West of Spithead en réponse à une question parlementaire du vicomte Waverley sur l'enregistrement obligatoire des utilisateurs de carte SIM : https://www.theyworkforyou.com/wrans/?id=2007-07-16b.4.3&s=%22pay+as+you+go%22+mobile+phones
78. GSMA, 2016. « Enregistrement obligatoire des utilisateurs de cartes SIM prépayées : Répondre aux défis par les bonnes pratiques »

Quand l'enregistrement de la carte SIM est décrété obligatoire, il convient d'aviser les clients existants de la nécessité d'enregistrer leur carte SIM, des modalités à suivre et des conséquences de leur éventuel manquement à le faire (par ex. risque de désactivation de leur carte SIM en cas de non-enregistrement). Dans ce cas-là, l'obligation d'enregistrement de la carte SIM doit être mise en œuvre de façon pragmatique qui tient compte des circonstances du marché local. Plusieurs facteurs peuvent jouer sur le marché local, et notamment dans quelle mesure l'accès par les citoyens à des pièces d'identité est répandu, si l'État conserve ou non des registres à jour de l'identité de ses citoyens et si les opérateurs de réseau mobile sont en mesure de vérifier les pièces d'identité de leurs clients.

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Malgré les avantages potentiels pour les clients et les citoyens de la mise en place de l'enregistrement obligatoire par les utilisateurs de leur carte SIM prépayée, il est préférable d'en supprimer l'aspect obligatoire. Dès lors que la décision est prise de rendre obligatoire l'enregistrement des utilisateurs de carte SIM prépayée, les États devraient prendre en compte les meilleures pratiques à l'échelle mondiale et imposer des modalités d'enregistrement souples, proportionnelles et adaptées au marché concerné, y compris quant au niveau de pénétration des pièces d'identité officielles sur le marché concerné.[79]

Si ces conditions sont satisfaites l'enregistrement de la carte SIMM aura plus de chances d'être efficace et d'aboutir à des registres de clients plus exacts. En outre, un système robuste de vérification et d'authentification des consommateurs peut permettre aux opérateurs de réseau mobile de faciliter la création de solutions d'identité numérique, et de donner ainsi les moyens aux consommateurs d'accéder à une variété de services mobiles et non-mobiles. Compte tenu des grandes bases de clients existantes dans tous les pays, il est nécessaire d'accorder une attention particulière à l'ampleur de la tâche et de réfléchir au temps qu'il faudra aux utilisateurs pour s'enregistrer, afin de minimiser le fardeau imposé aux clients et le risque de perturbation éventuelle des services.

La GSMA exhorte les États qui envisagent d'introduire ou de réviser des règles d'enregistrement obligatoire de la carte SIM de prendre les mesures suivantes avant de finaliser leurs plans :

- Consulter, collaborer et communiquer avec les opérateurs de réseau mobile avant, pendant et après l'exercice de mise en œuvre
- Trouver le juste équilibre entre les exigences de sécurité nationale et celles de protection des droits des citoyens, surtout si l'État impose l'enregistrement de la carte SIM pour des raisons de sécurité
- Veiller à la présence de mesures adéquates de sauvegarde de la vie privée et une surveillance juridique efficace pour protéger les données et la vie privée des clients
- Fixer des délais réalistes pour les procédures de conception, de mise à l'épreuve, de mise en œuvre et d'enregistrement
- Avant toute mise en œuvre, définir des obligations claires et certaines en matière d'enregistrement
- Autoriser/encourager le stockage de documents électroniques et la conception de modalités d'enregistrement administrativement « légères »
- Autoriser/encourager le client enregistré par carte SIM à accéder à d'autres services mobiles et numériques à valeur ajoutée
- Soutenir les opérateurs de réseau mobile dans la mise en œuvre de programmes d'enregistrement de la carte SIM en contribuant à des activités de communication communes et à leurs coûts opérationnels

79. GSMA, 2016. « Manuel des politiques de communications mobiles : Enregistrement obligatoire des cartes SIM prépayées »

Pour approfondir

L'enregistrement dans le cadre de partenariats public-privé en Amérique latine

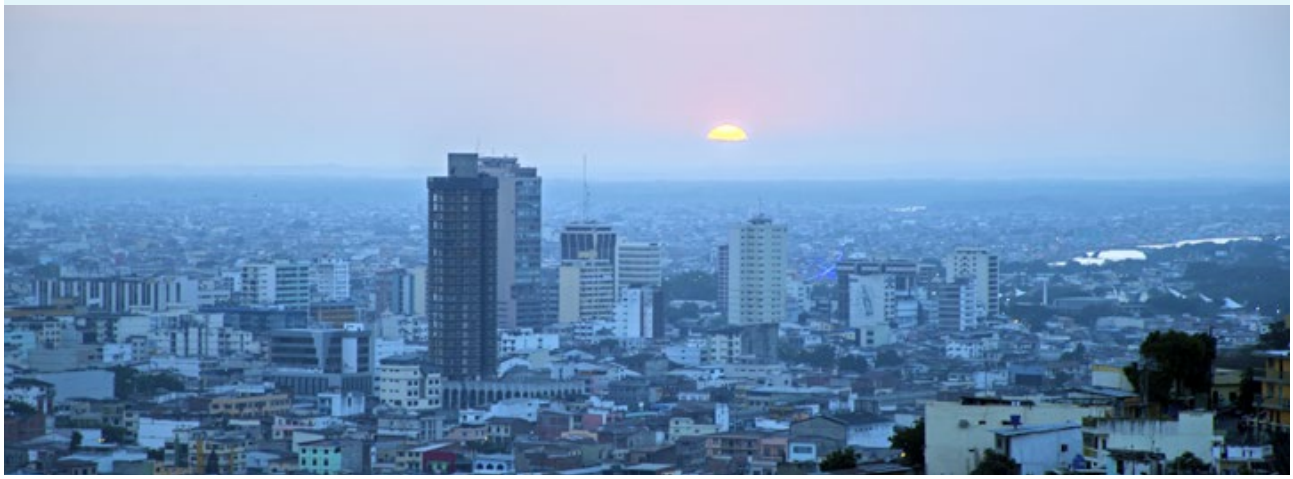
Durant l'année 2009 en Équateur et en décembre 2016 en Argentine, les autorités réglementaires nationales (CONATEL dans le premier cas et ENACOM dans le deuxième) ont demandé le recoupement et la validation de la procédure d'enregistrement des cartes SIM de tous les consommateurs par rapport à un registre d'identité public ou privé. Dans chaque cas, Telefónica a collaboré étroitement avec les pouvoirs publics pour le déploiement d'une solution adaptée aux consommateurs, à l'État et à leurs propres besoins.

