Rencontres du Risk Management AMRAE 2020

Atelier C7

RGPD : quel constat 2 ans après ?

Intervenants

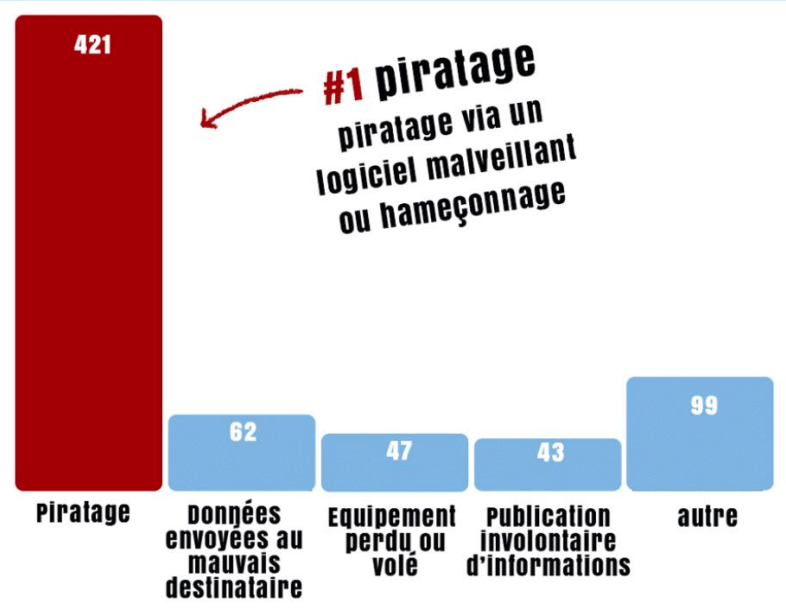
Jérôme Semik
Lagardère

Jérôme Avot
Faurecia

Pierre Craponne
Choisez Avocat

Sophie Parisot
AIG

Data privacy is coming…



Source : CNIL

Source : Google trends, recherche « data privacy » sur les 5 dernières années

Source : CNIL

RGPD : pour l'amour du risque

« Risque » : le mot apparaît 78 fois dans le RGPD.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Risque pour les personnes concernées,

Risque pour les entreprises qui traitent les données (financier, image)

=> Notre interrogation : quel recul sur les risques pour les entreprises 2 ans après l'entrée en vigueur du RGPD ?

Quel recul sur ces risques après 2 ans ?

- La vision de l'entreprise :
  - Quelles modalités de gestion

- La vision juridique :
  - Quels enseignements tirer des sanctions
  - Quelle sécurité juridique espérer

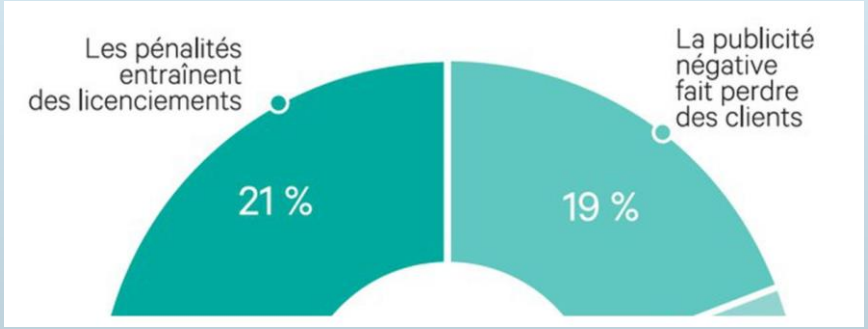
- La vision de l'assurance :
  - Quels enseignements tirer des sinistres
  - Comment y faire face

La vision de l’entreprise

Une approche par les risques et une recherche des opportunités au coeur du projet de mise en conformité

Retour vers le futur… RGPD Jour J – 12 Mois

- D’après un sondage réalisé en Avril 2017
  - **86 %** des entreprises interrogées (900) s'inquiètent des répercussions qu'entraînerait un défaut de conformité
  - **31 %** s’inquiètent de la **publicité négative** qui leur ferait **perdre des clients** (19%) ou impacterait leur **image de marque** (12 %)
  - **21 %** des entreprises craignent de devoir **réduire leurs effectifs** en cas d'amende
  - **18 %** redoutent **la faillite**



