Rencontres du Risk Management AMRAE 2020

Atelier A3

"On n'a pas de pétrole mais on a des données ….". Le nouvel enjeu stratégique pour l'entreprise

Panel d'intervenants

Modérateur

Eric Contégal	Responsable Audit Interne et Risques Délégué à la protection des données

Intervenants

Laurent Inard	Associé Responsable du département Financial Advisory
Sanaa Nouri	Senior Manager Risk Management
Vladimir Rostan d'Ancezune	Avocat associé Office Head pour la France

28èmes RENCONTRES DU RISK MANAGEMENT AMRAE
DEAUVILLE DU 05 AU 07 FÉVRIER 2020

Qu’est-ce qu’une donnée ?

- Une donnée est :
  - la représentation d'une information dans un programme
  - relative à du texte, du numérique, des images, des sons, …
- France
  - Article 2 de la loi informatique et libertés
  - sphère privée / sphère professionnelle
- Union Européenne
  - CJUE 6 octobre 2015 : Safe Harbor invalidé > Privacy Shield 1er juillet 2016
  - 27 avril 2016 : RGPD
- Adresses IP : une donnée comme une autre ?
  - CJUE
  - Cour fédérale d’Australie

Data et Valeur

Q1 : Dispose-t-on de référentiels de prix pour les Data ? (1/3)

- Sur le **Dark Net**, les data (notamment les data personnelles) ont depuis longtemps des prix, voire un marché

Comptes de services de paiement en ligne*	Comptes bancaires* (virnt à l'intl possibles)	Services de contenus en ligne*	Infos personnelles**
17 à 43 € (comptes < 900€)	**170 €** (comptes ≈ 2 000€)	**0.5 à 0.9 €** (streaming video)	**0.05 à 3 $** (n°SS qlque ou spéc.)
175 à 260 € (comptes < 7 000€)	**1 000 €** (comptes ≈ 17 000€)	**6.5 à 13.0 €** (chaînes TV)	**10 à 24 $** (n° de carte de crédit, yc informations perso)
			100 $ le FullZ

**: McAfee Labs d'Intel Security, « The hidden data economy », 2015*

*** : Fullz (SIM hijacking anti-double authentification), 2018*

Data et Valeur

Q1 : Dispose-t-on de référentiels de prix pour les Data ? (2/3)

- Quid du **prix fixé par les propriétaires** de données personnelles eux-mêmes* :

Identifiants et mots de passe **69 €**	Informations de santé **55 €**	N° de SS **51 €**	N° de CarteB **33 €**	Historique d'achat **19 €**
Géolocalisation **15 €**	Adresse postale **12 €**	Photos & Videos **11 €**	Etat Civil **8 €**	Sexe & Nom **3 €**

*:TrendMicro Ponemon Institute, 2015. Enquête sur 1 903 personnes dans 18 pays (Europe, USA, Japon)

Data et Valeur

Q1 : Dispose-t-on de référentiels de prix pour les Data ? (3/3)

- A noter que commencent à se développer des **Data Market Place légales**, dans lesquelles des fournisseurs de data les mettent à disposition d'autres acteurs.
- Par exemple, Dawex permet d'échanger ou monétiser ses données
- Ces marchés n'en sont qu'à leurs débuts, il est encore très compliqué même pour l'animateur de ce type de plateforme de tirer des métriques fiables sur les prix de telle ou telle data.

ON A PAS DE PÉTROLE MAIS DES DONNÉES

Le pétrole = Richesse matérielle
Raréfaction des ressources

Les données = Richesse immatérielle
Raréfaction de la donnée par le verrouillage de l'humain ?

Si le pétrole est une richesse…
… Et que la donnée est le nouveau pétrole…
Alors la donnée est une richesse

Les données au cœur de la guerre économique internationale

SiecleDigital
Amazon va automatiser les ventes de données entre professionnels

Forbes
Digital Healthcare Growth Drivers In 2020

Les "data", pétrole du XXIe siècle
Le Point

Le Monde
Palantir, l'embarrassant poisson-pilote du big data

LE BIG DATA
Le magazine I.A, Cloud et Big Data
LE BIG DATA TOUJOURS PLUS PRÉSENT DANS L'INDUSTRIE PÉTROLIÈRE

28èmes RENCONTRES DU RISK MANAGEMENT AMRAE
DEAUVILLE DU 05 AU 07 FÉVRIER 2020

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉS À CETTE RICHESSE ?

RISQUES ACTUELS

STRATÉGIQUE

- La donnée est un **actif immatériel** de l'entreprise, et fait partie intégrante du patrimoine de celle-ci.
- **Gouvernance** de la donnée (qualitée).
- Chute de l'activité ➔ Perte en Chiffre d'Affaires

ÉTHIQUE

- Les données et leur éco-système remplace l'humain, mettent en jeu la **liberté individuelle.**
- Forte **empreinte carbonne** des data centers.
  Exemple : En 2016, 3 % de l'électricité mondiale sont consommés par les datacenters
- Loi Pacte ➔ **Certificat d'Economie d'Energie** (CEE), recyclabilité de l'énergie des datas centers

OPÉRATIONNELS

- **Sécurité** : confiance entre clients et commerciaux, transparence sur le cycle de vie de la donnée collectée et traitée…
- **Dysfonctionnement** des systèmes, activités, processus…

Exemple : Salesforce, le géant américain du cloud pour les entreprises, a subit le 23 septembre une panne de ses datas centers, empechant ses clients d'accéder à leurs fichiers.

NON CONFORMITÉ

- La donnée au sens large est fortement **réglementée** :
  - RGPD sanctions financières 2% ou 4% du CA
  - Sanctions médiatiques
  - Sanctions opérationnelles (avertissement, mise en demeure…)
- Bénéficie d'une réglementation **sectorielle** exigeante (Ex : Solvabilité II banque et assurance)

RGPD, la panacée ?

- Problématique :
  - Du papier à l'électronique
  - De l'unité à la masse
  - Du traitement limité au traitement sans limite par l'informatique et l'IA
- Solution : "mettre sous clef les données personnelles"
- Sanctions :
  - 161.000 notifications d'incidents de sécurité en 18 mois
  - 114 millions d'euros d'amende infligées en Europe
  - France : 9ème position pour les notifications et 1ère pour les sanctions cumulées (Google)
- De la poudre aux yeux
  - La donnée est peu stockée en UE
  - Moyens légaux forçant l'accès à la donnée

Où vont “nos” données?

