Réglementer l'*InsurTech* : le rôle des autorités de réglementation dans la gestion des risques liés aux données et à la protection des consommateurs

Compte rendu de consultation téléphonique A2ii – AICA

JAN

2019

Les Consultations téléphoniques sont organisées dans le cadre du partenariat entre l'Initiative Accès à l'assurance (A2ii) et l'Association internationale des contrôleurs d'assurance (AICA) pour fournir aux contrôleurs une plateforme d'échanges sur les expériences et les enseignements relatifs au développement de l'accès à l'assurance.

Introduction

À l'échelle de la planète, la cadence des avancées technologiques est plus rapide que jamais. À ceci s'ajoute l'usage croissant d'une formidable quantité de données. La notion de *big data*[1] est un concept devenu omniprésent. Les assureurs et les entreprises du domaine de la technologie ont la capacité de stocker et d'utiliser ces données pour mieux comprendre les tendances des consommateurs, donc pour pouvoir développer des produits et services de meilleure qualité. Si les technologies orientées données ont favorisé l'essor d'une culture d'innovation, avec, à la clé, la promesse d'un beau potentiel d'appréciation de valeur pour les consommateurs, elles apportent aussi leur lot de nouvelles menaces. Avec le développement, par les entreprises de l'InsurTech, de nouveaux modèles commerciaux alimentés par de grandes quantités de données avec l'espoir d'améliorer l'expérience des consommateurs par la réduction des coûts administratifs, ces mêmes données sont évidemment sujettes à des failles de vulnérabilité. En effet, plusieurs cas de fuites de données ont déjà été rapportés. Le développement de produits essentiellement dopés par un flux de données pourrait également amener certains segments de clientèle à devoir s'acquitter de primes plus élevées, à ne plus faire partie de leur groupe de risque, voire à ne plus être assurés du tout.

