Mutuelles en danger : Pourquoi le manque de souveraineté des données est critique.

Avertissement *: Souveraine Tech revendique par vocation une approche transpartisane. Seule nous oblige la défense des intérêts supérieurs de notre pays. Nous proposons ainsi un lieu de « disputatio » ouvert aux grandes figures actives de tous horizons. La parole y est naturellement libre et n'engage que ceux qui la prennent ici. Cependant, nous sommes bien conscients des enjeux en présence, et peu dupes des habiles moyens d'influence plus ou moins visibles parfois mis en œuvre, et dont tout un chacun peut faire l'objet, ici comme ailleurs. Nous tenons la capacité de discernement de notre lectorat en une telle estime que nous le laissons seul juge de l'adéquation entre le dire et l'agir de nos invités.*

Vendredi 26 avril 2024

Jérémy Marlin est président et co-fondateur de Stan, « solution digitale et souveraine ».

1/ Quelle est la mission de Stan ?

Stan est une digital factory. Nous construisons des solutions numériques sur-mesure, principalement pour les acteurs de l'assurance de personnes (mutuelles, assureurs, institutions de prévoyance, courtiers, etc…). On automatise et on accélère des process traditionnels grâce à nos robots, notre IA maison et nos équipes basées en France. Concrètement, nous

transformons des process de 20 semaines à 2 minutes. Ce bond technologique améliore même la relation avec les clients finaux puisque 87% d'entre eux adhèrent chez l'assureur quand notre solution est embarquée. Récemment nous avons produit un rapport avec l'Ecole de Guerre Economique Junior Conseil intitulé « Assureurs santé : nouveaux tiers de confiance numérique ? » qui met en lumière notre l'importance de la donnée gérée pas ses acteurs, les normes européennes en vigeur ainsi que les notions de souveraineté impactées par leS « Patriot Act », »FISA » et « Cloud Act ».

2/ Qu'est-ce qui vous a poussé à produire le rapport « Assureurs santé : nouveaux tiers de confiance numérique ?«

La guerre économique qui nous entoure a mis en avant les enjeux de dépendance et la capacité de chaque état à maintenir sa souveraineté alimentaire, industrielle, technologique et numérique… à mon sens, il y a un acteur qui est souvent oublié qui est « la mutuelle ». La « mutuelle » c'est l'acteur qui connaît votre passé, votre présent et votre avenir. On associe aisément ces organismes aux coûts, aux augmentations annuelles… mais pas forcément au trésor de données qu'ils peuvent brasser au quotidien. Alors que se passerait-il si ces données étaient compromises ou dérobées par des hackers ?

Les cybercriminels savent qu'il est complexe d'attaquer dans grands-groupes de front alors pourquoi ne pas passer par des acteurs « périphériques ». La « mutuelle » se présente donc comme une cible de choix.

Attention le terme « mutuelle » est très largement dévoyé car en fait cela touche une multitudes d'acteurs avec des natures très différentes qui peuvent êtres des assureurs, des institutions de prévoyance, des mutualistes, des courtiers, des grossistes en courtage, des délégataires de gestion…

3/ Justement, que pensez-vous de la récente cyber-attaque qui a touché les acteurs de tiers-payant Viamedis et Almerys ?

Viamedis et Almerys gèrent les flux de remboursements pour une grande majorité des assureurs, mutuelles, institutions de prévoyance et courtier. Pour faire simple, entre votre mutuelle et votre pharmacien… il y a un tiers-payant comme Viamedis et Almerys.

D'après France Verif, l'outil de surveillance des violations de données, 96 000 usurpations d'identité ont été recensées le 16 février. Ce chiffre n'a fait que croître par la suite : 124 000 le 22 et 23 février et le 26 février, France Verif dénombrait 217 000 usurpations. Il resterait encore 32,7 millions de personnes dont les données n'ont pas encore été vendues.