En Équateur, Telefónica a mis en place la procédure d'enregistrement au moyen d'un système automatisé appelé « Interactive Voice Response » (IVR). Le service vocal était une amélioration par rapport à la procédure précédente, qui nécessitait le recoupement de l'identité du consommateur avec le « Registro Civil ».

En Argentine, Telefónica a mis au point une application qui se déclenche dès lors qu'une carte SIM est insérée dans l'appareil mobile. Cette application sert à collecter les informations de la carte SIM ainsi que l'identifiant personnel de l'utilisateur mobile. Ce système numérique est utilisé pour créer une base de données qui établit le lien unique qui existe entre le propriétaire de la carte SIM et celui de l'appareil mobile.

Telefónica a retenu de ces expériences de travail en partenariat avec les autorités nationales les trois principaux enseignements suivants :

1. Il existe plusieurs façons de valider le processus d'enregistrement de la carte SIM. Il revient aux opérateurs de réseau mobile d'élaborer celui qu'ils jugent le plus approprié
2. Le respect du calendrier est essentiel à la réussite de la mise en œuvre. Par exemple, en Équateur, les opérateurs de réseau mobile et le régulateur ont travaillé de concert pour mettre en œuvre une « phase statistique » qui a permis d'analyser les besoins véritables afin d'éviter une réglementation excessive
3. Un partenariat et une collaboration étroits public-privé entre les opérateurs de réseau mobile et les pouvoirs publics s'imposent pour envisager les diverses options de mise en œuvre et élaborer celle qui répond le mieux aux besoins de toutes les parties prenantes de manière équilibrée



5

6 Protection de la sécurité des réseaux et de l'intégrité des appareils

La sécurité de l'infrastructure de réseau sous-tend l'utilisation sûre et sécurisée des services mobiles. Dans sa forme la plus simple, cela signifie que les opérateurs de réseau mobile préservent l'intégrité des communications sur l'ensemble du réseau en sécurisant les actifs critiques (matériels, logiciels et données) et en empêchent tout accès ou intrusion non autorisés dans les nœuds ou les liens qui composent leurs réseaux. Du fait que l'appareil mobile de l'utilisateur final constitue le principal point d'accès au réseau du point de vue de l'utilisateur, la protection de l'intégrité des appareils mobiles est récemment apparue comme une exigence essentielle qui vient s'ajouter aux autres. Par nécessité, les réseaux mobiles sont accessibles à un très large éventail d'utilisateurs, en passant par toute une variété d'appareils et de protocoles de connexion. Ils doivent aussi s'interconnecter avec de nombreux autres réseaux de communications dans le monde (fixes, mobiles, de fournisseurs de services internet et d'entreprise) afin d'offrir la fonctionnalité des réseaux modernes : « n'importe où, n'importe quand ». Par conséquent, la protection des réseaux et des appareils est extrêmement complexe dans la pratique.

À l'origine, l'infrastructure du réseau de télécommunications a été conçue comme un système sécurisé en boucle fermée. Aux points d'interconnexion des réseaux, comme aux frontières nationales (généralement, les premiers opérateurs de réseau dans la plupart des pays étaient des monopoles d'État), la sécurité était assurée sur une base de transparence et de confiance mutuelles. Depuis, ces réseaux se sont multipliés et ont évolué à mesure que le monde est devenu de plus en plus interconnecté et que les technologies ont progressé. Aujourd'hui, il y a de fortes chances que tout appel téléphonique ou toute transmission de données emprunte de nombreux réseaux et, dans le cas des données, une série de chemins d'accès, le tout dans le cadre d'une seule et même communication. C'est en conséquence de cela que toute une série de vulnérabilités potentielles est apparue, exigeant de la part de tous les opérateurs de réseau et du secteur entier de faire preuve de grande vigilance et d'y remédier.

La Figure 6 résume une série de menaces susceptibles de nuire à l'intégrité des réseaux en raison des risques d'interceptions non autorisées, d'emprunt d'identité ou d'interruption de service qui existent. L'approche du secteur mobile à faire face à ces menaces s'appuie sur trois axes : (i) renforcement des mesures et des procédures de sécurité, (ii) promotion d'un débat transparent sur le juste équilibre à trouver entre commodité et sécurité, et (iii) intégration de fonctionnalités de sécurité toujours plus sophistiquées dans les normes et les protocoles techniques à mesure que chaque nouvelle génération de réseau mobile est développée et déployée.

Cette section du rapport aborde un certain nombre d'enjeux concernant la sécurité affectant les réseaux et les appareils et qui pourraient potentiellement compromettre la sécurité nécessaire pour faire en sorte que les communications des clients demeurent sûres et sécurisées :

- Sécurisation du réseau
- Intégrité des appareils mobiles
- Développements des réseaux du futur

Chacun de ces enjeux présente des implications importantes pour les pouvoirs publics, l'industrie et d'autres parties prenantes, et ils sont également abordés dans plus de détail plus loin dans ce chapitre.