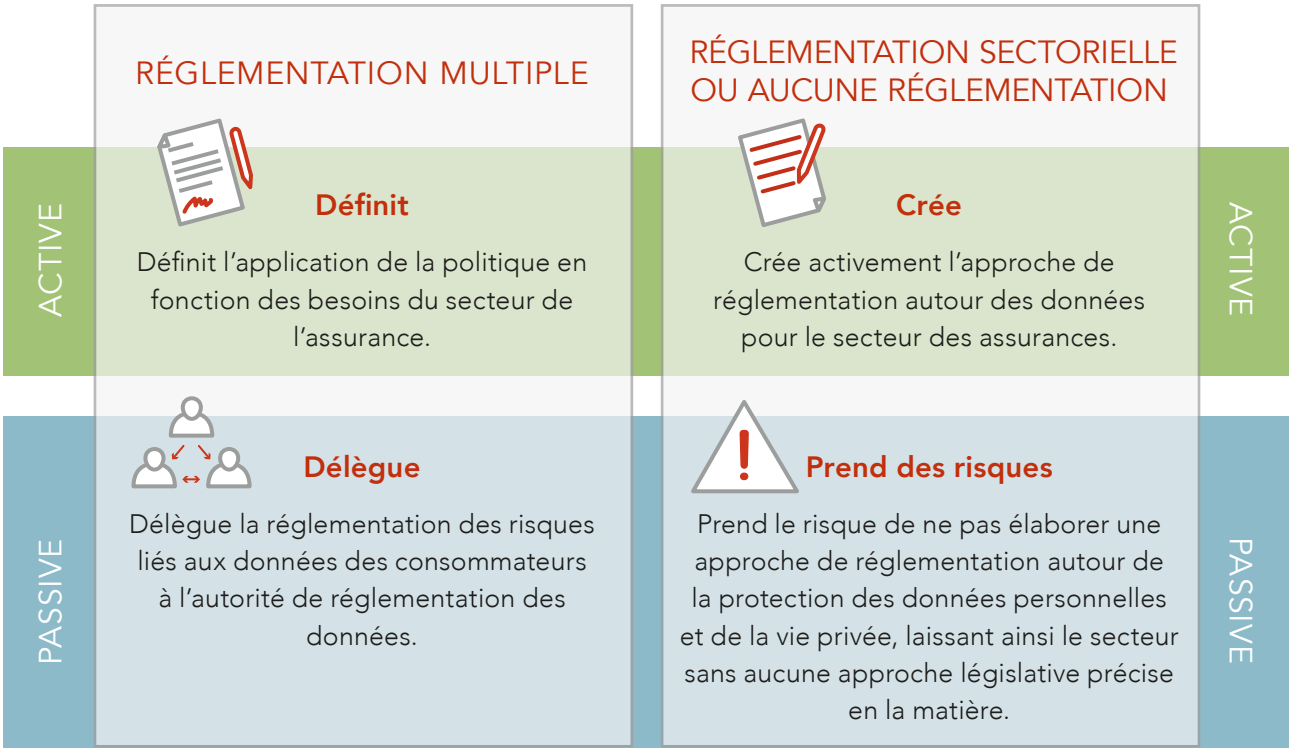
Cet appel s'inspirait du rapport thématique d'A2ii intitulé « la réglementation autour des innovations responsables en matière de traitement des données » *[Regulating for responsible data innovation]*.
Nous encourageons nos lecteurs à consulter la version anglaise du rapport ici. À partir de l'étude, Stefanie Zinsmeyer et Andrea Camargo, spécialistes en communication, ont donné un aperçu des grands risques que présentent les données des consommateurs et du rôle que l'autorité de réglementation peut jouer dans la gestion de ces risques. Les autorités suivantes ont également partagé leurs expériences en la matière : Elias Omondi de l'Autorité kenyane de réglementation des assurances et Tim Mullen de la *National Association of Insurance Commissioners* (NAIC, États-Unis) ont parlé des approches actuellement mises en place pour répondre aux préoccupations des consommateurs en matière de protection des données et de la vie privée. Kathleen Koehn de l'Autorité fédérale de supervision financière (BaFin, Allemagne) nous a également donné un aperçu de l'étude de la BaFin sur l'interaction entre les big data et l'intelligence artificielle. *[Big Data Meets Artificial Intelligence]*.

1 Les *big data* sont des ensembles de données devenus si volumineux qu'ils dépassent l'intuition et les capacités humaines d'analyse et même celles des outils informatiques classiques de gestion de base de données, qui exigent des formes de traitement de l'information novatrices et rentables permettant de gagner en visibilité, de renforcer les processus décisionnels et d'automatiser les processus» (Gartner, 2018). Leur usage le plus conventionnel tourne autour des activités des individus sur les réseaux sociaux, des listes d'appels des téléphones et de l'historique de navigation sur Internet, entre autres. Voir le rapport publié par l'A2ii sur la réglementation autour des innovations responsables en matière de traitement des données ici. (en anglais)

Aperçu de l'étude intitulée « La réglementation autour des innovations responsables en matière de traitement des données »[2]

En facilitant l'innovation, les autorités de réglementation de l'assurance doivent trouver le juste équilibre entre les retombées bénéfiques potentielles pour les consommateurs et leur protection. Les principales répercussions négatives pouvant survenir pour les consommateurs de produits d'assurance sont les suivantes : altération du degré de sécurité et de protection, exclusion et perte de valeur, risque réputationnel, pertes financières, manipulation, atteinte à la vie privée et perte de confidentialité. Ces répercussions peuvent être attribuables à des facteurs de risque tels qu'une gouvernance et des contrôles de données inadaptés, des erreurs, un consentement involontaire ou découlant de mauvais conseils, une faille dans le partage ou l'utilisation des données.

L'étude décrit trois approches courantes en matière de législation à l'échelle de la planète : la réglementation multiple (ou réglementation « omnibus »), la réglementation sectorielle et, l'absence de réglementation. La réponse du contrôleur des assurances dépend du contexte législatif dans lequel il travaille et de ses contraintes. À cela s'ajoutent quatre grandes stratégies de mise en œuvre : définir, créer, déléguer et prendre des risques.



