Compte rendu de la 19ème consultation téléphonique A2ii-AICA

Assurance mobile : le défi de la confidentialité des données

24 novembre 2016

Les consultations téléphoniques de l'A2ii sont organisées en partenariat avec l'AICA pour fournir aux contrôleurs une plate-forme d'échange sur les expériences et les enseignements relatifs au développement de l'accès à l'assurance.

La 19ème Consultation téléphonique, qui s'est tenue le 24 novembre 2016, portait sur l'étude des défis de protection des données associés aux modèles d'affaires de l'assurance mobile. Quatre consultations ont été organisées : deux en anglais, une en français et une en espagnol.

Les experts techniques, le Dr Nicola Jentzsch (consultant) et Andrea Camargo (Directeur de la réglementation et de la protection des consommateurs au sein de MiCRO, Microinsurance Catastrophe Risk Organisation), ont passé en revue les principaux risques en matière de confidentialité et de protection des données découlant de l'application du traitement des « mégadonnées » (« big data ») à l'offre d'assurance, ainsi que les aspects réglementaires correspondants intéressant les contrôleurs. Les experts nationaux Eugene Du Toit de South African Financial Services Board et Ranferi Gómez de la Commission nationale mexicaine des assurances et des finances ont partagé l'expérience de leurs juridictions en matière de protection des données dans le domaine de l'assurance mobile.

Introduction à l'assurance mobile

L'assurance mobile, autrement dit l'offre de produits d'assurance par le biais de l'écosystème de téléphonie mobile, a connu une croissance rapide dans le monde entier. En juin 2015, le secteur de l'assurance mobile comptait 120 services actifs représentant 31 millions de polices actives sur 33 marchés émergents[1]. La prolifération de l'assurance mobile, non seulement en termes d'échelle, mais également du point de vue de l'étendue de la couverture, en a fait un marché solide en pleine croissance doté d'un impact potentiel considérable.

Tendances de l'offre mobile sur le marché de la micro-assurance

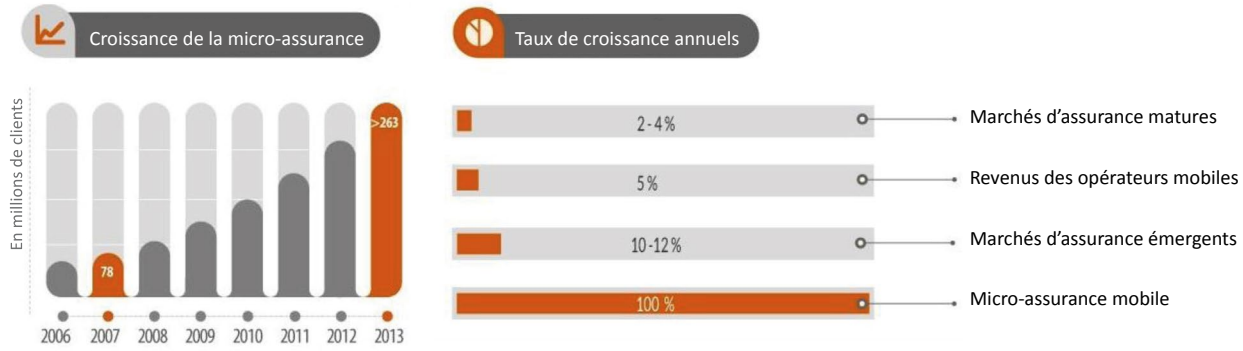
Le secteur de la micro-assurance a connu une croissance constante au cours des dernières années. Le premier recensement[2] complet réalisé en 2007 a dénombré plus de 80 millions de clients de micro-assurance dans le monde. En 2013, ce chiffre dépassait les 263 millions. Aujourd'hui, les experts estiment qu'il pourrait encore avoir doublé. Cette croissance est pour une large part due à la diffusion des produits d'assurance mobile, qui sont capables d'atteindre très rapidement une grande échelle. Tandis que les marchés d'assurance matures ont connu une croissance annuelle de 2 à 4 % environ et les marchés d'assurance émergents de 10 à 12 % environ, la micro-assurance mobile a enregistré des taux de croissance annuels de 100 % et plus. Par exemple, au Ghana, le prestataire de services techniques Tigo a atteint 1 million de clients dans l'année qui a suivi le lancement de son produit, et au Bangladesh, Grameenphone et MicroEnsure ont atteint 1 million de clients en 30 jours. L'application de la technologie numérique à l'assurance inclusive a déjà radicalement changé le paysage de l'assurance inclusive et constitue une évolution très prometteuse pour l'avenir.

> ***Assurer 1 million de vies prend un an via les ORM, contre 40 ans via le marché d'assurance traditionnel***
>
> *Accenture*

1 GSMA, 2015. *Mobile Insurance, Savings & Credit Report*. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/Mobile-Insurance-Savings-Credit-Report-2015.pdf

2 Accenture, 2014, Mobile Microinsurance (MMI): goes from experiential to exponential. Presentation by Thomas Meyer at the International Microinsurance Conference (IMC) Mexico.

Figure 1.



Source: Inclusivity Solutions

Caractéristiques des modèles d'affaires d'assurance mobile

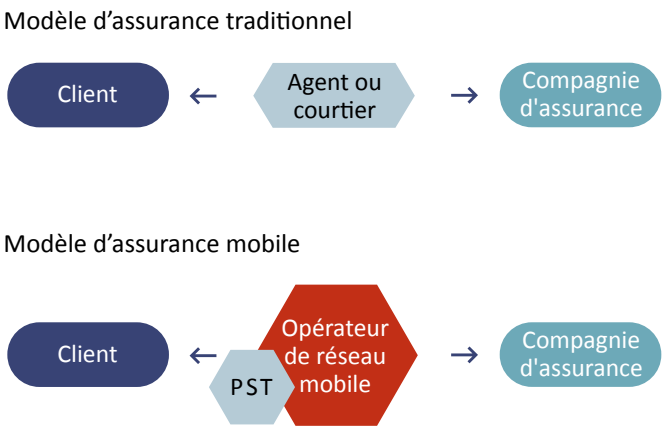
Un modèle d'assurance mobile désigne un modèle d'affaires d'assurance qui utilise le canal de la téléphonie mobile à un ou plusieurs stade(s) du cycle de vie du produit d'assurance. Le nombre et la nature des nouvelles entités impliquées, la numérisation de la chaîne de valeur de l'assurance et l'application des techniques de traitement des mégadonnées (« big data ») sont les principales caractéristiques qui différencient les modèles mobiles des modèles d'assurance traditionnels.