La cartographie des ~~risques~~ traitements

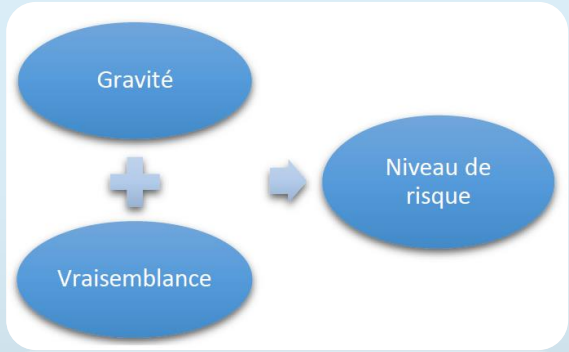
- La cartographie des traitements: un chantier initial souvent colossal pour les entreprises… mais un excellent point de départ:
  - Identification de l'ensemble des traitements de données personnelles et de l'ensemble de leurs caractéristiques:
    - **Finalités, personnes concernées, type et volume de données collectées, destinataires, durées de conservation, base légale, mesures de sécurité, prestataires…**
  - Identification des non-conformités et mise en œuvre des plans d'actions nécessaires
  - Mise en place et tenue du registre des traitements

Une approche par les risques… pour prioriser les plan d'actions

- Certaines entreprises ont dû faire face à de (très) gros volumes de demandes « d'évolutions » principalement:
  - Modification des durées de rétention (mise en place de « purges » automatisées)
  - Minimisation des données collectées (suppression de certains champs...)
  - Modification des dispositifs de sécurisation (chiffrement, gestion des accès…)
- Ces demandes ont dû faire l'objet d'arbitrage selon le « niveau de risque »:
  - Volume de données, sensibilité des données, pérennité de l'application…

Une approche par les risques… pour mettre en conformité les nouveaux traitements (AIVP)

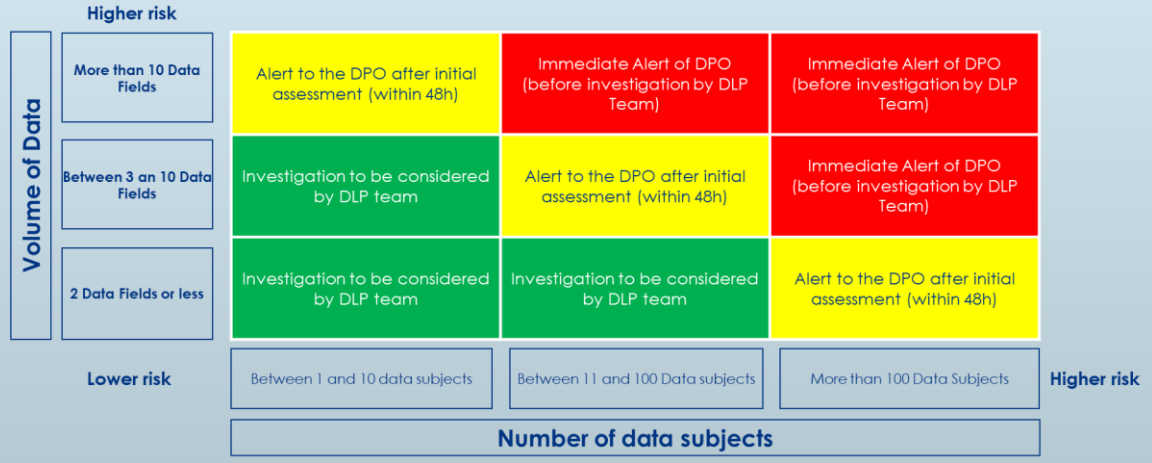
- L'Analyse d'Impact sur la Vie Privée (AIVP ou PIA) n'est autre qu'une analyse de risque focalisée sur 3 risques principaux:
  - Accès illégitime aux données
  - Modification non autorisée des données
  - Disparition des données



- La prise en compte des Mesures Techniques & Organisationnelles (MTO) permet de passer d'un risque « Brut » à un risque « Net »:
  - chiffrement, anonymisation, cloisonnement, contrôle d'accès, traçabilité, sécurité de l'exploitation, sauvegardes, sécurité des matériels, procédures, formations, gestion des incidents et violations, relations avec les tiers….

Une approche par les risques… pour gérer les fuites de données

- Lorsqu'une violation de données constitue un **risque** au regard de la vie privée des personnes concernées il est nécessaire de notifier la CNIL (dans un délai de 72h).
- La mise en œuvre d'un processus de remontée des violations combiné à un processus d'évaluation du risque permet de répondre à cette obligation.