Tiré de l'étude: « Réglementer sur les innovations responsables en matière de traitement des données » (A2ii, 2018) [en anglais][3]

2 *[Regulating for responsible data innovation]*

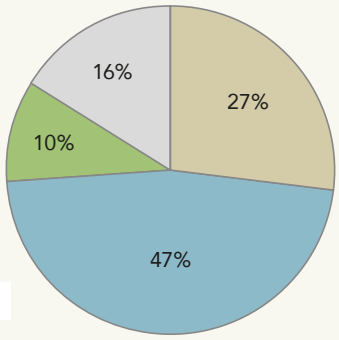
3 *Source: Regulating for Responsible Data Innovation (A2ii, 2018)*

- **Réglementation multiple (omnibus) :** cadre réglementaire transversal sur la protection des données. Dispose souvent d'une autorité de réglementation dédiée, par exemple dans l'UE, en Afrique du Sud, en Nouvelle-Zélande et en Argentine
- **Réglementation sectorielle :** aucune législation nationale ou régionale globale sur la protection des données. Chaque autorité de réglementation du secteur a la responsabilité d'assurer la protection des données personnelles et de la vie privée des consommateurs. Par ex. : aux États-Unis, en Inde et en Chine.
- **Absence de réglementation :** aucune législation ou réglementation régissant la protection des données personnelles et de la vie privée des consommateurs (par ex. au Kenya)

Lors de la consultation téléphonique, les autorités de contrôle ont également répondu à un petit sondage visant à déterminer la façon dont les autorités de réglementation gèrent les risques liés aux données personnelles des consommateurs et abordent la question de la réglementation. Les questions et réponses sont compilées dans les diagrammes ci-dessous :

Quelle appréciation donneriez-vous aux risques relatifs aux données personnelles des consommateurs dans vos juridictions?

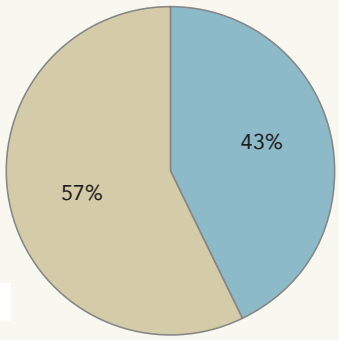
- Très bonne
- Bonne
- Faible
- Très faible



79 répondants

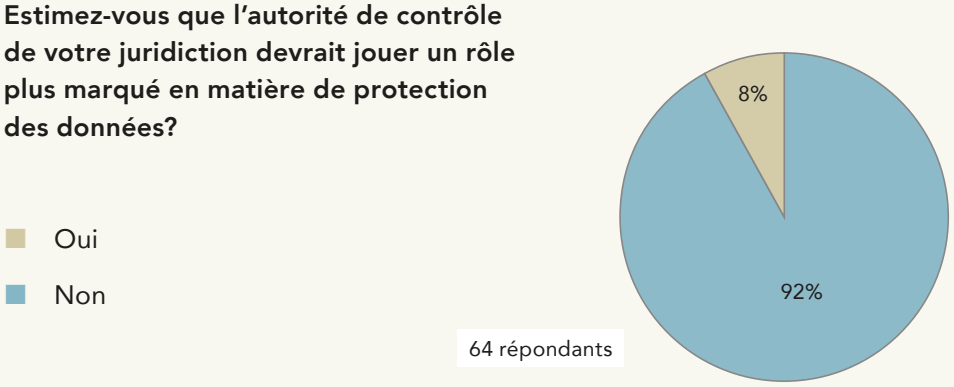
L'autorité de contrôle de votre juridiction a-t-elle adopté une approche proactive en matière de réglementation des données? («définit» ou «crée» la réglementation autour des données)

- Oui
- Non



69 répondants

Estimez-vous que l'autorité de contrôle de votre juridiction devrait jouer un rôle plus marqué en matière de protection des données?