Protection de la sécurité des réseaux et de l'intégrité des appareils

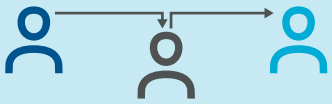
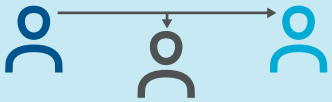
Les acteurs du secteur doivent travailler ensemble et de conserve avec les services de sûreté internationaux pour partager des renseignements sur les menaces qui existent, afin de contrer les attaques malveillantes perpétrées sur des réseaux et des appareils mobiles et d'en identifier les auteurs. Il s'agit pour cela de solliciter la participation des équipes existantes d'intervention en cas d'incident de sécurité et au besoin d'en créer de nouvelles pour combler les lacunes éventuelles. Les règlements, quand nécessaires, doivent s'appliquer de manière cohérente entre tous les prestataires de la chaîne de valeur, d'une manière neutre sur le plan du service et de la technologie, tout en préservant le modèle multipartite pour la gouvernance de l'Internet et en lui permettant d'évoluer. C'est dans cette démarche que la GSMA et les opérateurs de mobile qui en sont membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures pour protéger l'infrastructure sous-jacente et veiller à ce que nous apportions aux consommateurs le service de communication le plus sûr et le plus fiable, et ce comme suit :

- **Prendre des mesures pour sécuriser l'infrastructure de réseau que nous exploitons et contrôlons**
- **Promouvoir le partenariat public-privé afin de minimiser les risques soit de piratage, soit d'exploitation du réseau à des fins malveillantes par des approches mondiales et coordonnées**
- **Stipuler clairement la responsabilité qui incombe aux opérateurs vis-à-vis des infrastructures et la démarcation des limites avec d'autres infrastructures ou services**

Figure 6

Protection des réseaux

OBJECTIF DE SAUVEGARDE	DESCRIPTION DE LA MENACE	EXEMPLE D'ATTAQUE
INTÉGRITÉ – ÉVITER LA MODIFICATION DES DONNÉES	ALTÉRATION NON AUTORISÉE	INTERMÉDIAIRE 
CONFIDENTIALITÉ – PROTÉGER LES DONNÉES PRIVÉES	ACCÈS NON AUTORISÉ	ÉCOUTES 
DISPONIBILITÉ – MAINTENIR LE RÉSEAU ET LES DONNÉES À LA DISPOSITION D'UTILISATEURS LÉGITIMES	DESTRUCTION, VOL, SUPPRESSION OU PERTE DE DONNÉES, OU MISE HORS SERVICE DE RÉSEAUX	DÉNI DE SERVICE 

Sécurité du réseau

Infrastructure physique du réseau

La première étape dans la sécurisation des réseaux mobiles repose sur l'infrastructure physique à proprement parler : les sites de micro cellules, les actifs de transmission sur réseaux secondaires et ceux du cœur de réseau. Par exemple, tout réseau abrite des fonctions clés, tels que le registre des utilisateurs autorisés, qu'il est indispensable de sécuriser car elles représentent des points de vulnérabilité, que ce soit sujet à des attaques malveillantes ou à des défaillances techniques. Les opérateurs de réseau mobile et les fournisseurs d'équipement ne cessent d'élaborer et de déployer de nouvelles solutions pour les rendre plus robustes, et leurs efforts ont largement porté leurs fruits à ce jour, néanmoins ceux-ci requièrent des investissements continus dans la mise au point et le déploiement de nouvelles fonctions et fonctionnalités.

Le recours à des stations de base factices, ou des « catchers » IMSI (identité internationale d'abonné mobile), représente une vulnérabilité en l'absence d'authentification mutuelle sur les technologies 2G et de fonctionnalité capable de configurer automatiquement les appareils 3G et 4G à utiliser sur le réseau 2G. Les stations de base factices trompent les appareils mobiles qui se trouvent à portée pour qu'ils se connectent à elles plutôt qu'au réseau réel, vers lequel l'opérateur de la station de base factice peut relayer l'appel dans un deuxième temps. Une telle attaque dite de type « intermédiaire » soulève tout un éventail de risques d'interception, de géolocalisation, de déni de service et de fraude. Les législateurs, tels que ceux qui siègent au comité américain sur la réforme et la surveillance du gouvernement, sont actuellement en train d'élaborer des recommandations visant à empêcher l'utilisation non autorisée de ces appareils.[80] Les opérateurs de réseau mobile peuvent déployer des mesures standard de réseau et de sécurité pour aider à atténuer ce risque et la GSMA a élaboré des orientations allant dans ce sens en vue d'aider les opérateurs.

Les communications sur le réseau

Les technologies utilisées au sein des réseaux mobiles sont régulièrement mises à jour avec les dernières améliorations déployées de manière planifiée. Des niveaux élevés d'investissements dans de nouvelles infrastructures, et ce de manière périodique, ont beaucoup contribué à faire en sorte que l'infrastructure de réseau soit la plus raisonnablement robuste. Le maintien de la sécurité va de plus en plus reposer sur la nécessité de préserver la confiance dans cette capacité à investir, alors que les dispositions législatives et réglementaires changent en réponse à des menaces en constante évolution.

Le lancement des réseaux de deuxième génération (2G) en 1991 a introduit l'utilisation de la modulation numérique qui a permis la mise en œuvre d'une protection et d'une sécurité robustes. La norme GSM, qui sous-tend un grand nombre de réseaux 2G, utilise la technologie SIM (Subscriber Identity Module) pour authentifier un utilisateur à des fins d'identification et de facturation, et à l'appui du chiffrement par l'appareil afin de se protéger contre des attaques, d'interception par exemple. Le concept du SIM physique, qui reposait sur la technologie de la carte à puce, s'est avéré remarquablement robuste et continue d'être un élément essentiel des réseaux 4G aujourd'hui. Il va continuer d'en être ainsi à l'avenir grâce à des innovations telles que la carte SIM embarquée.[81]

Les réseaux 2G ont été principalement conçus pour prendre en charge les communications sur appel vocal, mais elles comportaient aussi des capacités de transmission de données de base, tout en introduisant également le service populaire de messages texte SMS. Les réseaux 3G, lancés au début des années 2000, ont été les premiers à intégrer à titre de capacité élémentaire la transmission de données, à introduire la navigation sur Internet en quasi haut débit et à intégrer les multimédias, tout en introduisant des fonctionnalités de sécurité supplémentaires.