Une approche par les risques… pour sélectionner ses prestataires

- Le RGPD impose un cadre juridique strict entre RT & ST
- Le RT est en première ligne en cas d'incident et doit donc s'assurer de la « fiabilité » de ses ST par différents moyens (audits, certifications, …)
- Le sujet des données personnelles est de plus en plus souvent au cœur des négociations (DPA, liability, lieu de stockage des données…) et rentre désormais en ligne de compte dans les critères de choix des prestataires

Un besoin de formation… contribuant à diffuser la culture de gestion des risques

- La formation des employés reste un pilier fondamental pour garantir le succès d'un programme de conformité au RGPD et ce afin de:
  - Transmettre les fondamentaux du RGPD (transparence, sécurisation, minimisation, durée de rétention…)
  - S'assurer de la connaissance des processus internes à l'entreprise (registre, exercice des droits, analyse d'impact, fuite de données…)
  - Véhiculer la culture de la **gestion du risque** en matière de protection des données personnelles

Des bénéfices pour les personnes concernées mais aussi pour l'entreprise

- Le RGPD a parfois servi de « bouc émissaire » au sein des entreprises pour lancer des chantiers ou débloquer des budgets
- Ce chantiers ont permis une amélioration globale de la gestion du risque « Cyber » au sein des entreprises:
  - Des applications plus sécurisées et contenant moins de données
  - Des infrastructures mieux contrôlées et adaptées aux enjeux
  - Des équipes mieux formées et conscientes des dangers
  - Des choix plus réfléchis en matière de sous-traitance

La vision juridique

Face au renforcement constaté des attentes et des sanctions, la nécessaire recherche d'une sécurité juridique dans les relations avec les partenaires

Aujourd'hui, qu'en est-il du (ou des) risque(s) liés au RGPD en terme de sécurité juridique ?

- 2 ans après l'entrée en vigueur du RGPD, doit on craindre ou tirer enseignement des sanctions prononcées sur ce fondement ?
- Quel est l'état de la règlementation et du contrôle de la protection des données à l'international ?
- Quelles conséquences pratiques en termes de relations contractuelles et de conformité sont à tirer au vu de ces constats ?

2 ans de décisions de la CNIL : craintes ou leçons ?

- Depuis l'entrée en vigueur du RGPD :
  - 21 décisions de la formation restreinte de la CNIL (**4 au visa du RGPD**) dont :
    - **15 sur un défaut de sécurité des données**
    - 4 sur un défaut d'information des personnes
    - 4 sur le non-respect des droits d'accès / d'opposition / d'effacement
  - 11 mises en demeure **publiques** dont :
    - 5 pour vidéosurveillance excessive
    - **4 pour défaut de sécurité des données**
    - 4 pour défaut de consentement au traitement des données

2 ans de décisions de la CNIL : craintes ou leçons ?

- Focus sur les 4 sanctions prononcées au visa du RGPD :
  - Délibération du 21 janvier 2019 (affaire GOOGLE LLC)
  - Délibération du 28 mai 2019 (affaire SERGIC)
  - Délibération du 18 juillet 2019 (affaire ACTIVE ASSURANCES)
  - Délibération du 21 novembre 2019 (affaire FUTURA INTERNATIONALE)

2 ans de décisions de la CNIL : craintes ou leçons ?

- Focus sur les 4 sanctions prononcées au visa du RGPD :
  - Délibération du 21 janvier 2019 (affaire GOOGLE LLC)
    - Manquements aux obligations de transparence, d'information et de disposer d'une base légale pour les traitements mis en œuvre
    - Manquements jugés graves (nature et ampleur) et perdurant au jour de la décision
    - Sanction = 50.000.000 € + publicité (environ 0,05% du CA / 15% du CA de l'établissement en France – rapporteur suivi)
  - Délibération du 28 mai 2019 (affaire SERGIC)
  - Délibération du 18 juillet 2019 (affaire ACTIVE ASSURANCES)
  - Délibération du 21 novembre 2019 (affaire FUTURA INTERNATIONALE)

2 ans de décisions de la CNIL : craintes ou leçons ?

- Focus sur les 4 sanctions prononcées au visa du RGPD :
  - Délibération du 21 janvier 2019 (affaire GOOGLE LLC)
  - Délibération du 28 mai 2019 (affaire SERGIC)
    - Particularité : absence de mise en demeure préalable
    - Manquements aux obligations d'assurer la sécurité et la confidentialité des données à caractère personnel et de conserver les données pour une durée proportionnée
    - Manquements jugés graves et une réaction jugée trop lente
    - Sanction = 400.000 € + publicité (environ 1% du CA)
  - Délibération du 18 juillet 2019 (affaire ACTIVE ASSURANCES)
  - Délibération du 21 novembre 2019 (affaire FUTURA INTERNATIONALE)

2 ans de décisions de la CNIL : craintes ou leçons ?