- Données numériques produites en 2018 : 33 zettaoctets,
  - env. 660 milliards de disques Blu-Ray d’une capacité individuelle de 50 Go
  - 33 millions de cerveaux humains
  - Le volume de données double tous les 18 mois
- 4 081 data centers répartis dans 118 pays
- data centers
  - dans des pays froids
  - près des centrales électriques
  - licence de production d'énergie (comme EDF)
  - Les plus grands data centers se trouvent aux USA et en Chine

USA – le torchon brul(ait) : Produire ou ne pas produire

- 24 juin 2010 : Morrison vs. National Australia Bank
- Cour de New York (24/01/2017) : Microsoft n’a pas à produire
- Tribunal de Philadelphie (03/02/2017) : Google doit produire
- Réponse : le Cloud Act

USA – Cloud Act ou la légalisation de l'accès aux données

- Le « Cloud Act » :« Clarifying Lawful Overseas Use of Data Act »)
- Loi fédérale américaine promulguée le 23 mars 2018
- L'obligation des fournisseurs de services de communiquer les informations détenues sans considération de la localisation des données
- La possibilité de conclure des accords bilatéraux sur l'accès aux données par les gouvernements étrangers
- Contradictions entre le Cloud Act et le RGPD
- Solutions ?

USA - California Consumer Privacy Act

- California Consumer Privacy Act (CCPA)
  - voté le 29 juin 2018;
  - entré en vigueur au 1er janvier 2020.
- Champ :
  - nouveaux droits au bénéfice des consommateurs résidant en Californie
  - Mais champ étriqué par rapport au RGPD
- Sanctions

USA – D'autres équivalent RGPD ?

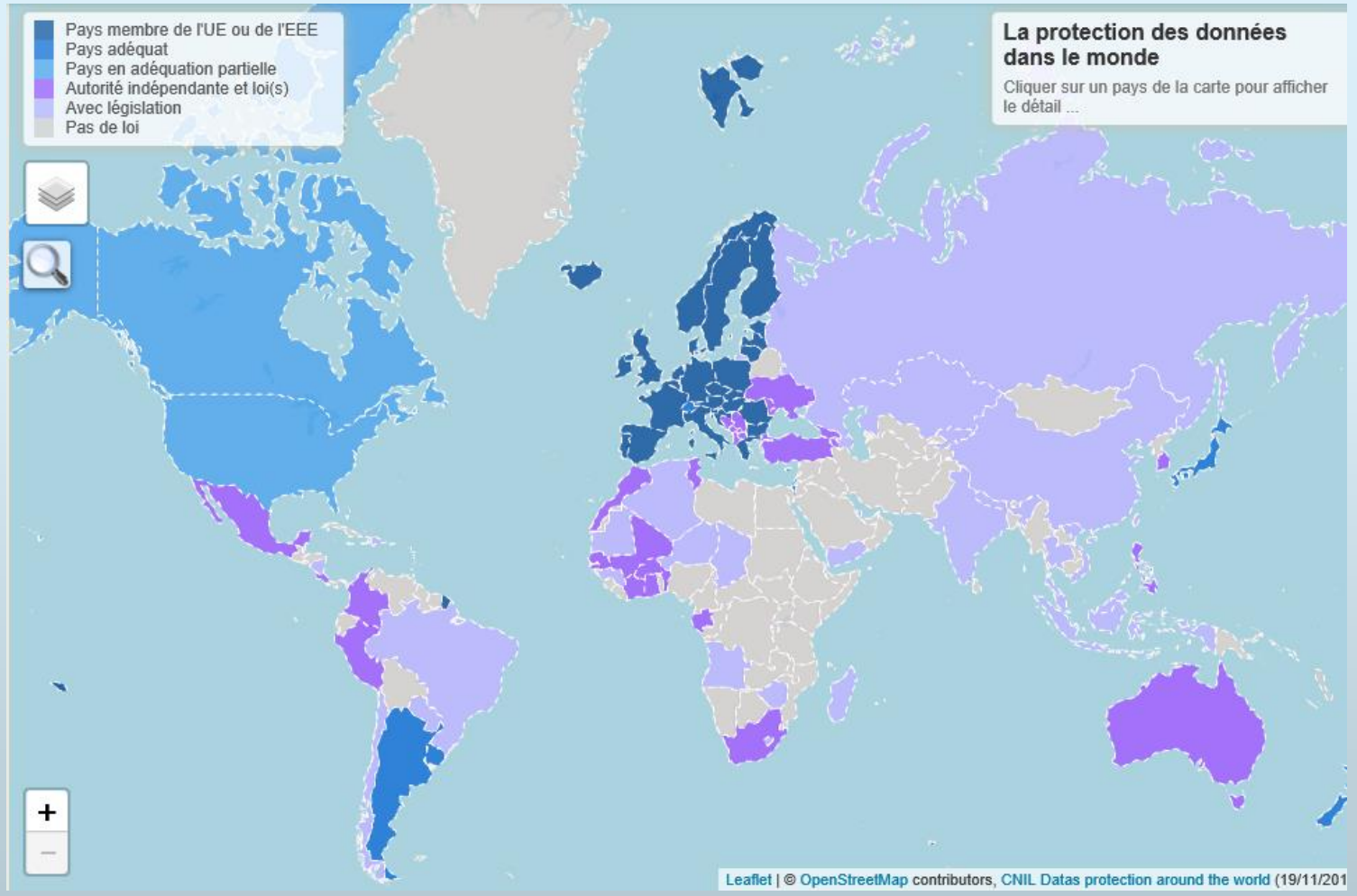
- Législation d'Etats fédérés:
  - Etat de New York : proposition de loi de mai 2019
  - Etat du Nevada :
    - 29 mai 2019 : « *Senate Bill 220* »;
    - Entrée en vigueur : 1er octobre 2019

- Législation fédérale
  - Sectorielle
    - Le *Social Media Privacy Protection and Consumer Rights Act*
    - Le *Data Care Act of 2018,*
    - L'*American Data Dissemination Act*
  - Vocation générale:
    - Le *Data Privacy Act*
    - L'*Information Transparency & Personal Data Control Act*
    - Le *Consumer Data Protection Act*

La Chine protège vos données?