Selon un communiqué de la CNIL, « les données concernées sont, pour les assurés et leur famille, l'état civil, la date de naissance et le numéro de sécurité sociale, le nom de l'assureur santé ainsi que les garanties du contrat souscrit. » La fuite de ces informations très sensibles amène la commission à alerter les particuliers sur les risques d'hameçonnage ou même d'usurpation d'identité. « Les données telles que les informations bancaires, les données médicales, les remboursements santé, les coordonnées postales, les numéros de téléphone ou encore les courriels ne seraient pas concernées par la violation », selon la CNIL. Reste à voir dans dans le temps, ce qu'il en est…

Cette cyber-attaque va laisser des traces pour les prochaines négociations avec les clients entreprises qui vont revoir leurs contrats santé. Ces sujets sont visés par les partenaires sociaux qui sont en demande de transparence sur la gestion des données personnelles. Apparaître comme un acteur incapable de gérer des données sensibles pourra être préjudiciable. Il ne faut pas sous-estimer le #shaming qui

peut faire des couler des grandes marques.

Ces acteurs doivent remporter des parts de marché en répondant à des appels d'offres souvent rédigés par des cabinets d'actuariat. Leur mission est d'encadrer et piloter ces appels d'offres autour de la solidité technique et financière, de prix et serviciels… mais aucunement de vérifier la solidité cyber de ceux-ci.

Allons-nous voir apparaître des nouveaux critères en terme de cyber ? (politique d'achat IT, hébergement souverain ?, par de la sous-traitance auprès d'ESN off-shore ?) Finalement, les choix technologiques de ces protagonistes sont aussi des engagement RSE. Consommer des services souverains, c'est aussi consommer local.

De plus, ces acteurs « assurantiels » ont l'habitude de la règlementation et font l'objet de contrôles rigoureux par l'AMF, ACPR, la CNIL… Il est a parié qu'il faudra compter avec de nouveaux gendarmes comme l'ANSSI. Selon l'Argus de l'assurance du 9 janvier 2024, l'ACPR publie son enquête 2023 sur l'externalisation des activités critiques ou importantes. En recourant fortement à cette méthode, le secteur assurantiel augmente les risques opérationnels.

Allons-nous voir un renversement des politiques d'achats et SI en faveur d'une souveraineté numérique pour se prémunir de lois extraterritoriales américaine (Cloud act/FISA)?

4/Mais en quoi le Cloud Act et le FISA remettent-ils en question la souveraineté et la protection des données européennes et françaises ?

L'émergence régulière de solutions *cloud* dites de confiance, souvent issues de partenariats avec un géant américain, pose un problème sémantique : l'utilisation d'un hébergement américain ne permet pas l'application des normes françaises et européennes sur la protection des données. Même dans le cas où les données sont stockées en France, l'extraterritorialité du

droit américain établie par le *Cloud Act* et le *FISA* leur permettent de s'y appliquer. Ces prérogatives donnent un accès complet de ces données à l'État américain. Pour être concret, stocker des données de santé en utilisant des solutions AWS ou Microsoft, c'est mettre à disposition de nos alliés, des informations hautement confidentielles. Cette situation permet aux autorités américaines d'accéder à des données stratégiques et sensibles, leur conférant un avantage concurrentiel certain.

Il est intéressant de voir la mode actuelle qui est d'inciter des cadres à utiliser de l'IA. Comment expliquer qu'utiliser « Copilote » n'est pas forcément le meilleur outil quand on gère la santé d'entreprises hautement sensibles pour le pays ?

Quelques éléments de compréhension :

Le *Cloud Act** *ou *Clarifying Lawful Overseas Use of Data Act*, adopté aux États-Unis en 2018, autorise les autorités américaines à accéder aux données stockées par les fournisseurs de services informatiques, même à l'étranger. Cette législation impose aux organismes soumis à ces règles, l'obligation de transférer toutes les données demandées par les autorités américaines, sans délai et sans possibilité pour les personnes concernées de s'y opposer, ni d'être informées de la consultation. Pour les européens, le *Cloud Act* remet en question les principes de protection des données établis par le RGPD, soulevant des préoccupations majeures concernant la souveraineté des données et la confiance dans les services de *cloud* américains.

Le *FISA** *ou Foreign Intelligence Surveillance Act, amendé en 2008, notamment avec l'introduction de l'article 702. Cette loi donne au gouvernement américain le pouvoir de surveiller les communications électroniques des individus à l'étranger. Elle impose aux fournisseurs de services de communication électronique, de services informatiques à distance et aux entreprises de télécommunications de coopérer en leur donnant

l’accès à leurs données.