Émergence de nouveaux acteurs

L'une des caractéristiques déterminantes des modèles d'assurance mobile est l'introduction de nouveaux acteurs dans la chaîne de valeur de l'assurance. Tandis que la structure des modèles d'assurance traditionnels se caractérise par la présence d'un client, d'un assureur et d'un intermédiaire (agent ou courtier), les modèles d'assurance mobile introduisent une multiplicité de nouveaux acteurs dans la chaîne de valeur, qui sont généralement extérieurs à la sphère de l'assurance : des opérateurs de réseau mobile (ORM) ou d'autres agrégateurs tiers exploitent des réseaux et offrent de l'assurance à une clientèle en grande partie préexistante, tandis que les prestataires de services techniques (PST) jouent un rôle d'intermédiaire entre l'assureur et l'ORM en mettant à disposition une infrastructure d'administration et de paiement, bien qu'ils soient aussi souvent impliqués dans la conception des produits. Chacune des trois parties prenantes peut prendre la tête de l'offre d'assurance. Cependant, c'est souvent l'ORM qui pilote l'initiative. Une étude récente a révélé que 63 % des services d'assurance mobile étaient dirigés par des ORM[3]. Lorsque c'est l'assureur qui prend la tête, l'ORM joue un rôle largement passif, soutenant les transactions via son opérateur mobile et/ou son infrastructure d'argent mobile, tandis que l'assureur, réglementé par le contrôleur d'assurance, souscrit le produit. Dans les modèles dirigés par des ORM, l'assureur est autorisé à utiliser les données de l'ORM pour cibler et faire adhérer les clients. Dans ce modèle, l'ORM offre la solidité de sa marque pour inciter à l'achat de l'assurance, le produit étant inclus dans l'offre combinée de l'ORM. L'ORM offre l'assurance dans le but d'accroître la fidélité de sa clientèle, de réduire le taux de désabonnement, d'accroître la notoriété de sa marque et/ou d'augmenter le revenu moyen par client. L'investissement de l'ORM peut inclure le paiement de la prime d'assurance au nom de ses abonnés, l'exploitation de sa propre infrastructure, le traitement des mégadonnées pour cibler les clients et/ou le cofinancement du marketing et de la publicité. L'ORM, en tant qu'agrégateur, détient la clientèle, fournit une « marque de confiance » et un mécanisme de collecte des primes prêt à l'emploi. Traditionnellement, les ORM ne sont pas placés sous la juridiction du contrôleur d'assurance.

3 GSMA, 2015. *Mobile Insurance, Savings & Credit Report*. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/08/Mobile-Insurance-Savings-Credit-Report-2015.pdf

Figure 2. Modèle d'assurance traditionnel | Modèle d'assurance mobile



Ces nouveaux acteurs et partenariats reposant sur la technologie ont un impact sur la chaîne de valeur de l'assurance et sur l'équilibre des pouvoirs sur le marché, ce qui pose des défis particuliers aux contrôleurs. En outre, la participation de nouveaux acteurs extérieurs à la sphère de l'assurance peut entraîner une divergence d'intérêts entre ces nouveaux acteurs et les assureurs, ce qui est susceptible de conditionner les ventes et de fausser la perception de l'assurance par les clients, exerçant une pression à la baisse sur la demande.

Numérisation de la chaîne de valeur de l'assurance

La généralisation des nouveaux modèles d'affaires est largement due aux gains d'efficience et à la réduction des coûts de transaction que permet l'utilisation des technologies de l'information à chaque stade de la chaîne de valeur de l'assurance. L'acquisition des clients, la conception et la distribution des produits, ainsi que la gestion de la relation clientèle sont grandement facilitées par l'utilisation des données des réseaux mobiles. Le recours à la technologie dans les partenariats d'assurance mobile a le potentiel d'éliminer un grand nombre des obstacles traditionnels présents à différentes étapes du cycle de vie du produit d'assurance inclusive, permettant finalement le déploiement à grande échelle.

- **La génération, la communication et l'analyse des données numériques** sont utilisées pour informer les assureurs sur les préférences des clients et leurs schémas comportementaux. Le traitement de gros volumes de données numériques peut renseigner sur la propension d'un client potentiel à recourir à une assurance ou permettre d'estimer sa disposition à payer. L'analyse des données numériques et l'intégration croissante des données permettent aux entreprises d'améliorer leur capacité de prévision ; cette analyse peut être exploitée pour améliorer le ciblage des clients, le marketing et la conception des produits dans le but d'adapter la distribution et de réduire le taux de perte de clients.
- **Contractualisation numérique** : les téléphones mobiles constituent un moyen simple et peu coûteux de communiquer avec les clients potentiels et d'émettre des polices en utilisant la signature électronique.
- Pour **réduire les coûts de distribution**, les prestataires d'assurance choisissent de s'associer avec des agrégateurs tiers pour faciliter la vente des produits et la collecte des primes. Les compagnies

d'assurance « se greffent » sur la clientèle et l'infrastructure numérique de leurs partenaires dans le but de réduire les coûts et d'atteindre des clients à faibles revenus situés à l'écart des points de service des réseaux de distribution traditionnels.

- **La collecte des primes** via les canaux mobiles est moins coûteuse pour l'assureur et plus pratique pour le marché cible composé de personnes souvent non bancarisées. Les primes sont souvent déduites du compte de communication mobile ou de l'infrastructure d'argent mobile d'un ORM.
- **Règlement des sinistres :** la téléphonie mobile peut faciliter la soumission et le règlement rapide des demandes d'indemnisation, par exemple lorsque les paiements sont effectués via des portefeuilles mobiles. Les traditionnels défis associés au règlement des sinistres, comme la faiblesse des infrastructures ou l'inaptitude des clients à fournir les documents requis, peuvent être réglés par le recours à des agrégateurs tiers en exploitant les relations et les flux de paiement existants entre les clients et ces entités pour soumettre et régler les demandes d'indemnisation.
- **Modélisation des risques :** l'application d'algorithmes sophistiqués aux grands ensembles de données peut aider les prestataires à mieux définir et modéliser le risque qu'ils souscrivent pour être plus efficaces lors de la conception du produit, de la sélection des risques et de la tarification des primes.

Analyse des mégadonnées

En tirant parti de l'infrastructure mobile à travers l'analyse des mégadonnées, les assureurs augmentent leur possibilités de lancer des produits pionniers auprès d'un plus grand nombre de clients, et ce plus rapidement. Les « mégadonnées », qui désignent de gros volumes d'informations numériques organisées au sein d'ensembles de données structurées et non structurées, facilitent à la fois l'efficience et l'efficacité du processus d'assurance à un degré sans précédent. Les mégadonnées se caractérisent par trois « V »: (i) volume de données très important (en téra- et pétabytes), (ii) vitesse d'accumulation (souvent à haute fréquence en temps réel), et (iii) variété (modèles d'appels mobiles, blogs, journaux des centres d'appels, etc.)[4].
La transmission d'informations informatisées contribue à la collecte des données en temps réel et permet aux assureurs d'établir des relations directes, sans intermédiaire, avec les clients, basées sur l'accès direct aux données non filtrées. Cette cartographie des préférences et des schémas comportementaux permet aux assureurs d'affiner leur connaissance du profil des clients et de l'évolution de leurs besoins dans le temps dans le but d'individualiser les offres.