- La Chine a évalué en 2016 à 11,5 milliards d'euros la perte pour son économie du fait des fuites de données
- Loi sur la cybersécurité du 1er juin 2017 (et succession de lois en 2018 et 2019)
  - Faire écho au RGPD
  - Interdiction de la vente de données (contrairement aux USA)
  - Collecte restrictive : pas d'information non liées aux services proposés
  - Interdiction de publier tout contenu portant atteinte à « l'honneur national », « troublant l'ordre économique ou social » ou destiné à « renverser le système socialiste »
  - Obligation de stocker sur le territoire chinois pour *« les services de communication, l'énergie, le transport, l'eau, la finance, le service public, l'e-gouvernement et autres »*
  - Contrôle : Grande Muraille numérique
    - Crainte d'un contrôle arbitraire
    - Crainte d'un contrôle aux contours non définis
- Pour les données chiffrées, la loi impose aux opérateurs de déchiffrer les contenus *« quand cela est nécessaire »* (1er janvier 2020)

Transfert de données hors de France



Data et Valeur

Q2 : Peut-on apprécier la valeur de l'actif "Data" ? (1/2)

- La valeur de la data diffère en fonction de l'acteur considéré dans la chaîne de transmission de la data (producteur, agrégateur, utilisateur)

Vagues de business pour lesquels le produit est la Data

La presse / Les actualités
La météo
Les instituts d'étude
Les agrégateurs (eg Bloomberg)

Les GAFA etc.

Vagues de business où la Data fait la différence

Les assureurs
Le courtage / l'intermédiation

La grande distribution
Les GAFA etc.

Data et Valeur

Q2 : Peut-on apprécier la valeur de l'actif "Data" ? (2/2)

- Lorsqu'un usage de la data est identifié, il est quelquefois possible d'appréhender la valeur que cet usage lui confèrera

Exemple 1 : la prescription d'actions anti-churn

La Fair Value des relations clients s'appréhendent par actualisation des « surprofits » futurs, minorés de l'attrition géométrique des clients. Le différentiel d'attrition permet d'approcher une valeur.

Exemple 2 : le ROI d'actions ciblées par la Data (ex en assurance)

Différentiel entre deux scenarii, le scenario factuel où l'exploitation de la data est mise en œuvre, le scenario contrefactuel où l'on n'agit pas.

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉS À CETTE RICHESSE ?

RISQUES ÉMERGENTS

CYBERSÉCURITÉ

- Virus « cryplocker »
- Phishing
- La fraude au Président ou au virement
- Technique du « point d'eau » et e-mails corrompus

TECHNOLOGIES ET INNOVATION

- Émergence des Intelligences artificielles (IA) et de ses difficultés opérationnelles :
  - Définir formellement ces propriétés pour que des algorithmes puissent être vérifié
  - Réaliser des analyses de données équitables

Exemple : Le bot Taï de Microsoft doté d'une IA qui intéragit avec les internautes 2016

- Émergence des monnaies électroniques : Bitcoin, Ethereum, Litecoin…
  - Risque d'anonymat provoquant de la fraude, volatilité de la monnaie

GÉOPOLITIQUE ET SOUVERAINETÉ

- Suprématie GAFAM ET BATX
- Cloud Act
- Palantir outil controversé

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉS À CETTE RICHESSE ?

Souveraineté

« la souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques » P.Bellanger

Apparition des méta-plateformes qui absorbent une quantité d'information qu'elles maitrisent et qui ont pour conséquences d'augmenter l'intimité avec laquelle leurs algorithmes nous analysent

GAFAM

L'invasion numérique dans nos sociétés

3 milliards d'euros d'investissement en Europe pour les datas centers

Moteur de recherche

Google

Apple

Investissement de 1,7 milliards ➔ Centre de données en Europe

10 millions d'euros d'investissement dans l'IA en France

Réseaux sociaux

facebook

amazon

Livraison 24h

Création de 2 000 CDI en France

30 millions d'euros d'investissement dans l'IA en France

Outlook

Microsoft

BATX

2019

Création d'un fond d'investissement de plus de 1,5 milliards pour financer des start-ups sur des technologies de conduite autonome

BAIDU

ALIBABA

TENCENT

XIAOMI

2018

- 2 data centers en Europe : Allemagne et Royaume-Uni
- **2 stores** Aliexpress ont ouvert à Madrid (25/08/2019) puis à Barcelone (29/11/2019)

2019-2020

- Investissement de 7 milliards de dollars dans l'IA, la 5G et l'IoT
- 1 millions de smartphones vendu en France

15/01/2020

Entrée au capital de **Lydia** (Fintech française) dans le cadre d'une levée de fonds de + de 40 millions d'euros

*Exprimé en milliards de dollars

Etude de l'école Financia Business school

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉS À CETTE RICHESSE ?

Souveraineté/Géopolitique

Contenu

2 grandes dispositions :

- Toutes sociétés américaines, y compris celles contrôlées par elles, doivent communiquer aux autorités américaines sur demande, les données de communication stockées, même si les données se trouvent dans un autre pays.
- Possibilité pour le gouvernement américain de collaborer avec d'autres pays étrangers dans le cadre d'une justice collaborative.

Le Cloud Act précise que **seules les infractions les plus graves** font l'objet d'une réquisition de données.

Définition

- Titre 18 du United States Code – Chapitre 121 -Stored Communication Act (SCA) relatif à la protection des données traitées ou stockées.
- Le Cloud Act a été promulgué le 23 mars 2018 par le Président des États-Unis et vient amender le SCA.
- Il né en anticipation à plusieurs divergences d'intérêts judiciaires entre différents pays.

Passe droit ?

Le Cloud Act n'est en aucun cas une loi extraterritoriale car :

- Une demande de réquisition du gouvernement américaine à un fournisseur doit être obligatoirement adressée avec un **mandat**,
- Les demandes doivent se baser sur le fondement d'une **ordonnance judiciaire** (court orders),
    - **Arrêté du 22 juin 2018** : possibilité de refus d'un fournisseur de communiquer les données de géolocalisation d'un téléphone sans mandat valable.
- **Un fournisseur est dans le droit de refuser un droit de communication** si le mandat n'est pas valable et a un délai de 14 jours pour transmettre son refus.

Mécanismes de blocage ?

3 lois significatives :

- Loi n°68/678 du 26 juillet 1968 : loi de blocage française
- Articles 44 – 45 – 46 – 47 – 49 du règlement de l'UE n°2016/679 relatif à la protection des données (RGPD)
- Article 48 (RGPD)

Zoom Article 48 RGPD

« Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel **ne peut être reconnue ou rendue exécutoire** de quelque manière que ce soit **qu'à la condition qu'elle soit fondée sur un accord international**… »

Données de santé

France

Législation antérieure au 25 mai 2018

Interdiction de traiter des données sensibles (art 8 LIL)

« *Specialia generalibus derogant* »

Les assurances s'appuient sur des textes spéciaux pour déroger à la loi Informatique et Libertés.