ÉTUDE DE CAS : LE KENYA

L'étude de cas sur le Kenya nous a été présentée par Elias Omondi, de l'*Insurance Regulatory Authority.*

Le Kenya ne dispose actuellement d'aucune législation spécifique en matière de protection des données. Cependant, un projet de loi a été déposé au Parlement en 2015. La priorité placée sur l'inclusion financière et la mise en place d'un environnement axé sur l'innovation au Kenya a rendu possible l'arrivée de nouveaux modèles commerciaux, mais elle a également soulevé des questions sur la manière de fournir une couverture d'assurance, de promouvoir l'innovation et la concurrence tout en garantissant la protection des consommateurs. À cet égard, l'Autorité de réglementation des assurances du Kenya (IRA) assume trois rôles importants qui visent à équilibrer les risques et les avantages pour le consommateur :

- Garantir l'impartialité, la protection et la stabilité du secteur de l'assurance
- Protéger les intérêts des assurés et des bénéficiaires
- Promouvoir le développement du secteur des assurances

En l'absence d'un régime explicite de protection des données, l'IRA applique une stratégie de type **création** [« créer »] afin de gérer les risques relatifs à l'usage des données des consommateurs. Les stratégies de mise en œuvre adoptées par l'IRA comprennent :

- **Des directives sur les pratiques du marché :** Ceci implique de modifier et d'interpréter les directives actuelles en matière de pratiques du marché afin d'assurer un degré de protection adéquat des données personnelles des consommateurs contre les risques.
- **De traiter équitablement les clients.** Ce modèle de protection des consommateurs (le TCF) vise à élever les normes dans la manière dont les entreprises exercent leurs activités en introduisant des modifications qui bénéficient aux consommateurs et qui contribuent à renforcer leur confiance dans le secteur des services financiers.
- **Une *sandbox* (ou environnement de test) sur la réglementation.** L'IRA a élaboré un projet de politique réglementaire à mettre à l'essai dans un environnement de test. Cette politique permettra de mettre en place un environnement expérimental dans le cadre duquel les entreprises issues de la FinTech ou de l'InsurTech pourront mettre à l'essai leurs idées et innovations en matière de conception, de développement et de distribution de produits, tout en limitant les conséquences d'un échec.
- **Des directives sur les produits d'assurance.** Les directives fournissent des indications sur les principes à respecter autour de la conception, de la tarification, de la commercialisation, des renseignements à fournir, ainsi que sur la manière dont

les demandes d'émission de produits nouveaux ou reconditionnés sont présentées à l'autorité de réglementation, de manière à permettre à une entreprise de tester les nouveaux produits.

Si vous avez des questions ou si vous souhaitez en savoir plus sur l'approche de l'IRA, vous pouvez les adresser à eomondi@ira.go.ke

ÉTUDE DE CAS : ALLEMAGNE

Kathleen Koehn de l'Autorité fédérale de supervision financière (BaFin, en Allemagne) nous a présenté un aperçu et les conclusions clés de l'étude de la BaFin sur l'interaction entre les big data et l'intelligence artificielle.

Voici les grandes questions que la BaFin a souhaité aborder dans le cadre de l'élaboration de l'étude : quelles seraient les répercussions potentielles de l'utilisation des big data, de leur analyse poussée et de l'intelligence artificielle sur le marché financier ainsi que sur la BaFin en qualité de contrôleur ? Quelle serait la nature du contrôle à fournir à l'avenir et faudrait-il ajuster les exigences en matière de réglementation ?