La mise en œuvre de nouvelles technologies et de techniques de traitement des données au sein de l'infrastructure mobile crée un environnement d'interconnexion et de partage d'information accru qui, s'il représente un formidable potentiel pour faire bénéficier de l'assurance des millions d'individus jusqu'ici non couverts, génère de nouveaux défis en matière de confidentialité, de protection des données et de cybersécurité.

Préoccupations croissantes en matière de protection de la vie privée

En dépit des avantages potentiels de l'assurance mobile, l'adoption croissante de techniques de traitement de l'information omniprésentes et souvent intrusives a conduit à accroître les préoccupations concernant la protection de la vie privée partout dans le monde. Une récente étude réalisée par KPMG[5] dans plus de 24 pays

4 Watson, H.J. (2014). *Tutorial: Big Data Analytics: Concepts, Technologies, and Applications*, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3785&context=cais
5 KPMG (2016). *Crossing the line: Staying on the right side of consumer privacy,* https://home.kpmg.com/content/dam/kpmg/au/pdf/2016/crossing-the-line.pdf

indique qu'en 2016, 55 % des consommateurs dans le monde ont renoncé à acheter un produit en ligne en raison de problèmes de confidentialité. Dans la même étude, 66 % des consommateurs ont déclaré être mal à l'aise avec les applications utilisant leurs informations personnelles. On observe également une préoccupation croissante concernant le respect de la vie privée dans de nombreux pays en développement et marchés émergents. Une autre enquête[6] réalisée auprès de plus de 24 000 consommateurs dans 20 pays a montré que le nombre de consommateurs « un peu plus » ou « beaucoup plus préoccupés » par la protection de leur vie privée que l'année précédente était en augmentation significative. Cette préoccupation croissante peut conduire à des problèmes de confiance qui, s'ils ne sont pas correctement traités, peuvent freiner l'adoption de services d'assurance mobile à l'avenir.

Protection des données

La protection des données englobe généralement des mesures politiques, juridiques, réglementaires et techniques, ainsi que des protocoles visant à protéger les données à caractère personnel[7]. En règle générale, la protection des données comprend les droits individuels de protection de la vie privée (comme le droit d'accès aux données, de correction des données, etc.) et ne concerne normalement que les individus, pas les entreprises. En fonction de la situation de chaque pays, il existe une variété de lois qui peuvent s'appliquer à la protection des données.

Les droits fondamentaux de protection des données des particuliers comprennent généralement des dispositions telles que la transparence des pratiques de traitement des données ; autrement dit, les organisations qui collectent des données personnelles doivent être transparentes et claires sur la question de leur utilisation. Les données personnelles doivent être collectées à des fins limitées et licites et ne doivent pas être utilisées à d'autres fins que celles mentionnées au moment de la collecte. L'objet de la divulgation doit également être précisé. Dans de nombreux régimes réglementaires, les particuliers ont le droit de consentir au traitement de leurs données, ce qui est fondamental dans la mesure où cela accroît la transparence du traitement. En outre, les lois sur la protection des données visent également à orienter les mesures de sécurité techniques et procédurales afin d'empêcher l'accès non autorisé aux données. D'autres dispositions prévoient que les données doivent être pertinentes, exactes et actualisées, et que toute personne doit avoir le droit d'accéder à ses données et de les corriger si nécessaire.

Défis liés à la protection des données dans l'assurance mobile

Propriété des données et responsabilités

L'un des principaux défis découlant des modèles d'assurance mobile est la question de la propriété des données et de leur diffusion. Qui exactement détient les données sur les clients et qui est responsable de leur protection et/ou de leur diffusion ? Il s'agit d'une question complexe qui dépend souvent du modèle d'affaires et des accords de service conclus entre les entités concernées. Si l'opérateur de réseau mobile (ORM) est propriétaire de toutes les données collectées par le biais de son réseau mobile, d'autres entités telles que

6 *2016 CIGI-Ipsos Global Survey on Internet Security and Trust*, https://www.cigionline.org/internet-survey-2016

7 D'après le nouveau règlement général de l'UE sur la protection des données, on entend par « données à caractère personnel » : « toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. » Source : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679&from=FR

les PST peuvent être engagées comme sous-traitants ou assurer des fonctions qui impliquent un accès aux données clients de l'ORM. Par exemple, les PST peuvent se voir confier des données dans le but d'effectuer une présélection visant à identifier les clients auxquels le produit d'assurance sera proposé. Cette fonction permet aux PST de contacter directement le client afin d'établir une relation et de recueillir directement des informations complémentaires sur son profil, qui seront ensuite partagés avec le prestataire d'assurance aux fins d'un accord de courtage. Ces transferts de données soulèvent des questions importantes en matière de protection de la vie privée et de protection des données, dans la mesure où ce traitement est souvent réalisé de manière non transparente sans le consentement éclairé des consommateurs.

Changements fondamentaux introduits par les modèles d'affaires d'assurance mobile

Asymétries d'information

L'assurance mobile introduit un changement fondamental dans les asymétries d'information existantes sur le marché, non seulement entre les clients et les entreprises, mais aussi entre les entreprises et les autorités de contrôle. Lorsque les entreprises commencent à exploiter les mégadonnées, elles pratiquent un traitement des informations qui est la plupart du temps non transparent pour les consommateurs. Lorsqu'un client demande une assurance, il renonce d'une certaine manière à la confidentialité de sa vie privée en acceptant la collecte d'informations personnelles issues de ses données mobiles. Toutefois, les consommateurs savent rarement ce qu'implique exactement le renoncement à cet actif immatériel, c'est-à-dire quel est le type de données personnelles utilisées pour l'estimation et le type d'analyse de données réalisée. Sachant qu'ils ignorent l'étendue exacte du traitement et de l'analyse de l'information, les clients n'ont pas les moyens d'évaluer correctement le compromis induit pour donner leur consentement éclairé. Le manque de sensibilisation des clients fait naître des préoccupations importantes en matière de protection des consommateurs au regard de la nécessité de préserver leurs droits fondamentaux intrinsèquement liés à la collecte et au traitement de l'information. En outre, les consommateurs sont souvent victimes de déséquilibres de pouvoir qui ne leur laissent pas d'alternative pour acquérir une assurance. S'ils veulent être couverts, ils n'ont d'autre choix que de signer ce qui leur est proposé.

S'agissant de la relation entre les entreprises et les autorités de contrôle, bien que les contrôleurs soient chargés de surveiller les entreprises qui ont recours au traitement des mégadonnées, les entreprises utilisent souvent des modèles sophistiqués qui compliquent la surveillance. L'utilisation des algorithmes d'apprentissage automatique, par exemple, creuse le fossé des connaissances entre les entreprises et les contrôleurs, ce qui rend leur surveillance très difficile. En outre, la question de savoir qui est responsable de la réglementation des différentes parties impliquées ajoute une couche supplémentaire de complexité. Si les ORM sont supervisés par l'autorité de réglementation des télécommunications et les assureurs par le contrôleur des assurances, le contrôleur des assurances doit également coordonner son action avec celle du régulateur des télécommunications pour surveiller les ORM et leurs activités, les PST tombant quant à eux souvent dans une zone de flou. Cette dimension supplémentaire de responsabilité de la surveillance complique encore davantage les obstacles réglementaires découlant de l'utilisation de technologies sophistiquées.