OUTIL DE RÉGULATION

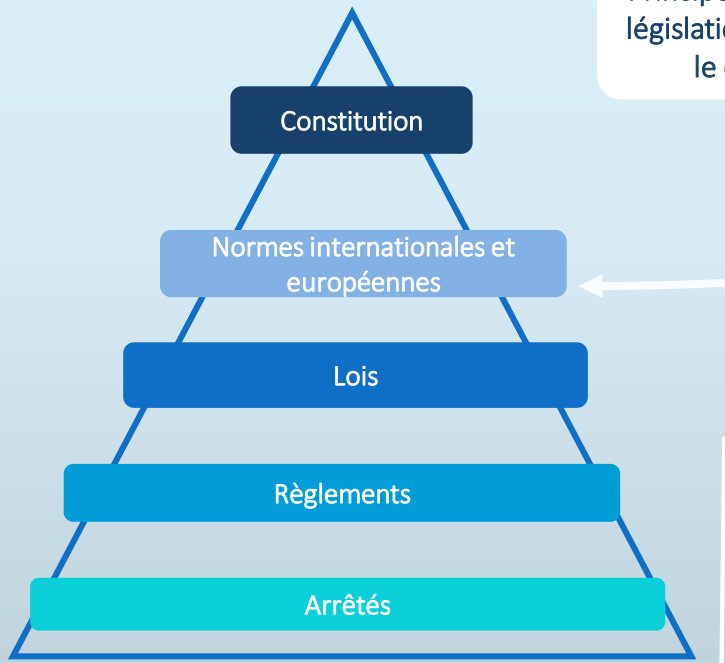
Depuis 2014, le pack de conformité constitue le nouvel outil de régulation de l'utilisation des données personnelles.
Ce référentiel s'adresse aux responsables de traitements ayant la qualité d'organisme d'assurance.

Après le 25 mai

Interdiction de traiter des données sensibles (art 9 RGPD)

« *Specialia generalibus derogant* »

Principe de primauté de la législation européenne sur le droit national



Application de la réglementation au secteur assurantiel

Concertation sur la place assurantielle sur un des cas d'exception de l'article 9 du RGPD qui pourrait être utilité comme fondement du traitement des données de santé

Art.9 2.b « le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale »

CNIL

29 Janvier 2019 : L'ancienne présidente de la CNIL, Isabelle FALQUE-PIERROTIN, affirme l'aménagement pour les acteurs de l'assurance qui peuvent se prévaloir de l'exception de l'article 9, paragraphe 2.b, concernant le traitement des données de santé.

Données de santé

France

3 types de produits intéressent les acteurs de l'assurance :

Assurance auto

L'assurance automobile avec l'apparition de la voiture connectée capable d'évaluer le style de conduite de l'assuré et les risques qu'il court au volant ;

Assurance habitation

L'assurance habitation car une maison connectée est une maison plus sûre : elle peut alerter en cas d'intrusion, de fuite ou de court-circuit par exemple ;

Assurance santé

L'assurance santé à travers notamment le bracelet connecté capable de mesurer en continu l'état de santé d'un utilisateur et de l'inciter à adopter un meilleur comportement (alimentaire, ou en matière d'activité, etc.) afin de limiter son risque de maladie ou d'accident.

Les opportunités pour les acteurs du marché de l'assurance :

- Développer la connaissance client
- Mieux gérer les risques
- Améliorer l'image des assureurs auprès du grand public et leur rôle sociétal

Les inquiétudes des assurés vis à vis des objets connectés

- Collecte massive de nombreuses données à caractère personnel
- Revente d'une partie de leurs données
- Individualisation de l'offre
- Hyper personnalisation

Data et Valeur

Q3 : Quels sont les drivers de la valeur de la data ? (1/2)

Qualité	Exploitabilité	Enjeu
FIABILITE	DEFINITION UNIVOQUE	RARETE / EXCLUSIVITE
REPRESENTATIVITE & VOLUME	STRUCTURE / HOMOGENEITE	DUREE D'INTERET (OBSOLESCENCE)
PROFONDEUR (HISTORIQUE)	COMPLETUDE	VALEUR STRATEGIQUE & FINANCIERE DES CAS D'UTILISATION
FREQUENCE DE MAJ ADAPTEE	PERENNITE DU SOURCING	

Data et Valeur

Q3 : Quels sont les drivers de la valeur de la data ? (2/2)

- La valeur d'une data peut résider en son exclusivité (ie les autorités de Bourse punissent sévèrement les délits d'initiés)
- La valeur d'une data peut être très importante à un instant donné, et nulle peu de temps après (eg opportunité d'arbitrage qui disparaît)
- … La valeur d'une data peut être nulle à un instant donné, et prendre de la valeur plus tard (eg certains acteurs stockent de la donnée cryptée non décodable aujourd'hui, tablant sur la capacité à décoder dans quelques années, notamment grâce aux quantum computing) => quelles sont les data qui auront encore de la valeur dans dix ans ? En avez-vous dans vos orga ?

La fin de l'assurance telle qu'on la connaît aujourd'hui ?

France

Vers un nouveau visage de l'assurance ?

GAFA

Association des assurances aux GAFA

Google Assurance

ASSURTECH

Les Assurtechs associent l'assurance aux nouvelles technologies (Big Data, blockchain, intelligence artificielle) et redessine les business models

QUELQUES CHIFFRES : LES BIG DATA LIÉES À LA SANTÉ REPRÉSENTAIENT 153 EXAOCTETS EN 2013. ELLES DEVRAIENT ATTEINDRE 2 314 EXAOCTETS D'ICI À 2020*.