La seule réponse face au *Cloud Act* et au *FISA*, en tant que français ou européen, est de garantir que le *cloud* ne soit pas utilisé, directement ou indirectement, par des personnes relevant de la juridiction américaine. Cependant, devant le constat que 71% des entreprises françaises préfèrent les solutions de *cloud* américaines, la question de la souveraineté des données reste largement en suspens.

5/ Quelles sont les initiatives françaises pour développer un hébergement cloud souverain ou de confiance, quelles difficultés rencontrent-elles face au droit américain, et comment certains acteurs français tentent-ils de garantir la souveraineté et la protection des données en conformité avec les réglementations européennes?

Face aux conséquences de cette dépendance, les Français s’efforcent de développer un hébergement souverain ou de confiance pour faire émerger plusieurs alternatives sur le marché national. Thalès et Orange ont par ailleurs tenté de monter ensemble un cloud souverain, Cloudwatt, sans succès. Cet échec est imputable au manque d’acculturation du marché. Les entreprises françaises n’étaient pas encore prêtes, et encore moins sensibilisées, à l’arrivée de ce cloud souverain.

Après cet échec, Orange s’associe avec Capgemini et Microsoft pour construire une offre de cloud de confiance : Bleu. Le but est de profiter de l’architecture de Microsoft tout en protégeant les données selon les réglementations françaises et européennes. Cette offre garantit que les données sont stockées en France et que les clients ont un contrôle total sur leurs données. Cependant, Microsoft est une entreprise américaine et reste donc toujours soumise au droit américain (Cloud Act). Cela signifie que les autorités américaines peuvent avoir accès aux données des français. Ainsi, l’offre de confiance Bleu ne parvient pas à garantir pleinement la

protection des données contre les autorités américaines en raison de l'application du Cloud Act dans ce contexte.

En parallèle, des initiatives telles que S3NS, une co-entreprise entre Thales et Google Cloud, cherchent à offrir des solutions de cloud de confiance aux institutions publiques et aux entreprises privées françaises, tout en respectant les réglementations européennes en matière de protection des données.

Par ailleurs, plusieurs acteurs français offrent déjà des alternatives aux hébergements étrangers. OVHcloud, leader européen du cloud, met en avant sa certification SecNumCloud de l'ANSSI et son expansion mondiale. Outscale, entreprise française de cloud computing, insiste sur la souveraineté, la durabilité et la confiance numérique, tout en étant qualifiée SecNumCloud. NumSpot, filiale de Docaposte, propose également une solution d'hébergement souverain et de confiance, garantissant la localisation des données en France et la conformité aux réglementations européennes. Enfin, Cloud Temple, spécialisé dans l'hébergement et l'infogérance d'applications d'entreprise critiques, se distingue également en mettant l'accent sur la sécurité et la souveraineté numérique, renforcée par des partenariats stratégiques avec des acteurs majeurs du secteur.

6/ Comment GAIA-X, une initiative européenne, vise-t-elle à contrer le Cloud Act américain et à promouvoir la souveraineté des données conformément au RGPD, et quelles sont les implications du retrait de Scaleway et de l'implication de géants non européens dans ce projet?

Pour faire face à cette situation favorable aux Américains, la France et l'Allemagne avaient lancé en 2019 GAIA-X. Cette initiative européenne vise à mettre en place une infrastructure cloud sécurisée conforme aux règles du RGPD. Son but est notamment de relever les défis posés par le Cloud

Act et de promouvoir différents principes tels que la transparence, la confidentialité, la portabilité des données et l'interopérabilité. Depuis 2021, GAIA-X ravive le débat sur la souveraineté des données, notamment après le retrait de Scaleway, une entreprise initialement impliquée dans le projet. Ce retrait fait suite à l'annonce du partenariat pour la gouvernance du conseil d'administration, impliquant des entreprises non européennes telles que Huawei, Alibaba, Microsoft et AWS (Amazon Web Services). Il est à noter que Scaleway faisait partie des trois premières entreprises françaises initialement prévues pour ce projet, aux côtés d'OVH et d'Outscale.