Expansion du marché et saturation du marché

Le marché de l'assurance connaît habituellement deux phases à la suite de l'introduction de ces nouveaux modèles d'affaires. Une première phase d'expansion du marché est suivie d'une phase de saturation. Dans la phase d'expansion du marché, la baisse des coûts de transaction permet aux entreprises de toucher davantage

de clients, ce qui a pour effet de donner accès à l'assurance à un plus grand nombre d'individus qu'auparavant, et se traduit par une augmentation du bien-être des consommateurs. Cependant, avec le renforcement de la concurrence, le marché connaît une saturation croissante. Les entreprises se livrent une concurrence féroce pour les parts de marché et commencent à personnaliser les prix et les produits sur la base des informations individuelles qu'ils ont recueillies sur les clients. La combinaison de prix et de produits personnalisés entraîne une baisse du bien-être des consommateurs dans la mesure où les prestataires de services commencent à fixer les prix de leurs produits en fonction de la propension à payer des consommateurs ou du niveau maximum de prix abordable[8]. En outre, une fois qu'un produit ou un service a été adapté aux préférences d'un individu, il devient difficile pour cet individu de le comparer avec des offres alternatives, car ses caractéristiques particulières ne permettent pas une comparaison directe avec d'autres produits. Ces incitations commerciales modifient les stratégies concurrentielles des entreprises d'une façon qui peut conduire à exposer les consommateurs à des pratiques prédatrices.

Un recul de l'accès à l'assurance ? Saturation du marché et mise à l'écart des consommateurs à faibles revenus

Q. La tendance à la saturation du marché aura-t-elle pour effet à terme d'écarter les individus à faibles revenus du marché ?

Il faut noter que dans la phase de saturation du marché, la personnalisation des prix n'a pas automatiquement pour effet d'écarter du marché les clients à faibles revenus. Pour maximiser leurs bénéfices, les prestataires de services auront tendance à vouloir fixer un prix juste en dessous du prix maximum que les consommateurs sont prêts à payer. Toutefois, ce n'est pas toujours le cas dans la pratique. Par exemple, si certains clients d'une entreprise donnée se sont avérés non rentables, l'entreprise va fixer un prix que ces clients ne sont pas prêts à payer, de façon à les écarter. On ne peut pas affirmer pour autant que, dans les stades ultérieurs du développement du marché, tous les individus à faibles revenus feront l'objet d'une discrimination et se trouveront écartés du marché par les prix, dans la mesure où certains d'entre eux pourraient en réalité s'avérer des clients rentables.

Stratégie concurrentielle des entreprises

Les modèles d'affaires d'assurance mobile ont également conduit à des changements dans les stratégies concurrentielles des entreprises, principalement parce que les compagnies d'assurance sont en mesure d'accroître la quantité d'informations collectées et analysées. Le recours au traitement des mégadonnées permet aux entreprises un micro-ciblage et une présélection des clients censés avoir une plus forte propension à répondre à une offre et à devenir des clients payeurs et rentables. Après le profilage et l'inscription des clients présélectionnés, les compagnies d'assurance vont essayer de concevoir des produits qui sont adaptés aux préférences spécifiques des individus. L'absence de standardisation de ces produits diminue la comparabilité globale des produits et par conséquent incite également les entreprises à appliquer des prix sur mesure.

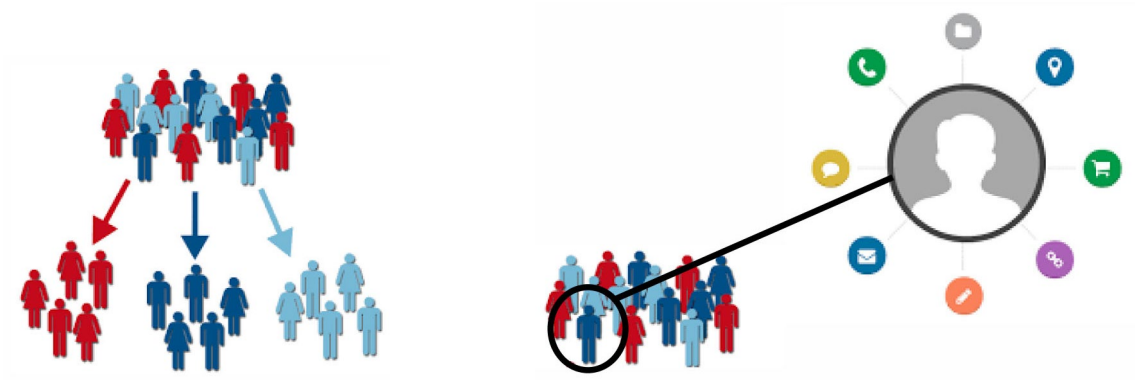
Vie privée : une vision à 360 degrés du client

Dans les modèles d'assurance traditionnels, les assureurs réalisent une segmentation du marché en fonction des facteurs démographiques et comportementaux observables des consommateurs, répartissant les individus

8 Ghose, A. et K.W. Huang (2009). *Personalized Pricing and Quality Customization, Journal of Economics & Management Strategy 18* (4), 1095-1135. Le modèle présenté dans ce document s'applique à un marché saturé. Dans un marché en expansion, l'effet net sur le bien-être des consommateurs peut être positif si le bien-être global des consommateurs augmente en raison de la prise en compte de nouveaux clients dans la tarification.

en différentes catégories de clients. Avec l'assurance mobile et le traitement des mégadonnées, les entreprises sont capables de procéder à un ciblage personnalisé grâce au volume d'informations recueillies sur les clients. La géo-localisation des individus, les caractéristiques des habitudes d'appel, ainsi que la durée et la direction des appels ne sont que quelques-unes des centaines de variables utilisées pour la modélisation des profils de consommateurs. Ces variables fournissent des informations de ciblage sensibles qui vont du réseau social de l'individu à ses revenus, en passant par son état de santé, ses habitudes de déplacement et même sa religion. Ces informations rassemblées grâce au traitement des mégadonnées sont ensuite utilisées pour construire une vision à 360 degrés du client, qui n'était pas possible auparavant avec la segmentation traditionnelle du marché.