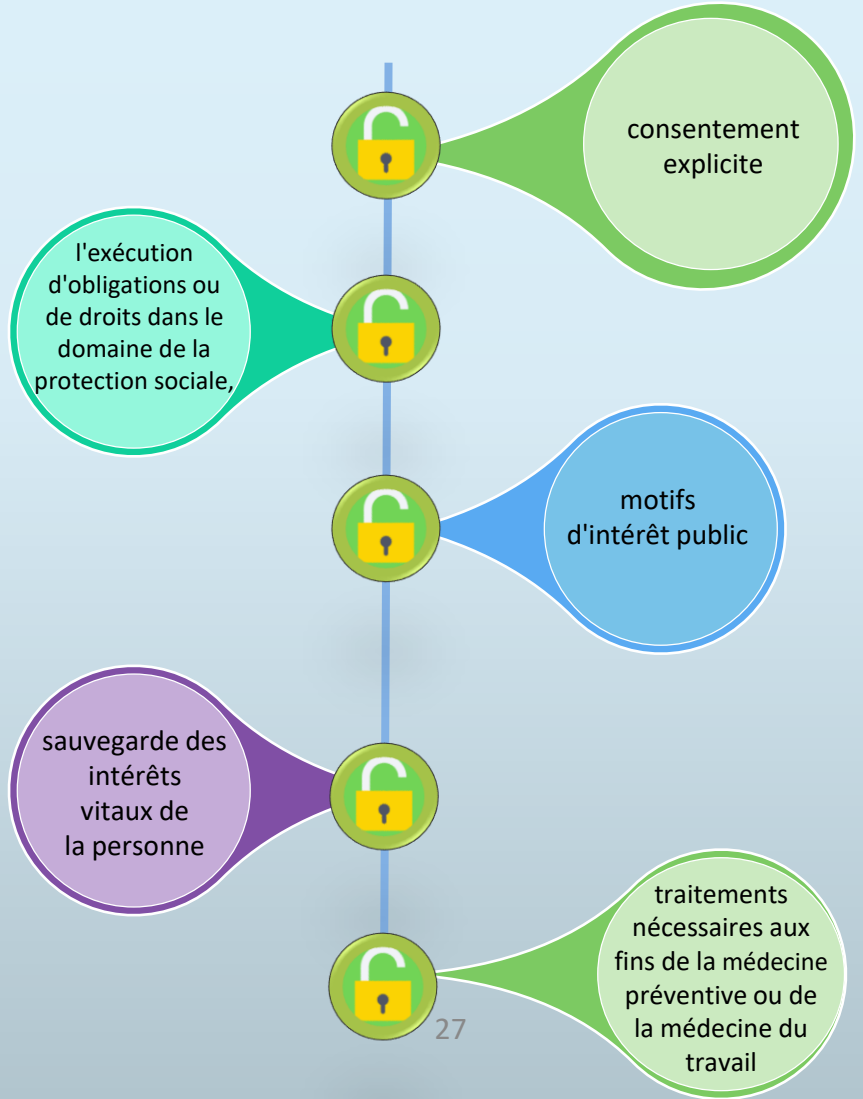
Vers la fin de la mutualité ?

Individualisation via un modèle prédictif parfait

Produit d'épargne

Le 23 janvier 2019 des députés ont déposés une proposition de loi visant à interdire le traitement de données à caractère personnel récoltées par un capteur de santé, relatives au mode de vie ou à l'état de santé du preneur d'un produit répondant aux définitions contenues dans le code des assurances ou du code de la mutualité. Pour les députés ce texte est rendu nécessaire en raison de l'évolution des technologies.

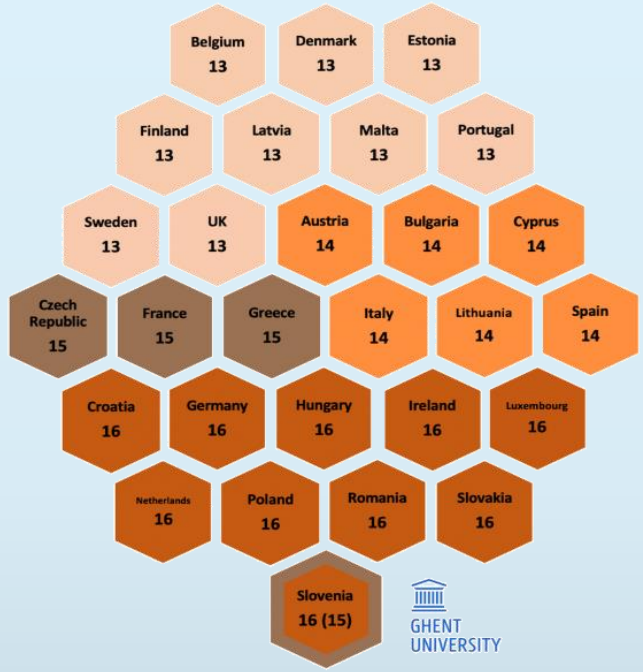
Interdiction de traiter des données sensibles (**art. 9 RGPD**)



Traitement de la donnée de santé est fondé sur le consentement

Disparité des règles nationales entre Etats membres.

- l'âge du consentement (le plus souvent mentionné comme problème de disparité)
- Règle de dispense du consentement explicite varient d'un pays à l'autre



Traitement de la donnée de santé est fondé sur l'intérêt public

Grande marge de manœuvre aux Etats membres pour décider de leurs propres règles, parce qu'ils relèvent de la catégorie exemptée de « l'intérêt public »

ÉTATS-UNIS

- Traitement de la donnée fondée sur le **« service »**
- Régulations imposées par le gouvernement fédéral, mais aussi des spécificités par États
- Les fournisseurs des actes de santé sont en grande partie des organismes privés (Kaiser Permanente, Predilytics (groupe Welltok), HealthVerity)

Google et Amazone sont en mesure de cartographier une épidémie de grippe

- **HIPAA** (Health Insurance Portability and Acountability Act) : définit la norme de sécurité des informations médicales des patients

CHINE

- Traitement de la donnée fondée sur **l'efficacité économique** et est considéré comme une **ressource** au service de l'État développemental

Quelques chiffres :

- ✓ 3 112 établissements médicaux ont mis leurs données en communs
- ✓ La banque nationale de données électroniques sur la santé au niveau de la province du Guangdong contient des informations sur 80 millions de résidents permanents

- Il n'existe aucune loi ou directive spécifique sur les données de santé.

Exemple : La loi sur la cybersécurité du 1er Juin 2017 ne mentionne pas le mot « santé »

QUESTIONS/REPONSES

MERCI DE VOTRE ATTENTION !

- **AVANT DE PARTIR , N'OUBLIEZ PAS DE REMPLIR L'EVALUATION !**

- Soit sur la feuille , à remettre à l'hôtesse à la sortie
- Soit directement sur l' **APPLI des RENCONTRES**

Vous aurez accès à la présentation la semaine prochaine, après avoir rempli l'évaluation générale du congrès.

Bonnes Rencontres !

Annexes

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉE À CETTE RICHESSE ?