- Focus sur les 4 sanctions prononcées au visa du RGPD :
  - Délibération du 21 janvier 2019 (affaire GOOGLE LLC)
  - Délibération du 28 mai 2019 (affaire SERGIC)
  - Délibération du 18 juillet 2019 (affaire ACTIVE ASSURANCES)
    - Particularité : absence de mise en demeure préalable
    - Manquement à l'obligation d'assurer la sécurité et la confidentialité des données à caractère personnel
    - Manquements jugés graves mais rapidité de la réaction et coopération avec la CNIL remarquées
    - Sanction = 180.000 € + publicité (environ 1,7% du CA)
  - Délibération du 21 novembre 2019 (affaire FUTURA INTERNATIONALE)

2 ans de décisions de la CNIL : craintes ou leçons ?

- Focus sur les 4 sanctions prononcées au visa du RGPD :
  - Délibération du 21 janvier 2019 (affaire GOOGLE LLC)
  - Délibération du 28 mai 2019 (affaire SERGIC)
  - Délibération du 18 juillet 2019 (affaire ACTIVE ASSURANCES)
  - Délibération du 21 novembre 2019 (affaire FUTURA INTERNATIONALE)
    - Manquements aux obligations de traiter des données adéquates, pertinentes et limitées à ce qui est nécessaire au regard de leurs finalités, d'informer les personnes, de respecter le droit d'opposition, de coopérer avec l'autorité de contrôle, d'encadrer les transferts de données à caractère personnel hors de l'UE
    - Manquements jugés graves (nature et nombre) et perdurant au jour de la décision
    - Sanction = 500.000 € + publicité (environ 2,5% du CA – rapporteur suivi)

2 ans de décisions de la CNIL : craintes ou leçons ?

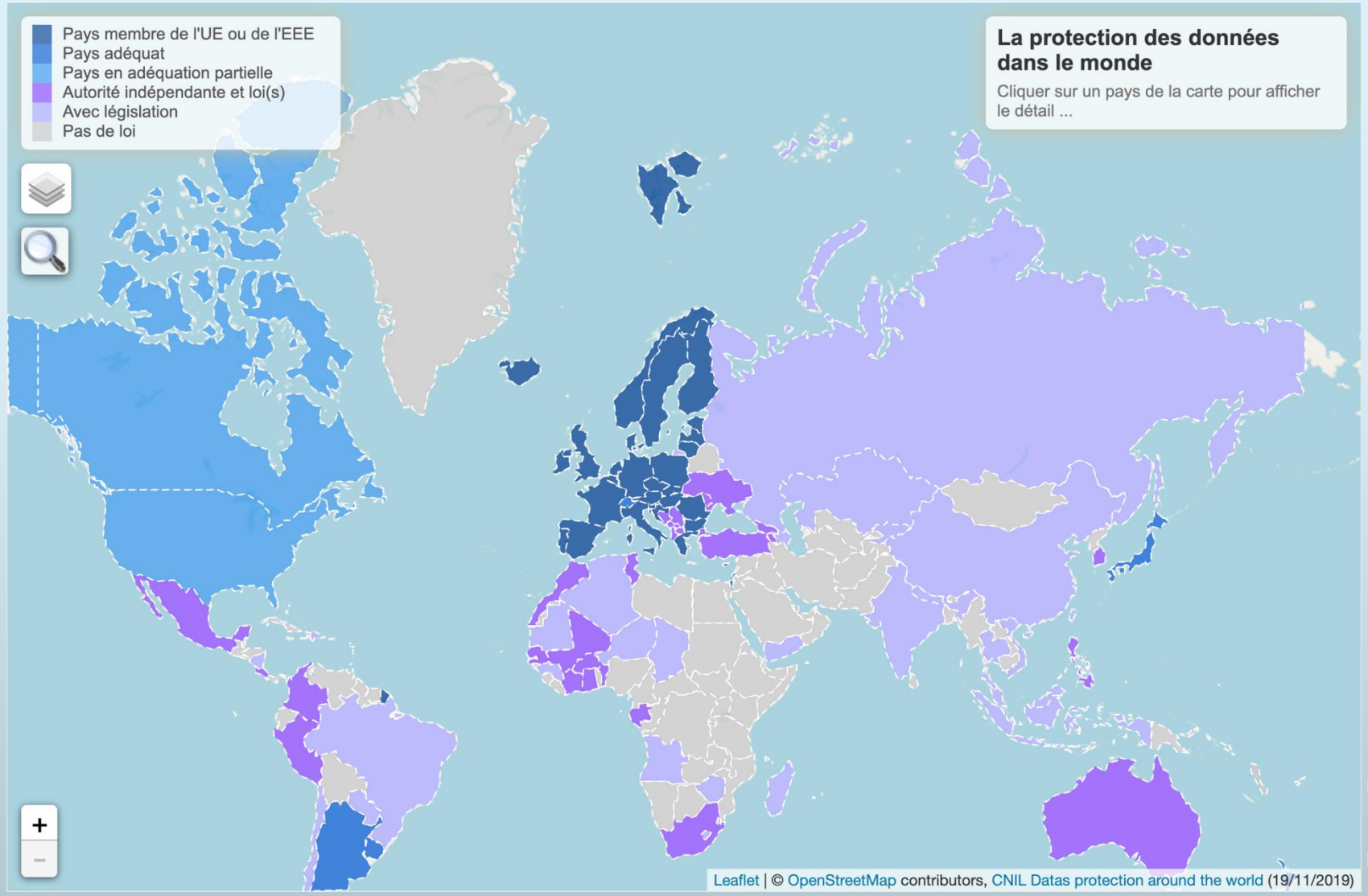
- En synthèse :