Figure 3. Segmentation des clients vs personnalisation



Considérations pour les autorités de contrôle

Avec le déploiement croissant des technologies de l'information utilisées pour l'offre d'assurance mobile, de plus en plus d'acteurs du marché collectent des informations personnelles sur les individus, d'ordre financier mais aussi relatives à la géolocalisation et au style de vie. Ce transfert d'informations sans précédent soulève des questions importantes pour la protection de la vie privée liées au traitement et à la diffusion des données à caractère personnel ainsi qu'aux défis que constituent les changements de stratégie concurrentielle des entreprises pour la protection des consommateurs. L'assurance mobile représente sans aucun doute une réelle opportunité pour l'amélioration de l'accès aux services financiers et le soutien au développement socio-économique. Toutefois, il est important que les autorités de contrôle traitent les questions soulevées par l'assurance mobile pour s'assurer que la réglementation facilite le développement du marché de l'assurance inclusive tout en protégeant les assurés et en garantissant la stabilité financière.

Cadre réglementaire

Les stratégies et les changements découlant de ces nouvelles configurations numériques soulèvent une foule de questions en matière de protection des consommateurs. Les autorités de contrôle peuvent néanmoins prendre un premier ensemble de mesures pour répondre à ces questions par le biais d'une réglementation adaptée.

Bien que certaines juridictions envisagent d'élaborer des réglementations spécifiques à l'assurance mobile, dans d'autres, la législation plus généralement appliquée à l'assurance inclusive est également appliquée à la réglementation de l'assurance mobile et de la protection des données. La réglementation de l'assurance mobile et du traitement des données sur les consommateurs est souvent un processus complexe, impliquant

un ensemble d'autorités de réglementation et de contrôle – contrôle des assurances, banque centrale, autorité des télécommunications, contrôle de la protection des données. La protection des données des consommateurs fait partie du mandat de différents organismes de réglementation. Le paysage réglementaire d'un pays donné est donc habituellement composé d'une partie ou de la totalité des textes législatifs pertinents : loi sur les télécommunications, loi sur l'assurance, loi sur la déclaration des informations de crédit et loi sur la protection des données.

→ *Loi sur les télécommunications*

En règle générale, une loi sur les télécommunications ne comprend pas de clause approfondie ni de règlement détaillé sur la protection des données, bien qu'elle puisse contenir des clauses de confidentialité éparses qui obligent les entreprises à traiter les données et les méthodes commerciales des clients comme des informations confidentielles. En effet, l'objectif premier d'une loi sur les télécommunications consiste à réglementer le marché des télécommunications, par exemple en réglant des questions telles que l'octroi de licences aux entreprises de télécommunications ou la création d'une autorité destinée à réglementer le système de télécommunications. Les mesures de protection des données ne sont pas expressément énoncées dans la législation sur les télécommunications.

→ *Loi sur les assurances*

Il en va de même pour la loi sur les assurances. La loi sur les assurances a pour objectif principal la supervision du secteur de l'assurance dans le but de développer et de conserver des marchés d'assurance équitables, sûrs et stables au bénéfice et pour la protection des assurés. Comme pour la législation sur les télécommunications, dans certains pays, la législation sur les assurances contient également des clauses de confidentialité relatives aux données sur les clients ; cependant, la loi sur les assurances n'a pas pour objet principal le respect de la confidentialité des données des clients.

→ *Loi sur la protection des données*

Une réglementation prévoyant explicitement des mesures de protection des données et de la vie privée requiert la création d'une loi distincte sur la protection des données. Les lois sur la protection des données définissent généralement des dispositions élémentaires relatives à la collecte, au traitement et à l'analyse des données, tout en établissant une autorité de protection des données chargée de protéger les droits fondamentaux des personnes concernées. La structure et la portée de la législation en matière de protection des données sont très variables : elles peuvent par exemple porter uniquement sur le secteur privé ou public, ou s'attacher à des secteurs d'activité particuliers. Dans de nombreuses juridictions, les lois sur la protection des données sont généralement des corpus législatifs globaux inscrits dans la constitution de l'État, et non conçus spécifiquement comme un sous-ensemble de la réglementation de l'assurance relatif à l'écosystème mobile.

→ *Loi sur les données de crédit*

Certaines juridictions ont également une loi qui régit le traitement des informations sur le crédit. Les implications d'une telle loi sur la protection des données dépend de la portée de la loi dans chaque juridiction. Certaines lois sur les données de crédit désignent les institutions qui peuvent communiquer des rapports de crédit à une centrale des risques. Si une compagnie d'assurance fait partie de ce groupe d'institutions, elle sera alors en mesure de communiquer des informations sur ses assurés et leur comportement de paiement à la centrale des risques. Cette loi peut jouer un rôle dans la façon dont fonctionne le partage de l'information et dans la manière dont il est contrôlé dans un pays donné.

→ *Défis juridiques : situation et mise en conformité des nouveaux acteurs*

La structure particulière de la législation d'un pays peut poser de nombreux défis en termes de protection des données et de la vie privée. Les entités extérieures au secteur de l'assurance impliquées dans la chaîne de valeur de l'assurance sont pour l'essentiel hors de la juridiction traditionnelle des contrôleurs d'assurance (par exemple, les ORM sont réglementés par l'autorité des télécommunications). Pourtant, l'implication de ces entités non assurées dans l'activité d'assurance peut faire courir à leur vaste clientèle de gros risques en matière de protection des consommateurs si leurs actions ne sont pas correctement supervisées. De plus, dans de nombreuses juridictions, la législation existante ne prend pas en compte les activités d'assurance mobile et les nouveaux acteurs tels que les PST. Les PST sont souvent impliqués dans la chaîne de valeur de l'assurance en soutien à différentes fonctions, mais sont généralement en première ligne s'agissant de la gestion des données sur les consommateurs ; si, dans certaines juridictions, les PST sont tenus de s'enregistrer en tant qu'agents auprès du contrôleur des assurances et dépendent donc de sa compétence, dans d'autres, ils ne relèvent pas de la législation en vigueur. Cette lacune réglementaire est encore aggravée s'il n'existe pas de loi sur la protection des données régissant le traitement des informations à caractère personnel. Il est donc important que les contrôleurs clarifient ou adaptent le cadre légal auquel les PST et d'autres intermédiaires doivent se conformer afin de protéger les consommateurs contre les risques découlant de l'environnement propre aux mégadonnées.

Il est essentiel d'adopter une approche de surveillance harmonisée des bonnes pratiques de protection des données, et de faire en sorte que toute nouvelle exigence prenne en compte les mandats et réglementations existants. Désigner clairement qui est responsable de la protection de quelles données est primordial, dans la mesure où de plus en plus de données sont recueillies par des tiers ou des intermédiaires pour être ensuite utilisées par les assureurs ou d'autres acteurs dans le cadre d'activités liées à l'assurance. Les différentes autorités de contrôle doivent travailler ensemble pour préserver les droits fondamentaux des consommateurs, en particulier dans un environnement caractérisé par la collecte omniprésente et souvent intrusive de données personnelles. Cette coopération doit se fonder sur une base légale et, idéalement, être codifiée dans un document (par ex. un protocole d'entente) qui définit les procédures de base pour le suivi et la réglementation des différentes entités concernées.