RISQUES ACTUELS

SÉCURITÉS

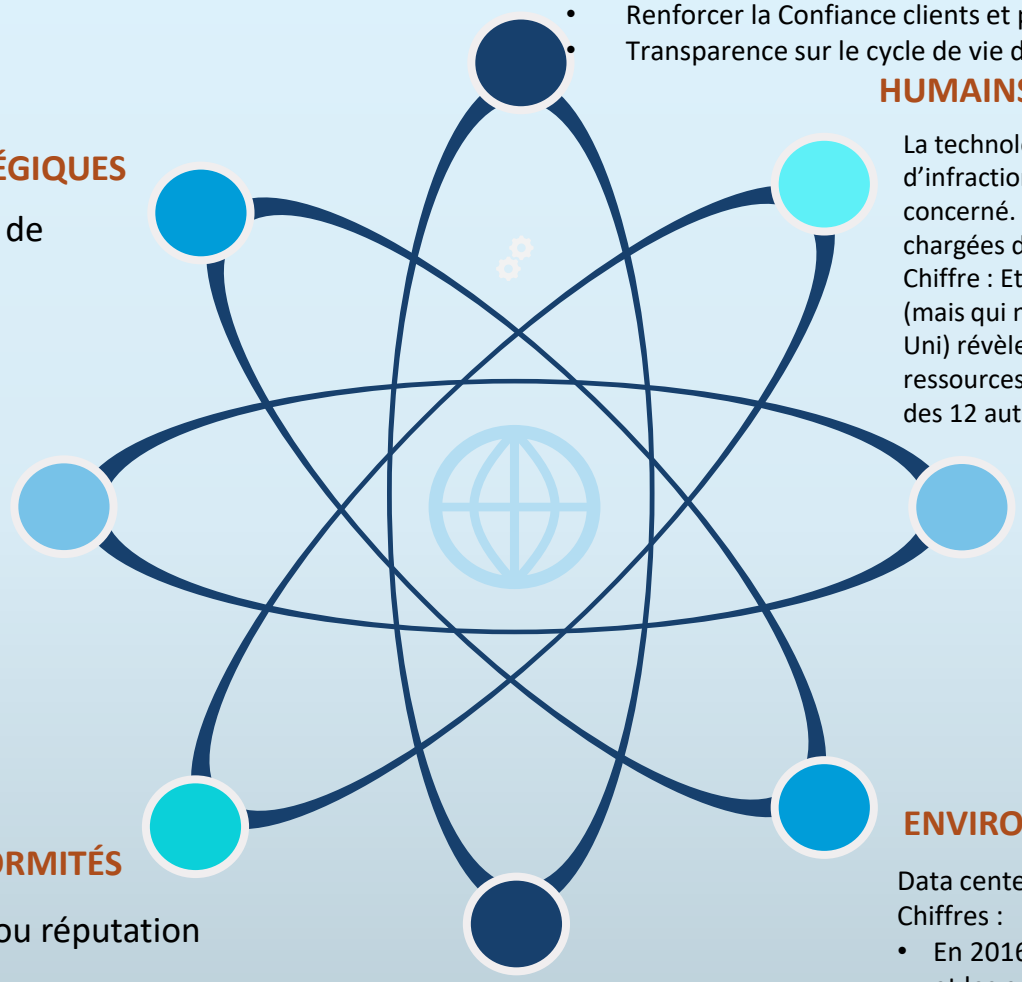
- Renforcer la Confiance clients et partenaires commerciaux
- Transparence sur le cycle de vie des données collectées et traiter

HUMAINS

La technologie numérique évolue, et par conséquent, que le volume et le nombre d'infractions peuvent prendre une ampleur énorme compte tenu du public concerné. Or, les organismes de réglementation, les tribunaux et les autorités chargées de l'application de la loi ne changent pas d'échelle.
Chiffre : Etude EDPB ➔ sur 17 États membres de l'UE ainsi que sur la Croatie (mais qui ne couvre pas des pays comme la France, les Pays-Bas ou le Royaume Uni) révèle que les autorités de contrôle polonaise et espagnole disposent des ressources humaines les plus importantes (environ 250 personnes) et que celles des 12 autres pays comptent moins de 50 personnes

STRATÉGIQUES

- Matière première du secteur de l'assurance
- Gouvernance de la donnée (qualité)



DÉVELOPPEMENTS ET TRANSFORMATIONS

FINANCIERS

Perte de CA/ chute de l'activité

ENVIRONNEMENTALS

Data centers : empreinte écologique du numérique.
Chiffres :

- En 2016, 3 % de l'électricité mondiale sont consommés par les datacenters et les estimations prévoient une part de 13 % d'ici à 2030.
- 380 millions de tonnes de déchets électroniques par an

Loi Pacte ➔volet sur ouvre les certificats d'économie d'énergie (CEE)/ **recyclabilité** des équipements Travaux de recyclage d'énergie des data centers.
➔ Apparatition des smarts greenn

NON CONFORMITÉS

Sanction pécuniaire ou réputation

OPÉRATIONNELS

Dysfonctionnements de l'activité et des systèmes

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉE À CETTE RICHESSE ?

RISQUES ÉMERGENTS

Risque de Cybersécurité : Nature des risques encourus :

- ✓ virus « cryplocker »
- ✓ Phishing
- ✓ La fraude au Président ou au virement
- ✓ Technique du « point d'eau » et e-mails corrompus

Risque technologiques :

émergence des Intelligences artificielles (IA)

Difficulté de l'IA :

1. Définir formellement ces propriétés pour que des algorithmes puissent les vérifier/garantir
2. Réaliser des analyses de données équitables – plus simple si la responsabilité est prise en compte très tôt, responsibility by design
3. Vérifier que des analyses disponibles sont équitables

Exemple : Le bot Taï de Microsoft doté d'une IA qui intéragit avec les internautes 2016

Csq de cet IA :

- Au japon : pas de problème
- Aux US : des internautes l'ont fait devenir raciste, misogyne, révisionniste…

Tay, c'est l'histoire formidable d'une intelligence artificielle passée de statut de « cool » à celui de nazi pro-Trump misogyne en à peine 24h

CSQ ➔ Il suffit pas de vérifier le code ; il faut aussi surveiller l'apprentissage et usage de cette IA

Risque géopolitique /souveraineté

- **Evgeny Morozov « Pour tout résoudre, cliquez ici,»**
- Suprématie GAFAM ET BATX
- Palantir outil controversé

Risque risque de digitalisation/dématérialisation

Monnaie numérique/ virtuelle : la cryptomonnaie, et le bitcoin par exemple, est devenue la nouvelle monnaie anonyme

Constat : monnaie était l'instrument d'échange symbolique entre les personnes

Aujourdhui : même les transactions en espèces les plus infimes peuvent être remplacées par des paiements électroniques

Question ouverte : Aide pour les pays (notamment la Chine) à échapper à l'entreprise du dollar ur les transactions internationales ?