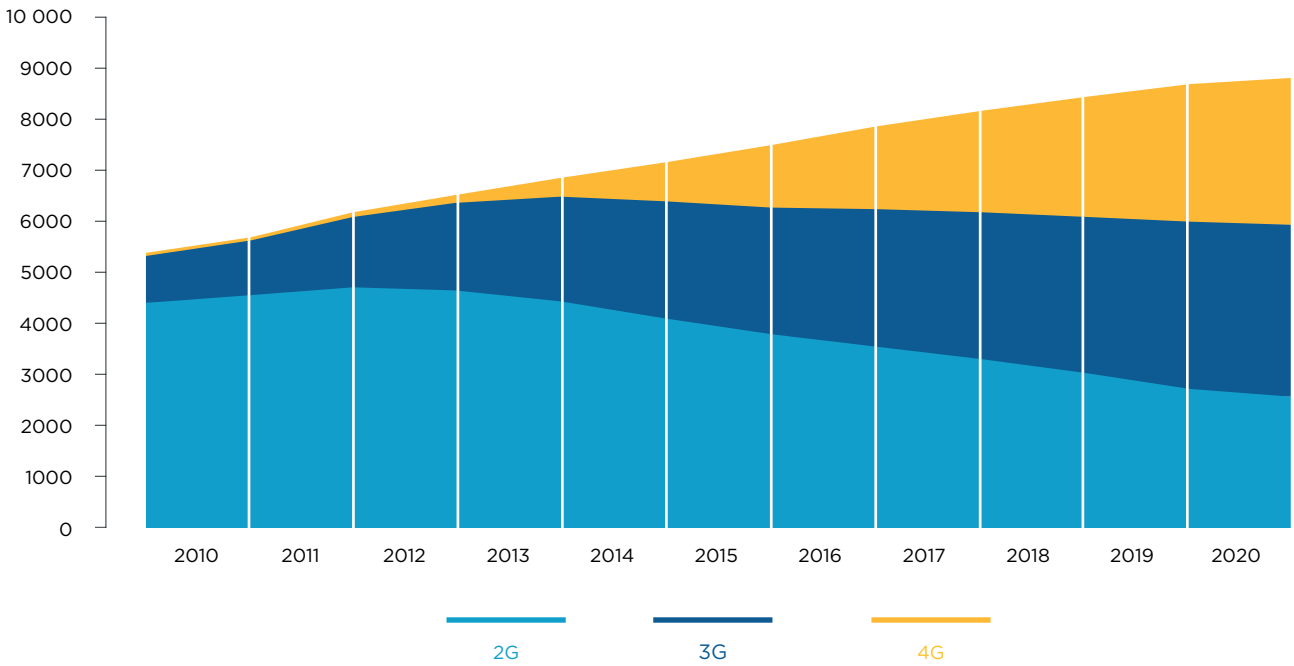
80. Committee on Oversight and Government Reform, 2016. « Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations »
81. La carte SIM embarquée est une puce installée dans des appareils mobiles qui procure le même niveau de sécurité que l'actuelle technologie SIM. Elle apporte une plus grande souplesse en permettant de télécharger les profils des opérateurs, afin que les utilisateurs puissent changer de fournisseur sans avoir besoin de changer la puce physique. Il s'agit là d'une fonction particulièrement utile pour les appareils de machine-à-machine (M2M). Voir : http://www.gsma.com/newsroom/press-release/leading-m2m-alliances-back-the-gsma-embedded-sim/

Néanmoins, les faiblesses de sécurité au niveau du protocole défini par l'UIT SS7 (Signalling System Number 7), ainsi que d'autres protocoles d'interconnexion qui sont utilisés pour acheminer des appels vocaux et des services de support entre et à travers des réseaux, sont autant de facteurs susceptibles d'exposer les réseaux mobiles et leurs clients à un éventail de vulnérabilités, notamment en matière d'écoute, de géolocalisation ou d'interception des données. Il existe des capacités de surveillance, de détection et de blocage pour atténuer les menaces sur les protocoles d'interconnexion et la messagerie. La GSMA reconnaît la nécessité d'une réponse exhaustive et collective de la part des opérateurs de réseau mobile en vue d'atténuer ces risques. Le Groupe Fraude et Sécurité de la GSMA a entrepris des travaux importants visant à fournir des conseils aux opérateurs de réseau sur la manière d'atténuer les risques de sécurité SS7.[82] Les opérateurs se doivent en outre de prendre toutes les précautions nécessaires pour se protéger contre l'interception de données sensibles, y compris les détails d'identification d'abonnés.

La quatrième génération de normes de communication mobile (4G) offre l'accès en haut débit mobile aux smartphones et à d'autres appareils. L'adoption de réseaux sans fil 4G (voir Figure 7) a introduit le passage au protocole all-IP qui résout la vulnérabilité de SS7 dès lors qu'il est mis en œuvre entre les opérateurs, néanmoins l'adoption de nouveaux protocoles peut en soi créer de nouveaux problèmes de sécurité. Il est possible de minimiser l'exploitation des vulnérabilités présentes sur ces réseaux en veillant au déploiement et à la configuration corrects de fonctions de sécurité qui sont inhérentes aux normes ; la GSMA peut donner des conseils sur la meilleure façon d'y parvenir.

Figure 7

Connexions mondiales par technologie (en millions, sauf M2M)



82. Pour en savoir plus, voir : http://www.gsma.com/newsroom/all-documents/ir-70-sms-ss7-fraud/

Une des difficultés signalées fréquemment en termes de communication a trait aux GSM-Gateways, ou « Boîtes de SIM » comme on les appelle communément. Les Gateways GSM peuvent permettre à des tiers non autorisés d'interférer avec l'acheminement des appels entre les réseaux mobiles et leurs clients, et cela peut présenter des problèmes en termes de sûreté et de sécurité. La fonction de l'appel identité (CLI) n'est généralement pas prise en charge par les GSM-Gateways de sorte que les services qui dépendent de la fonction CLI ne sont plus disponibles aux utilisateurs vers lesquels le trafic a été acheminé par des GSM-Gateways (par ex. le service peut être refusé aux utilisateurs de services prépayés qui doivent faire l'appoint de leurs niveaux de crédit). L'absence de fonction CLI peut aussi avoir des implications quant aux interceptions licites et aux obligations légales auxquelles les opérateurs de réseau doivent se soumettre pour venir à l'appui des services de sûreté sur leurs marchés sous licence. En raison des impacts sur la disponibilité du service et la sécurité générale, l'utilisation de GSM-Gateways est illégale dans certains pays. Là où elle est autorisée, les opérateurs de réseau mobile sont incités à mettre en œuvre des mesures visant à empêcher l'utilisation de gateways par des transporteurs tiers.