Législation sur la protection des données dans l'assurance mobile

Loi sur les télécommunications : clauses de confidentialité protégeant le caractère privé des données et des activités commerciales des clients

Loi sur les assurances : clauses de confidentialité protégeant le caractère privé des données et des activités commerciales des clients

Loi sur la protection des données : dispositions sur la protection des données relatives à la collecte, au traitement, à l'analyse et au transfert des données à caractère personnel, tâches assignées au contrôleur des données et droits des personnes concernées (individus)

Loi sur les données de crédit : dispositions sur la protection des données ainsi que sur les conditions de transfert des données des clients d'assurance aux centrales des risques

Études de cas : Afrique du sud et Régime mexicain de protection des données

AFRIQUE DU SUD

La surveillance de l'assurance mobile n'est pas explicitement réglementée en Afrique du Sud. Les questions transversales relatives à l'assurance mobile et plus particulièrement à la protection des données sont contrôlées par divers organes et sont aussi encadrées par la Constitution sud-africaine.

Structures et risques des partenariats d'assurance avec les ORM

Pour comprendre les différents défis réglementaires du contexte sud-africain, il importe de comprendre la structure des différents partenariats d'assurance impliquant des ORM et comment ils fonctionnent dans le secteur de l'assurance[9] .

- → **Assureur enregistré au sein du groupe de l'ORM** : l'ORM a son propre assureur établi au sein du groupe de l'ORM, et quasiment toutes les fonctions sont assurées en interne.
- → **Système de captive d'assurance** : l'ORM crée une entité distincte qui porte le risque assuré, en acquérant une catégorie spécifique d'actions cantonnées d'un assureur agréé. Cette opération est souvent couplée à un accord de sous-traitance ou à un accord global par lequel l'ORM assure diverses fonctions pour le compte de l'assureur (c'est-à-dire conduit l'activité d'assurance) tandis que l'assureur souscrit le risque.
- → **Accord de marque** : un assureur agréé assume l'entière responsabilité de l'assurance, bien que le partenariat puisse prévoir des accords de partage des données avec l'ORM dans le but de donner accès à sa base de clients. Le rôle de l'ORM est de fournir des données sur les clients pour permettre la distribution agrégée du produit ; il peut recevoir une rémunération pour l'accord de marque passé avec l'assureur (car l'assureur tire profit de la marque de l'ORM).

Les principaux risques identifiés sur le marché de l'assurance mobile en Afrique du Sud sont :

- **Des questions de protection et de confidentialité des données** découlent de l'interconnexion structurelle des entités et des asymétries d'information en résultant, qui conduisent à l'utilisation non autorisée des données en raison de la libre circulation de l'information entre les différentes entités. Par exemple, dans le cas d'une société captive, bien que l'ORM agisse pour le compte de l'assureur, il utilise les informations de sa société mère, ce qui pourrait constituer une violation de la protection des données au regard de la loi sud-africaine.
- De nombreux cas de **pratiques commerciales abusives** ont été relevés, comme la souscription forcée[10], l'identification insuffisante de l'assureur et le manque d'informations sur les clauses contractuelles essentielles.
- **Les risques opérationnels** spécifiquement liés à la sous-traitance et aux risques de partenariat : ils concernent notamment l'insuffisance de la surveillance de l'entité exerçant l'activité d'assurance pour le compte de l'assureur, ce qui se traduit par une protection inappropriée des consommateurs

9 Seules les trois structures les plus communes sont présentées. Cependant, les dispositifs de partenariat avec les ORM ne se limitent pas nécessairement à une structure unique et peuvent être constitués d'une combinaison de plusieurs d'entre elles.
10 Par exemple, un assureur qui vend des produits combinés propose une assurance obsèques gratuite pendant une certaine période, après laquelle il prélève automatiquement les primes sans que l'assuré ait demandé à continuer de bénéficier de l'assurance.

tout au long de la durée du produit. Ce risque est particulièrement répandu avec les systèmes de captives et dans le cas d'accords de délégation de souscription ou d'accord globaux.

Cadre réglementaire

L'actuel cadre réglementaire régissant l'assurance mobile et la protection des données comprend :

- La **Constitution sud-africaine** : législation suprême qui régit toute activité et consacre la Charte des droits. Toutes les lois en Afrique du Sud doivent être conformes à la Constitution. La Constitution dispose que tout citoyen a droit au respect de sa vie privée. Bien qu'il ne s'agisse pas d'une loi détaillée, elle fournit une base pour toutes les lois relatives à la confidentialité des données.
- La principale loi régissant la protection des données en Afrique du Sud est une loi d'application générale intitulée « **Protection of Personal Information Act » (POPI)**. La Loi POPI établit une autorité de réglementation de l'information (note : qui n'est pas le contrôleur des assurances) et lui confère des pouvoirs étendus pour administrer la Loi. Elle aborde également la question du traitement des données et accorde certains droits à la protection de la vie privée dans les contextes de connexion aux données personnelles et de traitement de ces données en Afrique du Sud. Il s'agit donc d'une loi générale qui s'applique à tous les assureurs, dans la mesure où il n'existe actuellement aucune législation spécifique à la protection des données dans le cadre réglementaire de l'assurance[11].
- Une autre loi d'application générale est la Loi sur la protection des consommateurs **(Consumer Protection Act, CPA)**, qui prévoit des dispositions limitées en matière de protection de la vie privée. Toutefois, la CPA ne s'applique pas aux fonctions, actes, transactions, biens ou services soumis à la législation sur les services financiers[12]. Le secteur des services financiers a donc ses propres **lois de protection des consommateurs**.
- Il existe également une loi sur les communications et les transactions électroniques **(Electronic Communications and Transactions Act)** qui contient certaines dispositions relatives à la protection des données.

Globalement, la Loi POPI est la principale loi régissant la protection des données en Afrique du Sud. Le défi pour l'autorité de réglementation des assurances consiste à établir des protocoles d'entente adaptés avec l'autorité de réglementation de l'information afin que les deux entités puissent coopérer dans le cas où des assureurs enfreindraient la loi sur la protection des données.