L'étude met en évidence le fait qu'une attention préalable en matière de contrôle et de réglementation est essentielle dans le cycle de l'innovation, en particulier dans les cas impliquant l'utilisation des big data et de l'intelligence artificielle. C'est parce que l'utilisation des big data et des outils connexes ont un effet d'autorenforcement et d'autonomie de plus en plus croissant, en ce sens que les consommateurs adoptent très rapidement les nouveaux processus, produits et services numériques, ce qui génère une abondance de données, en tout cas dans une quantité beaucoup plus importante que ce que les entreprises sont en mesure de traiter ou d'absorber. Il est donc vital que les autorités de contrôle agissent rapidement. Le recours aux big data pourrait avoir un impact sur la stabilité financière, le contrôle microprudentiel et la protection des consommateurs. Parmi les principes réglementaires mis en place par la BaFin pour pouvoir faire face aux avancées des big data et de l'intelligence artificielle, on peut citer : la neutralité technologique appliquée à l'ensemble des acteurs du marché (même type d'activité, mêmes risques, mêmes règles), l'adoption d'un cadre réglementaire basé sur des principes où tous les risques des nouvelles technologies sont pris en compte, et le développement des capacités dans les domaines des big data et de l'intelligence artificielle en qualité de contrôleur.

Pour aller plus loin dans l'étude de la BaFin sur la relation entre l'intelligence artificielle et les big data, vous avez accès à la version en anglais ici.

ÉTUDE DE CAS : LES ÉTATS-UNIS

L'étude de cas sur les États-Unis nous a été présentée par Tim Mullen de la *National Association of Insurance Commissioners* (NAIC).

La NAIC est l'organisme américain d'appui à la normalisation et à la réglementation. En réglementant les innovations responsables en matière de traitement des données, la NAIC encourage l'innovation, tout à fait consciente du fait que les avantages pour les consommateurs peuvent découler d'un marché en pleine évolution et du mode de fonctionnement des compagnies d'assurance. Cependant, tout en encourageant l'innovation, il est clair que l'aspect de la protection du consommateur est essentiel. Pour garantir cela, la NAIC soutient que les compagnies d'assurance doivent faire preuve de transparence vis-à-vis des autorités de réglementation en ce qui concerne les données et les algorithmes utilisés et leur impact sur les consommateurs.

Certains des avantages pour les consommateurs découlant directement de l'exploitation des données permettent d'obtenir des évaluations plus précises sur le risque de perte, de raccourcir les délais de traitement des devis et des sinistres, de mieux gérer les risques et prévenir les pertes. La NAIC souligne également les préoccupations suivantes formulées par les consommateurs : exactitude et exhaustivité des données, divulgation aux consommateurs, consentement des consommateurs, confidentialité et cybersécurité. Pour aborder les questions de la protection des données et de la vie privée, la NAIC a adopté un ensemble de lois et réglementations types : *Standards for Safeguarding Consumer Information Model Regulation* (2000), *Privacy of Consumer Financial and Health Information Regulation* (2002) et *Insurance Data Security Model Law* (2017). Par ailleurs, la structure des comités de la NAIC est régie par plusieurs groupes de travail qui examinent notamment la manière dont les entreprises utilisent les données et les nouvelles technologies. Ceci comprend un groupe de travail sur l'innovation et les nouvelles technologies et un second groupe de travail sur les big data.

Dans le contexte du marché américain, la NAIC a présenté une étude sur un cas de fuite de données dans une compagnie d'assurance maladie américaine qui a affecté près de 80 millions d'utilisateurs. En réponse à cette faille, les autorités de réglementation ont procédé à un examen en quatre étapes :

- **Intégration :** Interaction avec le personnel de la compagnie et les juridictions de l'État concerné et sélection des experts en cybersécurité pour remédier à la fuite de données.
- **Évaluation préliminaire :** Interviews du personnel clé et des experts en cybersécurité de la compagnie. Les autorités américaines de réglementation des assurances dans les États concernés ont également obtenu de la documentation technique et interne de l'assureur afin de leur permettre de mieux comprendre la nature de l'environnement de sécurité de la compagnie et les efforts déployés après l'effraction pour évaluer l'étendue des vulnérabilités.