Alors que les opérateurs de réseau mobile continuent d'atténuer les menaces posées à leur réseau et à leurs consommateurs, il est important de noter que l'on s'attendrait à une démarche similaire de la part des opérateurs de réseaux publics sans fil, tels que les « points actifs wifi » publics ou les connexions wifi dans les hôtels. Il revient aux opérateurs de ces réseaux et à leurs clients de déployer des mesures de protection appropriées (par ex., des réseaux privés virtuels) pour aider à sécuriser l'écosystème de communications pris dans son ensemble.

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

Bien qu'aucune technologie de sécurité ne soit garantie infaillible, les attaques perpétrées sur des réseaux et services GSM sont rares, car elles nécessiteraient des ressources considérables notamment un équipement spécialisé, en puissance de traitement informatique et en expertise technique qui dépasse les aptitudes de la plupart des gens ou des organisations.[83]

Les obstacles pour empêcher toute atteinte à la sécurité des communications mobiles ont été placés très haut et d'après la GSMA, les recherches effectuées sur les éventuelles vulnérabilités qui existent ont généralement été de très haut niveau.[84] Ceci dit, l'évolution du paysage technologique et l'émergence de nouvelles menaces et de nouvelles sources d'attaque requièrent l'adoption par le secteur d'une approche encore plus proactive à la protection des réseaux à l'avenir :

- Il est important que le secteur mobile veille à la mise en place des mécanismes, des outils et des opportunités adéquats pour faciliter le partage de l'information sur les menaces et les attaques qui existent, tout en s'assurant de la rapide diffusion des informations en réponse aux incidents. Une initiative de la sorte pourrait solliciter la participation des régulateurs et d'autres instances gouvernementales, comme des équipes de « Computer Emergency Response Teams » (CERT) sur le plan national
- Une action collective de la part du secteur entier est nécessaire pour protéger les réseaux et les consommateurs connectés en adoptant une approche de cohérence et de consensus dans l'élaboration de normes, et par l'emploi proportionné de capacités de surveillance, de détection et de blocage
- La sécurisation des réseaux et services mobiles est une tâche complexe. Elle nécessite que les opérateurs de réseau mobile et leurs fournisseurs prennent une multitude de décisions pour veiller à la bonne mise en œuvre des normes de sécurité, et au déploiement et à la configuration de tout un éventail de fonctionnalités. La GSMA offre à ses membres des conseils et des orientations quant à la manière de parvenir à des niveaux de sécurité optimale, et elle continue de travailler à la définition des exigences de sécurité de référence auxquelles tous les opérateurs de réseau mobile devront s'engager
- Les problèmes de sécurité persistants ne vont faire que s'intensifier avec l'évolution de la 5G, mais celle-ci présente aussi l'occasion de repenser la sécurité et la manière dont elle peut être assurée

Les règlements, quand nécessaires, doivent s'appliquer de manière cohérente entre tous les prestataires de la chaîne de valeur, d'une manière neutre sur le plan du service et de la technologie, tout en préservant le modèle multipartite pour la gouvernance de l'Internet et en lui permettant d'évoluer.

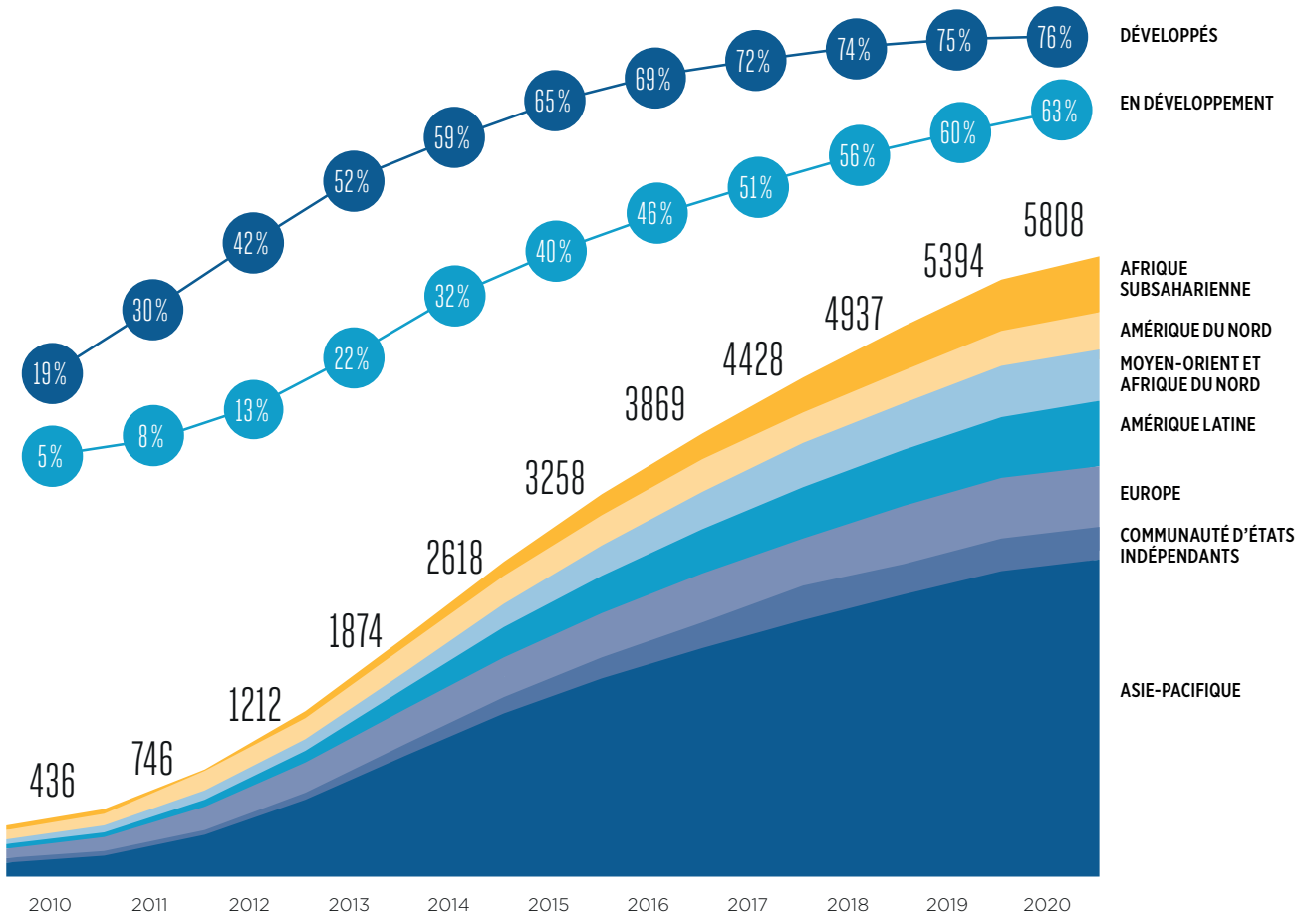
83. GSMA, 2016. « Manuel des politiques de communications mobiles : Sécurité des communications mobiles »
84. Ibid.