Mesures d'atténuation des risques prises par le Financial Services Board (FSB)

Projet d'amendements à la législation

Actuellement, la Loi sur l'assurance à long terme et la Loi sur l'assurance temporaire, qui régissent l'assurance en Afrique du Sud, ne comprennent pas d'exigences spécifiques sur la protection des données, ni sur l'assurance mobile. Néanmoins, le FSB travaille sur un projet de législation subordonnée pour traiter les questions de confidentialité des données et de protection des consommateurs. Bien que ces amendements ne soient pas spécifiquement orientés vers l'assurance mobile, ils sont par nature applicables à l'analyse des « mégadonnées » (Big Data) et à l'assurance mobile. Un amendement important traitant de questions relatives à la gestion des données impose aux assureurs un certain nombre d'obligations significatives le

11 Bien que la loi POPI ait été promulguée, les sections importantes relatives au traitement des données et à la protection de la vie privée n'ont pas encore pris effet. Seules les sections à caractère administratif (par exemple l'établissement d'une autorité de réglementation de l'information) ont pris effet à ce jour. La date de prise d'effet des articles de fond n'est pas définie, mais elle serait prévue pour 2017.
12 Section 28(2)(b) du Financial Services Board Act.

contraignant à adopter un cadre de gestion des données pour l'analyse des mégadonnées. Cette mesure permettra de répondre aux préoccupations relatives aux accords d'externalisation en reconnaissant la responsabilité de l'assureur et en lui imposant des exigences strictes en matière de surveillance, de conception des produits et de suivi. Des obligations de même nature concernent d'autres questions importantes, telles que la divulgation des informations, la publicité et les pratiques d'adhésion par défaut. Ces obligations sont indépendantes des supports utilisés, ce qui signifie que la législation s'applique à toute plateforme, mobile ou autre. Toutes ces politiques, bien que générales, auront un impact significatif sur l'assurance mobile. S'il n'introduit aucune loi d'envergure sur la protection des données et la confidentialité dans la réglementation de l'assurance, le FSB propose des amendements qui permettront indirectement à l'autorité de réglementation des assurances de prendre des mesures en cas de violation de la protection des données[13]. Le FSB devra également conclure un protocole d'entente avec l'autorité de réglementation de l'information pour favoriser la coopération et l'action chaque fois que nécessaire.

Approche de surveillance ciblée

Pour compléter la législation, le FSB envisage d'adopter une approche de surveillance ciblée pour réglementer les questions liées à l'assurance mobile et à la protection des données. Cela pourrait impliquer de cibler les prestataires d'assurance mobile et de veiller à ce qu'ils se conforment à la législation applicable préexistante.

RÉGIME MEXICAIN DE PROTECTION DES DONNÉES

Le régime mexicain de protection des données personnelles est composé d'un ensemble de lois codifiées dans la Constitution mexicaine. La Constitution stipule que toutes les informations concernant la vie privée et les données à caractère personnel des citoyens sont protégées dans les conditions fixées par la loi et que leur protection est reconnue comme un droit fondamental garanti. La conformité à ces lois est garantie par un organisme fédéral autonome, l'Institut national de la transparence, de l'accès à l'information et de la protection des données à caractère personnel (INAI), qui est responsable de la protection des données personnelles de l'ensemble des citoyens mexicains. L'autorité de contrôle des assurances, la Commission mexicaine des assurances et des garanties, n'est pas chargée de réglementer la protection des données.

Les principales lois relatives à la réglementation de la protection des données au Mexique et leurs dispositions sont décrites ci-dessous.

Loi générale sur la transparence et l'accès à l'information publique

- Crée *l'Institut national de la transparence, de l'accès à l'information et de la protection des données à caractère personnel (INAI)*, un organisme indépendant chargé de superviser l'utilisation des données à caractère personnel.
- L'accès aux informations personnelles n'est autorisé qu'à leurs propriétaires légitimes, à leurs représentants ou aux fonctionnaires autorisés.

13 Comprend un projet d'amendement qui imposera aux assureurs de se conformer à toutes les lois applicables en matière de confidentialité, de sécurité et de conservation des données ou des informations.

- Les détenteurs de données à caractère personnel doivent protéger ces données et ne peuvent autoriser l'accès à des informations confidentielles qu'avec le consentement du ou des propriétaires légitime(s) de ces informations.
- Établit une instance d'appel devant l'INAI.

Loi fédérale sur la transparence et l'accès à l'information publique

- Définit la structure et le rôle de l'INAI.
- Établit des comités de transparence au sein du gouvernement fédéral pour assurer le traitement transparent des données.

Loi fédérale sur la protection des données à caractère personnel en possession d'entités privées

- Sont concernés par cette réglementation les individus et entités collectant, utilisant, diffusant ou stockant des données personnelles.
- Oblige les entités qui traitent des données à caractère personnel à collecter ces informations en toute transparence et à les utiliser avec le consentement explicite de leurs propriétaires. Ces entités doivent informer les propriétaires de la collecte de leurs informations et de l'objet de cette collecte par le biais d'une déclaration de confidentialité.
- Permet aux entités en possession de données à caractère personnel de transférer ces données à des tiers sans le consentement de leurs propriétaires lorsque les informations sont transférées à des filiales ou à toute autre société contrôlant l'entité responsable.
- Établit que les titulaires de données à caractère personnel jouissent d'un droit d'accès, de correction, d'annulation et d'opposition.

Loi sur la réglementation des groupes financiers

- Une société en possession de données à caractère personnel et toute autre entité financière appartenant à un groupe financier peut partager des informations relatives aux services assurés par chaque entité avec ses clients sans que cela soit considéré comme une infraction à la confidentialité, tant que la nature du document partagé entraîne l'obligation de confidentialité.

Loi sur la protection et la défense des usagers de services financiers

- La Commission nationale de protection et de défense des usagers des services financiers va créer et assurer la mise à jour d'un registre des usagers qui ne souhaitent pas que leurs informations soient utilisées à des fins de marketing et de publicité.
- Il est interdit aux institutions financières d'utiliser les informations de leur base de données clientèle à des fins de marketing ou de publicité et d'envoyer des publicités aux clients qui ont explicitement demandé à ne pas en recevoir ou qui se sont inscrits sur le registre des usagers.

Loi sur les assurances et les garanties

- Les institutions d'assurance peuvent partager des informations dans le but de renforcer les mesures de prévention et d'identification des opérations en lien avec une association criminelle sans que cet échange d'informations soit considéré comme une violation des obligations de confidentialité.

Questions et discussion

Les consommateurs à faibles revenus ne sont généralement pas conscients qu'ils ont des droits à défendre. Existe-t-il des mesures visant à sensibiliser les consommateurs sur les risques de violation de leurs droits relatifs à la protection des données ?

Cela dépend vraiment du pays. Dans certains pays, en vertu de la loi sur la protection des données, et non de la législation sur les assurances, les entreprises qui collectent et qui traitent des données à caractère personnel doivent informer les consommateurs de leurs activités ; les consommateurs ont alors des droits spécifiques, notamment le droit de vérifier l'exactitude des données collectées et de rectifier toute erreur. Cependant, cette obligation n'a rien d'universel, de sorte que les clients ignorent souvent leurs droits. Les consommateurs entendent généralement parler des abus par les médias.

Que peuvent faire les contrôleurs si leur cadre réglementaire ne comprend pas de loi globale sur la protection des données ? Que peut-on faire dans le cadre d'une loi sur l'assurance ?