Risque XX

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉE À CETTE RICHESSE ?

Souveraineté

« la souveraineté numérique est la maîtrise de notre présent et de notre destin tels qu'ils se manifestent et s'orientent par l'usage des technologies et des réseaux informatiques » P.Bellanger

Apparition des méta-plateformes qui absorbent une quantité d'information qu'elles maitrisent et qui ont pour conséquences d'augmenter l'intimité avec laquelle leurs algorithmes nous analysent

GAFAM

L'invasion numérique dans nos sociétés

3 milliards d'euros d'investissement en Europe pour les datas centers

Moteur de recherche

Google

Iphone

Investissement de 1,7 milliards ➔ Centre de données en Europe

10 millions d'euros d'investissement dans l'IA en France

Réseaux sociaux

facebook

amazon

Livraison 24h

Création de 2 000 CDI en France

30 millions d'euros d'investissement dans l'IA en France

Outlook

Microsoft

BATX

2019

CA : 15 247*$
Capitalisation : 48 302 *$

BAIDU

ALIBABA

TENCENT

XIAOMI

2019

- Capitalisation : 4160 *$
- **2 stores** Aliexpress ont ouvert à Madrid (25/08/2019) puis à Barcelone (29/11/2019)

2020

- Investissement de 7 milliards de dollars dans l'IA, la 5G et l'IoT
- CA en hausse de 5.5% (dernier trimestre de 2019)

15/01/2020

Entrée au capital de **Lydia** (Fintech française) dans le cadre d'une levée de fonds de + de 40 millions d'euros

28èmes RENCONTRES DU RISK MANAGEMENT AMRAE
DEAUVILLE DU 05 AU 07 FÉVRIER 2020

*Exprimé en milliards de dollars

Etude de l'école Financia Business school

Souveraineté

Qu'est-ce que le Cloud Act?

Du Warrant Case au Cloud Act

- Titre 18 du United States Code – Chapitre 121 – Stored Communication Act (SCA) relatif à la protection des données traitées ou stockées.
- Le Cloud Act a été promulgué le 23 mars 2018 par le Président des États-Unis.
- Il né en anticipation à plusieurs divergences d'intérêts judiciaires entre différents pays.

Que prévoit le Cloud Act ?

- 2 grandes dispositions :
  - Toutes sociétés américaines, y compris celles contrôlées par elles, doivent communiquer aux autorités américaines sur demande, les données de communication stockées, même si les données se trouvent dans un autre pays.
  - Possibilité pour le gouvernement américain de collaborer avec d'autres pays étrangers dans le cadre d'une justice collaborative.
- Le Cloud Act précise que seules les infractions les plus graves font l'objet d'une réquisition de données.

Le Cloud Act est-il un passe-droit américain pour accéder aux données en Europe ?

- Le Cloud Act n'est en aucun cas une loi extraterritoriale car :
  - Une demande de réquisition du gouvernement américaine à un fournisseur doit être obligatoirement adressée avec un mandat,
  - Les demandes doivent se baser sur le fondement d'une ordonnance judiciaire (court orders),
  - Arrêté du 22 juin 2018 : possibilité de refus d'un fournisseur de communiquer les données de géolocalisation d'un téléphone sans mandat valable.
  - Un fournisseur est dans le droit de refuser un droit de communication si le mandat n'est pas valable et a un délai de 14 jours pour transmettre son refus.

Des lois françaises ou européennes existent elles pour limiter le Cloud Act ?

3 lois significatives :

Loi n°68/678 du 26 juillet 1968 : loi de blocage française

Articles 44 – 45 – 46 – 47 – 49 du règlement de l'UE n°2016/679 relatif à la protection des données (RGPD)

Article 48 (RGPD) : aucune autorité administrative ou juridiction d'un pays tiers ne peut exiger une divulgation de données sans accord international au préalable.

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉE À CETTE RICHESSE ?

Géopolitique

Perception et conception différentes de la data

objectif : protéger la sécurité nationale dans le sens la plus large et non garantir la confidentialité de la donnée

France et Europe

Respect de la vie privée et de confidentialité

Avec le RGPD, l'Union européenne adopte une philosophie centrée sur l'individu, et vise à rééquilibrer la balance en sa faveur, face aux géants du Net qui brassent d'immenses quantités de données » Steve Shillingford.

Les enjeux sont multiples : en termes de libertés individuelles et publiques constitutionnellement garanties, l'Internet constitue un élément désormais incontournable de l'exercice de la liberté de communication et d'information, mais également un facteur de risques nouveaux pour la protection de la vie privée et des données personnelles

USA

credit score est une note qui est censée refléter la fiabilité financière d'une personne. Ce score est calculé pour toutes les personnes qui ont un numéro de Sécurité Sociale. Il est établi par trois agences de notation privées (Equifax, Transunion, Experian), qui utilisent le système de notation d'une société californienne, Fico. (https://frenchmorning.com/credit-score-les-nuls/)

Secteur d'activité qui tilise le cérdit score : BANQUE/propriétaires pour vérifier la fiabilité financière de leurs locataires. Idem pour les compagnies d'assurance. Et même les compagnies téléphoniques ou fournisseurs d'accès internet/ EMPLOYEUR

« la collecte et le traitement des données est généralement autorisé aux États-Unis sauf si la loi dit que c'est interdit, tandis que dans l'UE, la collecte et le traitement des données sont interdits sauf si la loi dit que c'est autorisé » (https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1627&context=faculty_articles°

CHINE

Crédit social : système de notation de crédit : scoring

« dystopie Autoritaire du monde numérique » (https://www.institutmontaigne.org/ressources/pdfs/publications/donnees-personnelles-comment-gagner-la-bataille-etude.pdf)

Article 1 de la loi sur la cybersécurité ou Cybersecurity law (CSL) promulguée le 7 novembre 2016 et entrée en vigueur le 1er juin 2017

« **Article 1:** la loi est formulée pour garantir la cybersécurité, mais également pour sauvegarder la souveraineté du cyberespace et la sécurité nationale

russie

Le 1er novembre 2019, la loi russe sur un « Internet souverain » est entrée en vigueur, donnant au gouvernement, en cas d'urgence, le pouvoir de couper son réseau Internet du reste du monde (https://siecledigital.fr/2019/11/04/russie-internet-souverain/)

QUELS SONT LES PRINCIPAUX RISQUES ASSOCIÉE À CETTE RICHESSE ?