  - Une volonté résolument pédagogique de la CNIL d'expliciter le principe et le montant de ses sanctions
  - Des sanctions amenées à se durcir avec le temps (prise en compte de la durée du manquement et de la qualité de l'auteur)
  - **La CNIL est particulièrement vigilante sur la sécurité des données**
  - A noter sur ce défaut de sécurité : **peu de MED et des sanctions sans MED**

Et pendant ce temps, du côté des juridictions suprêmes …

- En marge des sanctions de la CNIL : **16 décisions relatives au déréférencement** :
  - CJUE, 24 septembre 2019, n°C-136/17 et C-507/17
  - Civ. 1ère, 27 novembre 2019, n°1814675
  - CE, 6 décembre 2019, n°391000, n°393769, n°395335, n°397755, n°399999, n°401258, n°403868, n°405464, n°405910, n°407776, n° 409212, n°423326, n° 429154
- Apport de ces décisions : un **mode d'emploi du déréférencement** donc une **plus grande sécurité juridique** sur cette question

Tour d’horizon : privacy abroad



Comment sanctionnent nos voisins ?

- Au total, 114.000.000€ d'amende dans l'UE (51.100.000€ en France)
- **Retour sur deux affaires British Airways et Mariott devant l'ICO**
  - Sanction proposée : British Airways 203.000.000€ / Mariott 110.000.000€
  - Faits reprochés : négligence et non-conformité au RGPD ayant conduit à des incidents de sécurité et la captation en masse de données personnelles
- **Interrogations sur l'affaire ACCOR actuellement pendante**
  - Faits : défaut de paramétrage d'un serveur ayant conduit à un défaut de protection de données personnelles et bancaires de nombreux voyageurs
  - Notification à la CNIL le 16 novembre 2019

Analyse d'impact du RGPD sur les relations commerciales

- En clair, le risque lié à la protection des données est réel et la CNIL sanctionne (de plus en plus ?) lourdement
- Les autorités et les règlementations à travers le monde, et même au sein de l'EEE, restent toutefois hétérogènes
- Dans ces conditions :
  - Comment organiser ses relations commerciales et contractuelles sur cette question de la protection des données ?
  - Comment aborder les responsabilités en cas d'exposition de ses propres données ou des données du client du fait d'un partenaire ?

Analyse d'impact du RGPD sur les relations commerciales

- **<u>Première réponse : technique</u>**
  - Solliciter un audit de conformité RGPD avant toute forme de relation commerciale (certification européenne (article 42), cahier des charges …)
  - Partager des solutions de mise en conformité technique pour assurer un contrôle homogène au sein d'un même groupe / réseau (accountability)
- **<u>Deuxième réponse : juridique</u>**
  - Prévoir contractuellement la circulation des données entre partenaires et notamment en présence d'un sous-traitant
  - Intégrer des clauses de partages / de limitation de responsabilité sur ces questions dans la limite de la règlementation applicable

Et après le RGPD ?

- Le RGPD est appliqué à « marche forcée » par la CNIL et les juridictions judiciaires et administratives
- 2 ans après son entrée en vigueur, les principaux risques en résultant sont globalement identifiés
- Pourtant ce début de « stabilité juridique » pourrait être remis en cause par le Règlement dit « e-Privacy » …
- … potentielle source d'insécurité juridique (voir la lettre ouverte du 8 octobre 2019 au Conseil de l'UE)

La vision de l’assurance

Un accroissement des sinistres, une recherche de solutions en accompagnement des entreprises

Qu’entend-on par Cyber-Risques ?