Intégrité des appareils mobiles

À mesure du déploiement des réseaux 3G, 4G et, à l'avenir, 5G, l'adoption et l'utilisation d'appareils mobiles de type smartphones n'ont fait que s'accroître. Il est prévu que d'ici 2020, deux connexions sur trois dans les marchés émergents, et trois connexions sur quatre dans les marchés développés, seront des connexions sur smartphone (voir Figure 8). Les fournisseurs d'applications sont en train de réfléchir à la manière dont les smartphones, éventuellement au moyen de modules enfichables, peuvent remplacer des appareils dédiés en vue de les utiliser dans des hotspots ou dans d'autres milieux hautement sensibles. De plus, on s'attend à enregistrer au moins un milliard de connexions machine-à-machine (M2M) d'ici à 2020, avec toutes les répercussions qu'elles pourront avoir sur les foyers, les usines, transports, etc., et à ce qu'elles représentent au moins 10 % du marché mobile mondial.[85]

Figure 8

Connexions et adoption mondiales du smartphone (millions)



85. GSMA, 2014. « Cellular M2M forecast and assumptions: 2010–2020 »

Parallèlement aux opportunités offertes aux consommateurs et aux entreprises d'utiliser ces services, il existe le risque que la mauvaise gestion de ces appareils crée des vulnérabilités qui ouvrent la voie à de potentielles infractions de réseaux et des impacts sur un ensemble plus large d'utilisateurs.

Les attaques menaçant la sécurité concernent toutes les formes de technologies, y compris celles du mobile. Les appareils mobiles sont ciblés pour toutes sortes de raisons. Comme objet attrayant pour les voleurs (en raison de leur valeur relativement élevée et de leur petite taille), les bandes organisées cherchent souvent à changer le numéro IEMI[86] IMEI d'un mobile volé afin de le réactiver après que son vol ait été déclaré. D'autres criminels ont recours à des malware (logiciels malveillants) aux fonctions potentiellement préjudiciables pour les utilisateurs, généralement par des moyens d'usurpation d'identité et de fraude s'y rapportant.[87]

La menace sans doute la plus grave est celle d'une attaque perpétrée à grande échelle, préméditée et systématique, visant à rendre tout un réseau inopérant, affectant tous les utilisateurs. Il y a le risque que les infractions d'appareils mobiles (par ex. des logiciels malveillants envoyés dans des e-mails de phishing) servent de point d'entrée pour se propager à d'autres appareils connectés, avant d'être exploitées pour attaquer des réseaux basés sur IP. Par exemple, l'attaque du 21 octobre 2016 à l'encontre d'un dispositif de commande majeur de l'infrastructure du système de noms de domaine, Dyn,[88] provenait d'un logiciel malveillant situé sur un ordinateur qui s'était propagé à d'autres appareils, créant ainsi un « botnet » qui a ensuite été utilisé pour lancer une attaque DDoS (déni de service distribué).[89] Sur une échelle encore plus grande, il est possible d'imaginer une approche similaire qui viendrait inonder un réseau mobile basé sur IP avec un trafic qui viendrait à le submerger à tel point qu'il en deviendrait inutilisable. La prévention de ce type d'attaques nécessite une étroite coopération entre les opérateurs de réseau mobile et les services de sûreté nationaux, s'inscrivant dans le cadre d'un plan global de sécurité : en effet, l'attaque de réseaux mobiles n'est qu'un moyen d'attaque parmi d'autres à la disposition de parties hostiles.

La GSMA a contribué à l'élaboration de mécanismes de protection tels que ceux décrits dans les Lignes directrices de la GSMA pour l'efficacité des connexions IoT[90] afin de protéger les réseaux mobiles du déploiement de masse d'appareils IoT inefficaces, précaires ou défectueux. En outre, la GSMA encourage ses membres à offrir des correctifs d'appareils critiques à la sécurité dans les délais les plus raisonnables et les plus brefs possibles.

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

L'adoption par les fournisseurs du secteur de bonnes pratiques et politiques en matière de sécurité est absolument fondamentale. Des programmes tels que le régime d'agrément de sécurité de la GSMA,[91] qui prévoit la certification des fournisseurs, servent à garantir et à attester la démarche qui encourage un engagement envers des niveaux de sécurité. La GSMA veille depuis quelque temps déjà à l'assurance en matière de sécurité des fournisseurs et de leurs produits dans le cadre du régime d'agrément de sécurité pour les fournisseurs de SIM et par l'actuelle élaboration d'un programme destiné aux équipementiers (OEM) d'infrastructures.

La GSMA cherche aussi à obtenir le soutien de fournisseurs de services Internet ou de développeurs d'applications qui opèrent sur le réseau et qui sont tenus de rendre des comptes de leurs mesures visant à se protéger d'être utilisés comme brèche pour porter atteinte à l'intégrité d'un réseau mobile.