« Le big data constitue aujourd'hui "le pétrole" des services de renseignements français. » dixit Jacques Monin (https://www.franceinter.fr/emissions/secrets-d-info/secrets-d-info-22-septembre-2018)

Les Echos

«Big Data : faute de solution française, les services secrets signent à nouveau avec Palantir»

Le 27 novembre 2019

https://www.lesechos.fr/industrie-services/air-defense/big-data-faute-de-solution-francaise-les-services-secrets-signe-a-nouveau-avec-palantir-1151255

Exemples:
Palentir outil de **data crunching qui fait débat** ➔ Le *data crunching* est une méthode des sciences de l'information qui permet de mettre en place un **traitement automatisé de grandes quantités de données et d'informations** (*Big Data*).

Les principaux clients de Palantir sont les banques, les assurances, mais aussi les services de renseignement, particulièrement intéressés par la puissance de ces algorithmes

« Palantir : l'œil américain du renseignement français »

A l'été 2016, un contrat de 10 millions d'euros aurait été conclu avec la Direction générale de la Sécurité intérieure (DGSI), le service de renseignement intérieur et de police judiciaire du ministère de l'Intérieur français (https://www.numerama.com/tech/564297-au-fait-pourquoi-palantir-sappelle-palantir.html)

Données de santé

Europe

Interdiction de traiter des données sensibles (art 9 RGPD)

Une série d'exceptions autorise leur traitement

- le consentement explicite de la personne sauf si le droit d'un État membre ou de l'Union prévoit que l'interdiction ne peut être levée par ce seul consentement,
- l'exécution d'obligations ou de droits dans le domaine de la protection sociale,
- la sauvegarde des intérêts vitaux de la personne ,
- l'intérêt légitime du responsable de traitement moyennant des garanties appropriées,
- les motifs d'intérêt public ,
- l'ensemble des traitements nécessaires aux fins de la médecine préventive ou de la médecine du travail, de diagnostics médicaux, de la prise en charge sanitaire ou sociale ou de la gestion des systèmes et des services de santé ou de protection sociale

Traitement de la donnée de santé est fondé sur le consentement

1. Disparité des règles nationales entre Etats membres.

Exemples :

- l'âge du consentement (le plus souvent mentionné comme problème de disparité) cf image
- Règle de dispense du consentemer explicite varient d'un pays à l'autr

https://www.betterinternetforkids.eu/web/porta
wareness/detail?articleId=3017751#FR

Traitement de la donnée de santé est fondé sur l'inté ic

GHENT UNIVERSITY

Grande marge de manœuvre aux Etats membres pour décider de leurs propres règles, parce qu'ils relèvent de la catégorie exemptée de « l'intérêt public »

2.Réticence pour l'UE de créer un service de cloud dans la santé (des services de santé numérique)

3. Informations médicales cloisonnées et souvent conservée sous une forme non numérique

États-Unis

Traitement de la donnée fondé sur le concept de « service » / marketing :
des entités des secteurs public ou privé « achètent » des services de santé à des « fournisseurs », ceux-ci étant soumis à des régulations **imposées par le gouvernement fédéral** mais également **spécifiques de chaque Etat**
business

CSQ

Les fournisseurs des actes de santé sont en grande partie d'organismes privés (Kaiser Permanente, Predilytics (groupe Welltok), HealthVerity etc.;)

Qui sont les fournisseurs des actes de santé ?
Dans le cadre de la réglementation fédérale, un fournisseur d'acte de santé, « health care provider » est défini comme un fournisseur de services médicaux ou de santé (détaillés dans la section 1861(s) du « Social Security Act ») ou toute autre personne ou organisation qui fournit, facture ou est rémunéré pour un acte de santé.

- Business/Marketing des données de santé : GOOGLE et AMAZONE sont en mesure de cartographier les épidémies de grippe, en se référant aux recherches ou commandes de médicaments en vente libre
- Stimuler la publicité numérique des sociétés du secteur de la santé et du secteur pharmaceutique reste un objectif prioritaire

PBLM

- **HIPAA** (Health Insurance Portability and Accountability Act) est la loi sur la portabilité et la responsabilité des assurances maladie. Elle définit la norme de sécurité des informations médicales des patients. Cette réglementation définit les exigences de sécurité et de confidentialité des données pour les organisations qui traitent des données de santé protégées (appelées PHI pour Protected Health Information).
- L'analyse de risque proposé par l'HIPAA se base sur une approche objective du traitement des données de santé, à l'inverse le RGPD repose sur une analyse subjective (droits et libertés des personnes)

Chine

Traitement de la donnée fondé sur l'efficacité économique

Conception stratégique de l'utilisation des big data en santé considérée comme une ressource au service de l'Etat développemental

Quelques chiffres :

- 3112 établissements médicaux de santé ont mis leurs données en commun
- La banque nationale de données électroniques sur la santé au niveau de la province du Guangdong contient des informations sur 80 millions de résidents permanents

CSQ

Il n'existe aucune loi ou directive spécifiques sur les données de santé.
Loi sur la cybersécurité entrée en vigueur le 1er juin 2017 ne mentionne pas le mot « santé ».
La spécification PIS a inclus le terme « informations médicales » dans la définition des informations personnelles sensibles, mais sans aller plus loin

S'il s'agit en effet de gagner des utilisateurs hors de Chine, la finalité est ailleurs selon le chercheur : "*Aujourd'hui, quand on regarde par exemple les travaux de recherches sur l'intelligence artificielle, on voit qu'une entreprise comme Baidu est toute aussi impliquée que Google. Les deux vont rapidement être en concurrence.*" En 2017, le gouvernement chinois annonçait un plan de développement de l'intelligence artificielle : 59 milliards de dollars de budget en 2025. A titre de comparaison, en 2018, les estimations du budget alloué par les Etats-Unis à la recherche sur l'IA ne dépassaient pas les 11 milliards de dollars.
https://www.franceculture.fr/numerique/lexpansion-des-batx-les-gafam-chinois

Sources

Loi n°68/678 du 26 juillet 1968 - loi de blocage française

http://archives.lesechos.fr/archives/cercle/2011/08/30/cercle_37239.htm

https://www.franceinter.fr/emissions/secrets-d-info/secrets-d-info-22-septembre-2018

https://frenchmorning.com/credit-score-les-nuls/

https://www.franceculture.fr/numerique/lexpansion-des-batx-les-gafam-chinois

https://www.lir.asso.fr/wp-content/uploads/2019/04/PLATEFORME-DES-DONNEES-DE-SANTE.pdf

http://www.senat.fr/compte-rendu-commissions/20190708/ce_souverainete.html#toc5

https://www.franceculture.fr/numerique/lexpansion-des-batx-les-gafam-chinois