Une fois de plus, les géants américains sont au cœur du processus, ce qui pourrait leur permettre de mettre en œuvre le Cloud Act pour accéder aux données des européens. Cette situation soulève de nombreuses interrogations, notamment celle concernant la capacité des européens à créer une infrastructure adéquate sans l'aide des entreprises américaines.

Les Européens ripostent au Cloud Act avec leur projet e-evidence. Cette réglementation permettrait aux autorités de l'Union Européenne de demander un accès direct aux preuves électroniques, indépendamment de la localisation des données. Les données pourront être demandées de la même manière que pour le Cloud Act, à condition qu'une entreprise fournisse des services dans l'UE, qu'elles soient établies dans un État membre ou représentées par une entité concernée.

7/ Quels obstacles freinent l'adoption des solutions de cloud souverain ou de confiance en France, et comment les préoccupations relatives à la capacité, aux coûts, à la réglementation, et à la fidélité aux fournisseurs actuels influencent-elles la décision des entreprises?

Plusieurs obstacles permettent d'expliquer la réticence d'adopter des solutions de *cloud* souverain ou de confiance en

France. Tout d'abord, le manque de connaissance et de compréhension du concept d'hébergement souverain et de ses avantages constitue un défi majeur. La taille et la capacité des infrastructures des fournisseurs nationaux suscitent également des interrogations sur leur capacité à rivaliser avec les géants internationaux en termes de disponibilité et de fiabilité des services. Les performances des *clouds* souverains sont également examinées de près, avec des doutes sur leur capacité à fournir des performances équivalentes, voire supérieures, à celles des *hyperscalers* (géants du *cloud*, qui fournissent des services de *cloud* à grande échelle). De plus, les entreprises doivent tenir compte des bénéfices de leurs choix d'infrastructure, craignant que les coûts des solutions de *cloud* souverain ne soient trop élevés par rapport aux offres concurrentes des *hyperscalers*, ce qui pourrait impacter leur rentabilité et leur compétitivité.

Les barrières légales et réglementaires, notamment en ce qui concerne la souveraineté des données et les impératifs de conformité, représentent également des obstacles significatifs pour les organisations qui envisagent d'adopter ces solutions. Ces contraintes juridiques et réglementaires imposent des exigences strictes en matière de gestion et de protection des données. Ces exigences complexes peuvent engendrer des ralentissements dans le processus d'adoption en raison de la nécessité de se conformer à des normes spécifiques, ce qui peut parfois être perçu comme une charge administrative supplémentaire.

En outre, les entreprises ont tendance à rester fidèles à leurs fournisseurs de services *cloud* actuels plutôt que d'explorer de nouvelles options. Elles privilégient la relation établie et les investissements déjà réalisés. Cette fidélité peut découler de divers facteurs, tels que la familiarité avec les plateformes existantes, la confiance dans leur fiabilité et leur sécurité, ainsi que les investissements financiers et temporels déjà réalisés pour s'adapter à ces

solutions. En conséquence, cette tendance freine parfois l'exploration de nouvelles options de *cloud* souverain ou de confiance.

Outre les considérations techniques et réglementaires, les décisions concernant l'adoption d'un *cloud* souverain sont également influencées par des facteurs commerciaux. Les entreprises doivent évaluer leur capacité à maintenir leur compétitivité sur le marché mondial, tenir compte des implications du libre-échange sur leurs opérations et répondre à l'exigence d'innovation constante.

8/ Quels sont les défis de souveraineté et de protection des données auxquels fait face le Health Data Hub français en utilisant Azure de Microsoft, et comment des entreprises françaises offrent-elles des alternatives conformes aux normes européennes?

Dans le domaine de la santé, le *Health Data Hub* (HDH) ou Plateforme des données de santé (PDS), instauré le 30 novembre 2019, a pour objectif de simplifier le partage des données médicales afin de promouvoir la recherche. Sa mission inclut la collecte, l'organisation et la mise à disposition des données de santé, ainsi que la promotion de l'innovation dans ce domaine. En tant que responsable du traitement du Système National des Données de Santé (SNDS), conjointement avec la Caisse Nationale d'Assurance Maladie (CNAM), le HDH stocke et met à disposition les données de la base principale du SNDS et du catalogue du SNDS.