Définition : les conséquences d’une atteinte aux données numériques détenues et/ou gérées par l’entreprise, que celles-ci lui appartiennent ou qu’elles lui soient confiées par des tiers, ainsi que les conséquences d’une atteinte au système informatique.

Les atteintes aux données numériques

- Données appartenant aux tiers
- Données des collaborateurs
- Données des clients
- Données des fournisseurs, prestataires ou sociétés partenaires

Les atteintes au système informatique

- Intrusion dans les systèmes informatiques
- Interruption des systèmes informatiques
- Contamination des systèmes informatiques (virus, bombe logique…)
- Utilisation illégale des systèmes et du réseau

Le marché Cyber 2019

Le marché cyber poursuit sa croissance en France et en Europe, le RGPD étant un vecteur poussant les entreprises à s'assurer.

Chez AIG, nous avons constaté une augmentation immédiate des soumissions et souscription suite à son entrée en vigueur en 2018.

- En 2019, le portefeuille AIG EMEA a connu une croissance de plus de 20%.
- Marché cyber en France s'établit à 80M€ selon la FFA
- Taux de pénétration demeure faible pour les PME
- Marché plutôt haussier tiré par la sinistralité

Que peut-on transférer? Les garanties principales

Gestion d'incident

- Actions d'urgence
- Frais et Dépenses garantis

Responsabilité Civile

- Atteintes aux données
- Atteintes au système informatique

Dommages

- Perte d'exploitation
- Enquête et Sanction
- Cyber Extorsion

Focus RGPD: Volet Enquêtes et Sanctions

Enquête d'une autorité administrative

Prise en charge des frais de défense dans le cadre de toute enquête introduite à son encontre par une autorité administrative pendant la période d'assurance

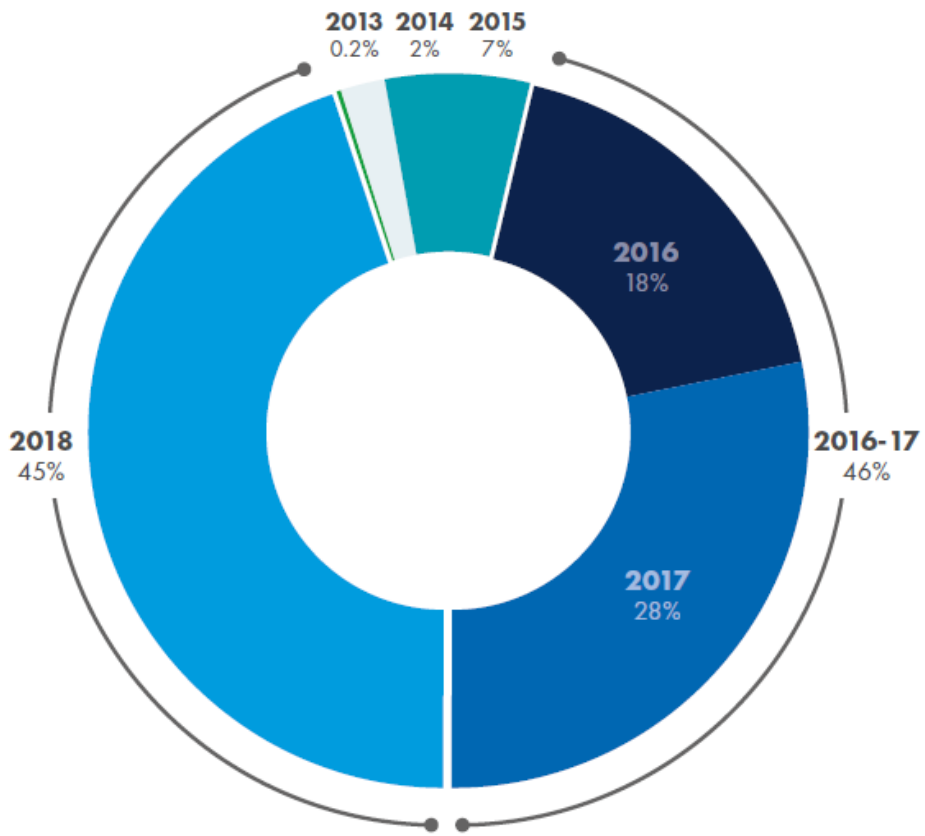
Sanctions pécuniaires prononcées par une autorité administrative

Prise en charge des sanctions pécuniaires légalement assurables suite à une enquête