La GSMA apporte son soutien aux normes de sécurité mondiales pour les services émergents et reconnaît le rôle que peuvent jouer les éléments sécurisés basés sur carte SIM, comme alternative à l'intégration de fonctions sécuritaires à l'intérieur de l'appareil mobile ou sur une carte numérique externe (carte microSD), compte tenu de la résilience avérée de la carte SIM à résister aux attaques.[92]

6

86. Les questions relatives au numéro IMEI et au vol d'appareils mobiles sont abordées plus en détail à la Section 3. Protection du consommateur
87. Ces questions sont abordées dans plus de détail au chapitre intitulé « Protection du consommateur »
88. Dyn est un fournisseur du système de noms de domaine (DSN) pour des fournisseurs de services Internet comprenant Twitter, Amazon, AirBnB et Spotify. L'organisation a pu restaurer leurs services après chaque attaque tout en évitant une interruption du système entier, et se parer d'une troisième attaque sans impact sur les consommateurs. Pour prendre connaissance de sa déclaration publique, voir : http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
89. USA Today, 2016. « Hacked home device caused massive Internet outage »
90. Pour en savoir plus, voir : http://www.gsma.com/connectedliving/gsma-iot-device-connection-efficiency-guidelines/
91. Pour en savoir plus, voir : http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/security-accreditation-scheme
92. GSMA, 2016. « Manuel des politiques de communications mobiles : Sécurité des communications mobiles »

Développements des réseaux du futur

L'Internet des objets (IoT) constitue un vaste ensemble de développements qui impliquent la connexion de tout un ensemble de nouveaux appareils à Internet, en partant des voitures jusqu'à des appareils ménagers connectés. Ces appareils se connecteront à un éventail de réseaux, y compris des réseaux wifi, des réseaux dédiés de faible puissance, ainsi que des réseaux mobiles, en utilisant du spectre à la fois sous licence et sans licence. La prochaine génération de technologies pour les réseaux mobiles (qu'il s'agisse de la technologie NFV, de virtualisation de fonctions de réseau, et de la 5G, par exemple), assurera une partie de la connectivité de l'IoT. Elle inaugurera une ère nouvelle de haut débit mobile encore plus rapide et ouvrira la voie à des services optimisés par la 5G. Ces services optimisés peuvent inclure le support à des technologies de pointe, telles que l'Internet tactile, la réalité virtuelle et des services de radiodiffusion améliorés.

Sécuriser l'Internet des objets

L'IoT présente un potentiel de croissance phénoménal pour le secteur mobile et pour bien d'autres. Avec la venue de nouveaux partenaires commerciaux et de nouveaux fournisseurs, il est essentiel que la sécurité figure au tout premier rang des préoccupations de ceux qui entrent dans cet espace commercial. Beaucoup d'appareils et d'équipements qui, jusque-là, n'ont jamais été connectés à la moindre forme de réseau, vont devoir comporter des dispositifs de sécurité adéquats dont l'intégration dans les équipements et les services devra être conçue dès le départ. Pour cela, les fournisseurs et développeurs qui jusque-là n'ont jamais eu à se préoccuper de ce genre de questions vont devoir s'atteler à inclure sans tarder des dispositifs de sécurité aussi robustes que sophistiqués. La GSMA a publié des Lignes directrices sur la sécurité de l'IoT[93] et un programme associé d'auto-évaluation de la sécurité[94] qu'elle met à la disposition de tout un éventail d'acteurs de l'écosystème.

Des normes et protocoles 5G, y compris ceux relatifs à la sécurité du réseau, sont en train d'être élaborées spécifiquement pour cette technologie. La GSMA joue un rôle de premier ordre à cerner et prioriser les exigences et à veiller à ce qu'elles soient prises en compte et intégrées dans les nouvelles normes. Ceci dit, cette approche ne remédie qu'à un maillon de la chaîne future de l'IoT, et il sera nécessaire de déployer des efforts et une attention considérables pour assurer la sécurité des nombreux autres composants et services au sein de l'infrastructure hautement interconnectée qui feront partie de l'IoT à mesure de son évolution.

Principales implications pour les pouvoirs publics, l'industrie et les autres parties prenantes

La GSMA a l'ambition de jouer un rôle important pour aider à façonner le développement stratégique, commercial et réglementaire de l'IoT, ainsi que de l'écosystème 5G.[95]

- La GSMA reconnaît qu'elle a un rôle essentiel à jouer dans la collecte et la priorisation des exigences de sécurité de la 5G à des fins de normalisation. Des discussions sont déjà en train d'avoir lieu et la GSMA, ainsi que ses membres, sollicitent la participation d'autres experts en la matière ainsi que celle des services de sûreté pour veiller à comprendre clairement tous les besoins qui existent
- Il revient aux pouvoirs publics de donner leur appui à l'envergure mondiale des marchés des réseaux futurs et de la vaste variété d'appareils qui se connecteront à l'Internet de demain, et d'apporter leur soutien aux travaux déployés dans les pays pour assurer la cohérence et la clarté de la réglementation et des obligations en matière de sécurité des réseaux pour tous les acteurs impliqués dans ce domaine à la fois complexe et aussi en rapide mutation
- Le secteur mobile poursuivra son dialogue avec l'écosystème pris dans son ensemble et continuera à encourager des investissements appropriés, que ce soit directement ou par l'intermédiaire de fournisseurs et de partenaires de l'écosystème, en vue d'assurer la sécurisation des réseaux et des appareils à mesure que les technologies se développeront, notamment lors de la transition au NFV et à la 5G

6

93. Pour en savoir plus à propos des Lignes directrices sur la sécurité de l'IoT de la GSMA, voir http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
94. Pour en savoir plus sur le programme d'auto-évaluation de la sécurité IoT, voir http://www.gsma.com/connectedliving/iot-security-self-assessment/
95. GSMA, 2016. « Manuel des politiques de communications mobiles : 5G — La voie vers la prochaine génération »

7 Principes de sécurité, de respect de la vie privée et de sûreté du secteur mobile

Dans l'action continue de la GSMA portant sur les thèmes de la sécurité, de la protection de la vie privée et de la sûreté, la GSMA et les opérateurs qui en sont membres reconnaissent la nécessité d'adopter une approche souple et évolutive en vue de parvenir au juste équilibre entre les droits du consommateur et du citoyen, les besoins de sécurité publique et le rôle des opérateurs de réseau mobile à soutenir les uns comme les autres. Les meilleures réponses à ces enjeux tiennent compte des besoins et des variations du marché local, plutôt de se contenter de suivre une approche dogmatique. Quoi qu'il en soit, la nécessité d'un travail de collaboration et de partage des enseignements entre les différents groupes de parties prenantes ne fait pas l'ombre d'un doute.

La GSMA et ses organisations membres ont établi les principes suivants, qui orientent la manière dont elles n'ont de cesse d'élaborer des solutions aux questions soulevées dans le présent rapport.