Cela dépend beaucoup de la portée de la loi sur les assurances existante et du pouvoir que détient le contrôleur pour mettre en œuvre des mesures de protection des consommateurs selon des dispositions spécifiques. S'il a cette possibilité, il est important qu'il transfère la responsabilité de la protection des données et de la confidentialité à l'assureur. Les règles fondamentales de protection des données à mettre en œuvre doivent alors viser à renforcer les connaissances des clients sur la collecte, le traitement et l'utilisation de leurs données.

L'absence de plaintes dans le domaine de la protection des données est-elle réellement un indicateur de l'absence d'abus ? Ou bien les abus sont-ils le plus souvent invisibles pour le consommateur dans la mesure où celui-ci n'est pas conscient de la nature des atteintes, par exemple à sa vie privée ?

L'absence de plaintes est à rapprocher de l'absence de transparence de l'environnement propre aux mégadonnées. L'absence de comparabilité et de standardisation des services électroniques rend difficile la détection des discriminations pour les clients. D'un point de vue réglementaire, l'absence de plaintes n'est pas un indicateur idéal. Toutefois, dans certaines juridictions, il peut ne pas s'agir d'un aspect prioritaire pour les autorités de réglementation des assurances, s'il existe une législation sur la protection des données qui place la responsabilité de la protection des consommateurs sous la compétence d'une autre autorité. Les autorités de contrôle de l'assurance doivent coopérer avec les autres autorités de réglementation de façon à traiter ces questions de manière proactive, soit par le biais d'une approche visant spécifiquement l'assurance mobile, soit par une approche d'application plus générale.

Quels effets sur la concurrence requièrent la vigilance des contrôleurs dans l'avenir ?

Il découle généralement de la configuration des modèles d'affaires d'assurance mobile des effets verticaux complexes sur la concurrence. Par exemple, les ORM ont souvent un intérêt stratégique à s'engager avec des assureurs et des PST pour fournir de l'assurance dans le but d'accroître la fidélité de leurs clients, de réduire le taux de désabonnement, de renforcer la notoriété de leur marque et/ou d'accroître le revenu moyen par client. Les PST, quant à eux, sont incités à s'impliquer dans des activités d'assurance, car ils reçoivent une commission pour les transactions qu'ils facilitent en tant qu'intermédiaires. Ces diverses incitations peuvent conduire à des déséquilibres de pouvoir sur le marché et donner lieu à des stratégies visant à tirer parti d'opportunités lucratives plutôt qu'à s'assurer que les produits et les primes sont adaptés au consommateur final. Les contrôleurs doivent être vigilants vis-à-vis des effets pervers des incitations commerciales et doivent chercher à savoir si les services sont combinés et si les consommateurs ont le choix d'acquérir ou non le produit d'assurance d'un PST ou d'un assureur donné. Il peut arriver que les consommateurs n'aient pas le choix et qu'ils soient malgré eux captifs de la domination du marché par une compagnie d'assurance particulière.

Par quelle réglementation les contrôleurs d'assurance peuvent-ils garantir que les intermédiaires d'assurance mobile sont des canaux de distribution responsables pour l'assurance ?

Il existe une grande variété d'approches et d'exigences adoptées par les contrôleurs pour réglementer les intermédiaires d'assurance mobile. Dans certains pays, les PST sont enregistrés en tant que courtiers ou agents de souscription pour l'assurance. Dans d'autres, c'est l'ORM qui est considéré comme le canal de distribution et qui doit donc s'enregistrer en tant qu'agent, ce qui le place de fait sous la supervision de l'autorité de contrôle. En fin de compte, le mode d'enregistrement d'un intermédiaire et la nature de la réglementation à laquelle il doit se conformer dépendent en grande partie des fonctions spécifiques qu'il assure. Outre les fonctions de valeur, l'externalisation doit également être définie. Par exemple, si un assureur externalise une fonction à une autre entité, il doit accepter d'être responsable de cette entité qui émet une assurance en son nom.

Quelle est la répartition des responsabilités entre l'ORM, l'assureur et le PST en matière de propriété des données, et comment ces responsabilités sont-elles établies – par exemple, par la réglementation, par un protocole d'entente ou par d'autres mesures ?

En règle générale, l'ORM, la compagnie d'assurance et le PST déterminent eux-mêmes ces responsabilités dans le cadre des contrats qui les lient. En fonction du régime réglementaire, en supposant qu'il existe une loi générale sur la protection des données, chacune des institutions collectant des informations est responsable de ces informations. À partir du moment où une entité collecte des données, elle relève de la loi sur la protection des données et doit par conséquent se conformer aux règles énoncées dans cette loi. Cela dit, si une compagnie d'assurance externalise une fonction essentielle comme la souscription ou l'administration, elle est généralement responsable de l'entité à laquelle elle a externalisé cette fonction, et par conséquent de toutes les questions de traitement de l'information associées.

L'utilisation du temps de communication d'un service mobile pour le paiement des primes est-elle considérée comme une forme de transfert d'argent électronique ? Existe-t-il des cas de conflit avec la législation sur les transferts d'argent électronique ?

C'est une question difficile qui dépend du contexte du pays. Dans certains pays émergents et en développement, il existe des lois ou des réglementations sur l'argent électronique ; dans d'autres, le temps de communication n'est pas considéré comme un dispositif de paiement électronique, dans d'autres encore la situation reste indéfinie. Par exemple, en Afrique du Sud, les transferts d'argent électronique n'ont pas été inclus dans le cadre réglementaire, car il ne s'agissait pas d'une question très courante sur le marché. La question de savoir si le temps de communication mobile peut être considéré comme une forme d'argent est un sujet encore débattu par de nombreuses banques centrales.

Existe-t-il des questions de confidentialité associées au modèle « freemium » et les données des clients peuvent-elles être utilisées sans le consentement des clients ?

Cela dépend de la manière dont le modèle est mis en œuvre. Si les clients ne donnent pas leur accord explicite pour le partage des données, il y a effectivement un problème de protection des données. Les clients doivent être informés par un moyen simple, transparent et facilement compréhensible de ce qu'il advient de leurs données et de la façon dont elles sont utilisées. Les modes de consentement (ou de refus de consentement) doivent être simples et lorsqu'une personne refuse le partage de ses données, ce choix doit être respecté. Outre les modes utilisés, le cadre réglementaire est également important. Certains pays adoptent une approche de consentement par défaut, ce qui signifie que les données et l'ensemble des informations sur le consommateur peuvent être partagées sauf si le consommateur demande explicitement à ce que ces données ne soient pas utilisées. Cette approche peut être problématique pour les clients. À l'inverse, une réglementation qui prévoit que les données ne peuvent pas être utilisées à moins que le consommateur ne consente explicitement à leur partage/utilisation offre une plus grande protection aux consommateurs.

Initiative Accès à l'Assurance
Hébergée par GIZ Secteur Système financier
Approches de l'assurance
Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Allemagne

Téléphone : +49 61 96 79-1362
Fax : +49 61 96 79-80 1362
E-mail : secretariat@a2ii.org
Site : www.a2ii.org

L'Initiative est un partenariat entre :

Hébergée par :