La CNIL en France ou toute autorité équivalente à l'étranger

Retour d'expérience: volume sinistres Cyber EMEA AIG

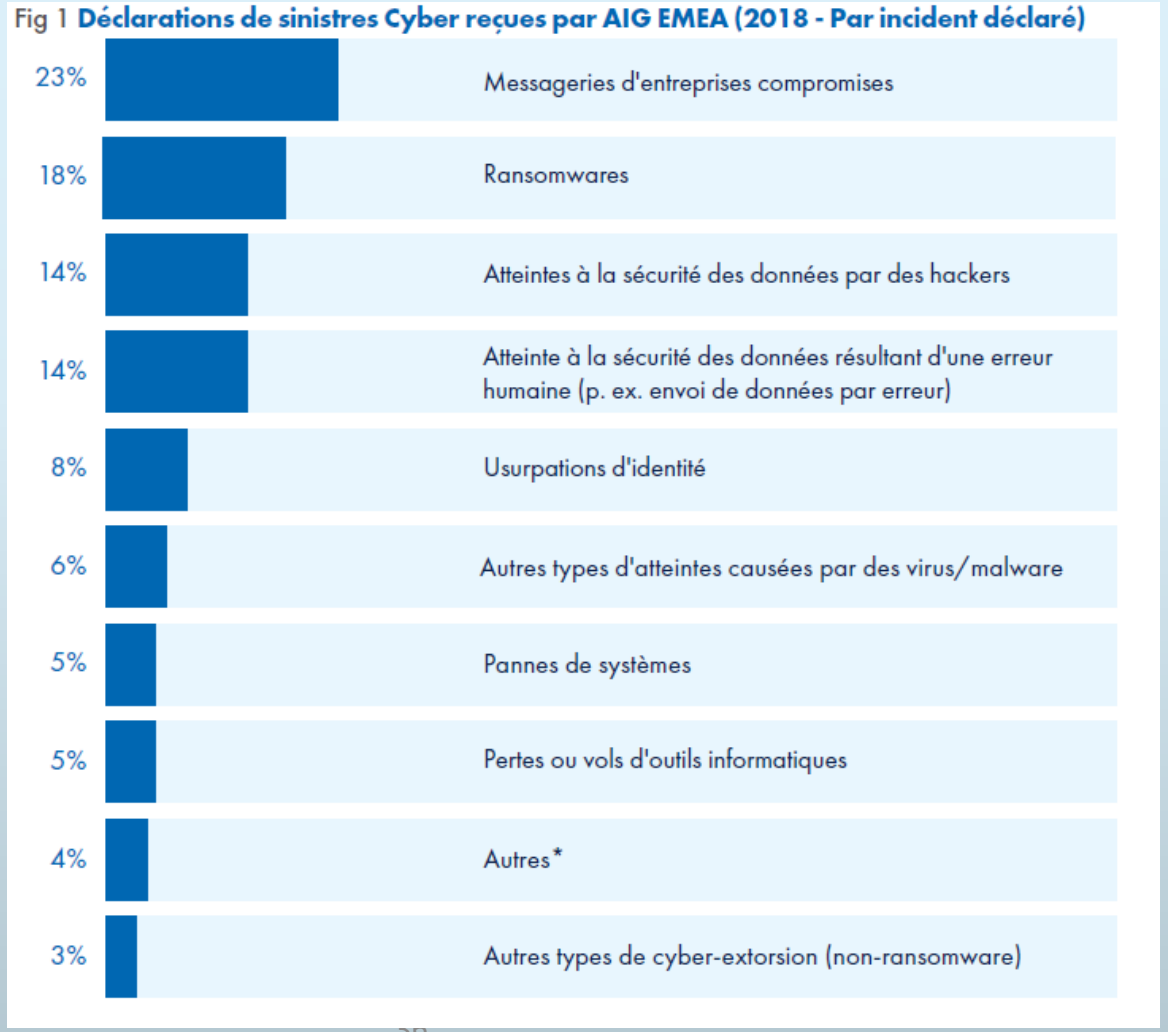
Fig 3 **Déclarations de sinistres Cyber reçues par AIG EMEA (2013-2018) - Volume**



- En moyenne 1,8 notification reçue par AIG EMEA par jour contre 1,4 notifications en 2017 (plus de 6 notifications par jour aux USA)
- En 2019, la tendance se poursuit, avec plus de 70 sinistres gérés en France soit autant que depuis le lancement de l'offre en 2012.
- 20% des sinistres déclarés incluaient une notification en vertu du RGDP

Retour d'expérience sur la sinistralité: par type d'incidents

Fig 1 **Déclarations de sinistres Cyber reçues par AIG EMEA (2018 - Par incident déclaré)**