Protection du consommateur

Des efforts multipartites doivent être déployés pour encourager une utilisation sûre et responsable sur mobile des services en ligne et d'appareils connectés. Il est particulièrement important que les pouvoirs publics et leurs services de sûreté veillent à la présence de cadres juridiques, de moyens et de processus appropriés pour empêcher, identifier et poursuivre des comportements criminels. Bien souvent, une telle démarche nécessite une coopération globale. Il incombe aussi à d'autres acteurs de l'écosystème du secteur, comme les fabricants d'appareils et les prestataires de services basés sur mobile par exemple, de participer à des initiatives visant à protéger les consommateurs lorsqu'ils utilisent des appareils et des services mobiles et à les éduquer sur l'adoption de comportements sécuritaires et de bonnes pratiques, pour qu'ils puissent continuer à bénéficier de ces services sans courir de danger. Les opérateurs de réseau mobile ont un rôle à jouer en sensibilisant les consommateurs aux dangers et en appelant à leur vigilance, et en les incitant à prendre l'ensemble complet des mesures de sécurité mises à leur disposition. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures proactives pour la protection des consommateurs en luttant contre les activités illicites et préjudiciables liées ou bien à l'utilisation du téléphone mobile ou bien aux activités que le mobile rend possibles, en adoptant les mesures suivantes :

- **Travailler en collaboration avec d'autres organismes pour offrir des solutions multilatérales**
- **Mettre en œuvre des solutions destinées à empêcher l'utilisation de réseaux à des fins d'activités frauduleuses et criminelles, et celle d'appareils en vue de nuire au consommateur**
- **Éduquer les consommateurs à des comportements sécuritaires, afin de renforcer leur confiance, lors de l'utilisation des services et des applications mobiles**

Protection de la vie privée du consommateur

La protection de la vie privée vise essentiellement à renforcer la confiance en la protection adéquate des données à caractère privé, en conformité avec la réglementation et les exigences en matière de respect de la vie privée. Pour cela, toutes les parties concernées doivent adopter une approche cohérente, neutre sur le plan technologique, et constante entre l'ensemble des services, des secteurs et des territoires. Les pouvoirs publics peuvent y contribuer en accordant la souplesse nécessaire à l'innovation, en adoptant des cadres basés sur les risques de sauvegarde des données à caractère privé, et enfin en encourageant des pratiques responsables en matière de gouvernance numérique en accord avec la réglementation locale. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures proactives afin de protéger et de respecter la vie privée des consommateurs et de leur permettre de faire des choix éclairés sur le type de données recueillies et la manière dont leurs données à caractère personnel sont utilisées, en mettant en œuvre des politiques qui encouragent :

- **Le stockage et le traitement en toute sécurité des informations à caractère personnel et privé, en conformité avec les exigences légales le cas échéant**
- **Être transparent avec les consommateurs sur les données que nous partageons sous forme anonyme et en pleine conformité avec les exigences légales**
- **La mise à disposition aux consommateurs des informations et des outils nécessaires pour faire des choix simples et significatifs au sujet de leur vie privée**

Protection de la sécurité publique

Dans le cadre des lois et des règlements, y compris des obligations de licence, et conformément à la législation locale, les opérateurs de réseau mobile sont tenus dans l'obligation d'assumer des responsabilités supplémentaires pour aider les services de sûreté dans le respect de l'objectif global de protection de la sécurité publique. Il est important que les États aient en place un cadre juridique proportionnel qui précise clairement les pouvoirs à la disposition des services de sûreté. Le cadre juridique doit également veiller au caractère nécessaire et proportionné des demandes d'assistance, en s'assurant de les adresser au fournisseur du service de communication ou de technologie le plus approprié et compatible, et dans le respect des principes des droits de l'homme. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à se conformer à l'ensemble des obligations juridiques et de licence dans leurs réponses aux préoccupations de sûreté et de sécurité publique présentes dans les pays où ils opèrent, dans le plein respect des droits de l'homme. Nous nous engageons à coopérer avec les organes de sécurité en vue de protéger la sécurité publique en adoptant les mesures suivantes :

- **Dès lors que la situation l'exige, travailler avec les organismes compétents à l'élaboration et à la mise en œuvre de solutions appropriées en vue de parvenir à l'objectif final tout en faisant subir le minimum de perturbations aux consommateurs et aux services essentiels**
- **Renforcer les réseaux disposant de la fonctionnalité de remédier à des situations d'urgence et de sécurité, le cas échéant**
- **Stipuler clairement notre limite d'action vis-à-vis de la chaîne de valeur en soulignant les domaines qui relèvent de l'intervention de tiers**

Protection de la sécurité des réseaux et de l'intégrité des appareils

Les acteurs du secteur doivent travailler ensemble et être coordonnés avec les services de sûreté internationaux pour partager des renseignements sur les menaces potentielles, afin de contrer les attaques malveillantes perpétrées sur des réseaux et des appareils mobiles et aussi pour identifier ses auteurs. Il s'agit pour cela de solliciter la participation des équipes existantes d'intervention en cas d'incident de sécurité et au besoin d'en créer de nouvelles pour combler les lacunes éventuelles. Les règlements, quand nécessaires, doivent s'appliquer de manière cohérente entre tous les prestataires de la chaîne de valeur, d'une manière neutre sur le plan du service et de la technologie, tout en préservant le modèle multipartite pour la gouvernance de l'Internet et en lui permettant d'évoluer. C'est dans cette optique que la GSMA et ses opérateurs membres ont convenu du principe suivant :

Les opérateurs s'engagent à prendre des mesures pour protéger l'infrastructure sous-jacente et veiller à ce que nous apportions aux consommateurs le service de communication le plus sûr et le plus fiable, et ce comme suit :

- **Prendre des mesures pour sécuriser l'infrastructure de réseau que nous exploitons et contrôlons**
- **Promouvoir le partenariat public-privé afin de minimiser les risques soit de piratage, soit d'exploitation du réseau à des fins malveillantes par des approches mondiales et coordonnées**
- **Stipuler clairement la responsabilité qui incombe aux opérateurs vis-à-vis des infrastructures et la démarcation des limites avec d'autres infrastructures ou services**

7

SIÈGE DE LA GSMA
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
Royaume-Uni
Tél. : +44 (0)20 7356 0600
Fax : +44 (0)20 7356 0601