- **Évaluation de la faille de données :** L'équipe de spécialistes a pu examiner l'étendue de la fuite telle qu'elle avait été effectuée par la compagnie. Cette analyse a été réalisée pour dégager toutes les conclusions sur le plan technique. Les spécialistes ont également pris le temps d'évaluer les mesures prises par la compagnie pour détecter, contenir et réagir à la fuite de données.
- **Évaluation de la cybersécurité :** Les experts en cybersécurité ont procédé à un examen approfondi des contrôles en la matière effectués par la compagnie et qui étaient en place avant et après la fuite de données. Ces mêmes experts ont également effectué un test pour déterminer si les protocoles de cybersécurité de la compagnie étaient efficaces dans la détection et la prévention d'une éventuelle nouvelle faille.

Les conclusions de l'examen ont permis de révéler le niveau de défense de la compagnie et son degré de préparation en matière de cybersécurité avant la faille. Les constatations révèlent que la compagnie avait mis en place un programme d'intervention de cybersécurité adéquat et a su réagir rapidement pour remédier à la fuite de données. En ce qui concerne les conclusions post faille, la compagnie a mis en place de nouvelles mesures et rehaussé ses normes afin de réduire le risque d'occurrence de faille de ce type à l'avenir. Les mesures correctives concernent principalement les consommateurs individuels, la compagnie les ayant informés des mesures mises en place pour pallier la situation. La compagnie avait également informé la police et les autorités de réglementation de l'assurance.

Pour toute question ou pour en savoir plus sur l'approche et l'étude de cas de la NAIC, vous pouvez contacter TMullen@naic.org

Questions et discussion

› **Étant donné que les autorités de réglementation appliquent des approches différentes en matière de protection des données personnelles et de la vie privée, comment la NAIC coopère-t-elle avec d'autres acteurs du secteur financier aux États-Unis pour traiter les cas de cybersécurité et autres défis liés à la protection des données ?**
Les organismes de réglementation des assurances des États concernés coordonnent régulièrement leurs activités avec les autorités de réglementation financière aux niveaux fédéral et des états afin de faciliter la communication et de rechercher des moyens de coordonner efficacement les approches réglementaires en matière de gestion et d'évaluation des risques de cybersécurité, mais aussi pour répondre à d'autres préoccupations en matière de sécurité et de risque pour les données. La démarche implique de passer par le FBIIC (Financial and Banking Information and Infrastructure Committee), un comité réunissant les autorités de réglementation financière du niveau fédéral et des États, créé dans le but de renforcer la coordination et la communication entre les divers organes de réglementation du secteur financier afin de consolider la fiabilité et la sécurité de l'infrastructure du secteur financier.

› **Dans la mise en œuvre de l'approche multiple (ou « omnibus ») à la réglementation, comment la BaFin coopère-t-elle avec les autorités de protection des données de leur juridiction ?**
Le cadre juridique en vigueur sur le marché allemand définit les fonctions des différentes autorités. Le rôle de contrôle en matière de sécurité des données ne s'inscrit pas dans le mandat de la BaFin.
Par conséquent, il serait souhaitable que les autorités de contrôle se concertent davantage avec les autorités compétentes déjà familiarisées avec les domaines nouveaux et émergents tels que les big data et l'IA. Cela favoriserait l'échange de compétences, de connaissances et d'opinions et permettrait de réduire les éventuels doublons. L'expérience de la BaFin a été positive dans le renforcement de la coopération avec l'Office fédéral de la sécurité des technologies de l'information (BSI).

The Initiative is a partnership between:

Hosted by:

Access to Insurance Initiative
Hosted by GIZ Sector Project
Financial Systems Approaches to Insurance
Deutsche Gesellschaft für Internationale
Zusammenarbeit (GIZ) GmbH
Dag-Hammarskjöld-Weg 1-5
65760 Eschborn, Germany

Telephone: +49 61 96 79-1362
Fax: +49 61 96 79-80 1362
E-mail: secretariat@a2iiorg
Internet: www.a2ii.org

a2ii_org

Promoting access to responsible, inclusive insurance for all.