- ❑ Les atteintes aux données représentent 28% des incidents déclarés en 2018 contre 19% en 2017

⇒ L'entrée en vigueur du RGPD a entrainé un pic de déclarations, les obligations strictes en matière de notification se traduisent par une déclaration rapide des assurés

- ❑ Les paiements effectués au titre des actions d'urgence sont 50% supérieurs si le sinistre concerne une atteinte aux données personnelles
- ❑ Fossé entre Europe du Nord et Europe du Sud en termes de notifications

Cas pratique 1: cyber attaque

Sinistre

L'Assuré est un site de vente en ligne. L'Assuré est informé par une de ses banques partenaires d'une activité suspicieuse sur son réseau. Après investigation, l'Assuré découvre qu'il est victime d'une attaque Web Shell.

Les données personnelles et données bancaires de 146.000 personnes concernées seraient compromises avec de plus de 10 nationalités différentes.

Situation

Experts informatiques missionnés pour établir l'intrusion et y remédier.

Cabinet d'avocats missionné pour évaluer la nécessité et la formalisation de la notification dans les différentes juridictions (voir ci-après).

Notification de l'atteinte aux personnes concernées (40.976).

Cabinet de communication de crise missionné pour établir la communication auprès des personnes concernées et possibilité de la prise en charge d'un service de monitoring des données dérobées.

Cas pratique 1: cyber attaque

Pays	Notifications obligatoires ?
China	Oui: personnes concernées et autorités
Hong-Kong	Oui: personnes concernées et autorités
India	Non, obligatoire seulement si l'atteinte se produit sur un SI en Inde
Indonesia	TBC
Japan	Oui: personnes concernées et autorités
Philippines	Oui: personnes concernées et autorités
Singapore	Non mais le PDPC recommande la notification si l'impact potentiel est élevé sur les personnes concernées
South Korea	Oui: personnes concernées et autorités
Taiwan	Oui: personnes concernées

Cas pratique 1: cyber attaque

Conséquences pécuniaires

- Audit informatique: 60k€
- Experts informatiques: 200k€
- Communication de crise: 27k€
- Frais de notification : 60k€
- Frais d'avocat: 327k€
- Pénalités PCI-DSS: 350k€

=> Plus d'un 1M€

Cas pratique 2: cyber attaque

Sinistre

L'Assuré est un site de généalogie en ligne. Atteinte aux données personnelles des utilisateurs (92M – adresse email + MDP). Les données concernant l'ADN et l'arbre généalogique ne sont pas concernées.

Situation

Notification de l'atteinte aux autorités locales mais également aux autorités anglaises, autorités de 14 états aux USA, aux autorités Brésiliennes, Canadiennes, Russes et Australiennes.

13/09/18: class action introduite aux USA par des utilisateurs pour défaut de sécurité des systèmes, atteinte à la confidentialité, atteinte à la vie privée

Conséquences pécuniaires

Gestion de crise: USD 50k

Frais de notification : USD 150k

Frais d'avocat dans le cadre de la class action (USD 400k jusqu'à la MTD ou USD 1.2M si MTD rejetée) et prise en charge des éventuels D&I

Cas pratique 3: erreur humaine

Sinistre

L'Assuré est une entreprise de communication. En septembre 2019, dans la filiale Sud africaine, un employé du service RH transmets par erreur un fichier Excel contenant les données personnelles de 175 employés à 42 personnes. Cette pièce jointe a ensuite été transférée à 165 personnes dans une liste de distribution puis transférée à un nombre inconnu de personnes.

Les données personnelles contiennent notamment: nom, prénom, email, salaire, adresse postale, données bancaires, numéro de sécurité sociale, handicap ect.

Situation

Le cabinet d'avocat missionné localement évalue les obligations légales de notification.

Après investigation, pas d'obligation de notification localement ni la CNIL en France.

Communication de crise réalisée par l'Assuré

Conséquences pécuniaires

Gestion de crise : 50k€

Pas de réclamation des personnes concernées à ce stade

Conclusion

En France, les sinistres concernant une atteinte aux données ont un coût plus important en moyenne mais les sinistres d'intensité observés concernent les pertes d'exploitation.

Le RGPD a permis l'allocation de budget pour souscrire des polices d'assurance cyber dont la vocation est de traiter le risque cyber au-delà de la seule problématique RGPD.

N'ayant pas de cas concret à exposer sur 2019, l'assurabilité des sanctions CNIL demeure une question ouverte.

L'année 2020 sera charnière, à suivre!

Conclusion générale