Cependant, le choix initial du *cloud d'Azure* de *Microsoft* pour héberger le PDS a soulevé des préoccupations quant à la conformité aux lois européennes sur la protection des données. Bien que les centres de données *d'Azure* soient situés aux Pays-Bas, *Microsoft*, en tant qu'entreprise américaine, est soumise aux lois extraterritoriales des États-Unis, telles que le *Cloud Act* et la loi *FISA*. Suite à la pression de la CNIL et du Conseil d'État, le gouvernement français a promis de migrer

la plateforme vers une solution européenne, mais ce processus a été retardé à plusieurs reprises.

En attendant, plusieurs acteurs français se positionnent pour héberger le PDS et son équivalent européen, l'Espace Européen des Données de Santé (EHDS). Des entreprises telles *qu'OVHcloud, NumSpot,* et *Cloud Temple* offrent des solutions alternatives de cloud souverain, conformes aux réglementations européennes en matière de protection des données. *OVHcloud*, notamment, s'est publiquement proposé pour accueillir le PDS français, tandis que *NumSpot* montre également un intérêt pour le marché. Quant au *Cloud Temple*, certifié *SecNumCloud* et reconnu comme un leader des services *cloud* managés, considère le PDS comme un dossier emblématique pour l'année 2025, sous réserve de la tenue de l'appel d'offres.

La question de la souveraineté des données de santé en France soulève des défis complexes, notamment en raison de la décision de confier l'hébergement des données médicales des citoyens français à *Microsoft Azure*. Cette décision, bien que suscitant des inquiétudes quant au respect des normes de sécurité établies par le *SecNumCloud* de l'ANSSI, souligne également les efforts déployés pour réduire la dépendance aux grandes entreprises technologiques américaines.

Les initiatives telles que le cloud souverain, le cloud de confiance et les certifications de souveraineté visent à fournir des alternatives conformes aux normes européennes en matière de protection des données. Cependant, la réalité montre que ces solutions sont souvent associées à des partenariats avec des géants du cloud américains, ce qui peut compromettre la protection des données des Européens en vertu du Cloud Act et du FISA.

En France, des acteurs du cloud tels qu'OVHcloud, NumSpot et Cloud Temple se positionnent pour offrir des alternatives de cloud souverain. Malgré les défis et les délais, le secteur de la santé poursuit ses efforts pour garantir la protection des

données de santé et promouvoir l'innovation, en mettant l'accent sur les solutions d'hébergement conformes aux normes européennes.

9/ En conclusion, quel est votre message pour les entreprises et le secteur de l'assurance de personnes concernant la souveraineté des données ?

Arrêtons de jouer la défense. Il est temps d'adopter une posture proactive en matière de souveraineté des données. Ce n'est pas seulement une question de conformité ou de sécurité, mais une question d'identité et d'indépendance. La souveraineté des données est le fondement sur lequel nous construirons un avenir numérique sûr et autonome. Comme pour les notions de RSE qui ont atterries dans les choix de solutions, la souveraineté doit désormais intégrer les valeurs des entreprises qui gèrent nos données de santé.

Reste à définir, qu'est-ce que la « souveraineté », est-ce qu'elle se limite aux frontières de notre état ou bien à l'Europe des nations ? Beau sujet d'actualité en ces temps d'élections européennes.

10/ Question subsidiaire : Pouvez-vous citer en vrac 10 références, personnalités, ouvrages, événements, citations qui vous semblent illustrer l'idée de souveraineté ?

Personnalités :
– Christian Harbulot, Directeur de l'EGE
– Le Général de Gaulle

Livres :
– « Ces guerres qui nous attendent 2030-2060 » aux Éditions des Équateurs
– Les futurs de Liu Cixin aux Editions Delcourt

Événements :
– Déclaration d'indépendance des États-Unis en 1776
– Révolution française de 1789

Séries :
– House of Cards
– The Crown

Oeuvre musicale :
– La Marseillaise de Rouget de Lisle

Citation :
« L’État, c’est moi » – attribuée à Louis XIV, cette phrase illustre l’idée absolutiste de la souveraineté royale.