

Algo & risque

David Dubois

Voahirana Ranaivozanany

Journée de Deauville ... à Paris

16 septembre 2021

Algo et risque

1

Les algorithmes peuvent-ils être générateurs de (nouveaux) risques ?

2

La gestion des risques peut-elle être « augmentée » par les algorithmes ?

Les algorithmes sont des instructions générales d'action pour résoudre des problèmes

« un algorithme est une suite finie et non ambiguë d'instructions permettant d'aboutir à un résultat à partir de données fournies en entrée » (CNIL, 2017)

- Le monde numérique repose sur des algorithmes avec une généralisation des algorithmes depuis 15 ans (secteurs privé et public)
- Recherche de performance dans les algorithmes
 - Recherche des meilleurs résultats avec la moindre consommation de ressources possibles (données, temps de calcul, ...)
- Nécessité de mettre en place un **regard critique** sur les dérives possibles
 - Impacts et enjeux en termes de droits pour ceux qui en subissent les conséquences
 - Débat citoyen non engagé (lois, morale et culture)

Utiliser la Data science, c'est choisir d'explorer une méthode en ambitionnant une création de valeur

- Piloter avec la data science c'est choisir d'innover, et comporte encore une grande dimension d'exploration
- Vouloir faire de la data science c'est vouloir faire parler les données à travers des algorithmes pour en extraire les informations essentielles
- Motivations : Mieux connaître, mieux décider, mieux agir, avec un objectif de création de valeur

Des risques comme pour tout mais de nouveaux risques car une nouvelle approche

- Appliquer la Data Science pour piloter dans l'assurance reste **une utilisation émergente**
- Trois principales sources de risques : données, algorithmes, informations extraites
- Nouvelle approche donc nouvelles pratiques donc **nouveaux risques** ou **nouveaux niveaux de risques**



Nouvelles menaces
engendrées par
l'Intelligence Artificielle

Exemples d'application de l'IA

| | Education | Justice | Santé | Sécurité | Travail, RH | Culture | Autres |
|-----------------------------------|--|---|--|--|--|---|---|
| Générer de la connaissance | Mieux cerner les aptitudes d'apprentissage des élèves | Mettre en évidence les manières différenciées de rendre la justice selon les régions | Tirer profit de la quantité immense de publications scientifiques | Repérer des liens insoupçonnés pour la résolution d'enquêtes par les services de gendarmerie | Comprendre les phénomènes sociaux en entreprise | Créer des œuvres culturelles (peinture, musique) | Affiner le profil de risque d'un client d'un assureur |
| Faire du matching | Répartir les candidats au sein des formations d'enseignement supérieur (AP8) | | Répartir des patients pour participation à un essai clinique | | Faire correspondre une liste de candidatures avec une offre d'emploi | | Mettre en relation des profils « compatibles » sur des applications de rencontres, etc. |
| Prédire | Prédire les décrochages scolaires | Prédire la chance de succès d'un procès et le montant potentiel des dommages-intérêts | Prédire des épidémies Repérer des prédispositions à certaines pathologies afin d'en éviter le développement | Détecter les profils à risque dans la lutte anti-terroriste Prédire l'occurrence future de crimes et délits | Détecter les collaborateurs qui risquent de démissionner dans les prochains mois | Créer des œuvres ayant un maximum de chance de plaire aux spectateurs (Netflix) | |
| Recommander | Recommander des voies d'orientation personnalisées aux élèves | Recommander des solutions de médiation en fonction du profil des personnes et des cas similaires passés | | | Proposer des orientations de carrière adaptées aux profils des personnes | Recommander des livres (Amazon), des séries télévisées (Netflix), etc. | Individualiser des messages politiques sur les réseaux sociaux |
| Aider la décision | | Suggérer au juge la solution jurisprudentielle la plus adéquate pour un cas donné | Suggérer au médecin des solutions thérapeutiques adaptées | Suggérer aux forces de police les zones prioritaires dans lesquelles patrouiller | | | Aider le conducteur à trouver le chemin le plus court d'un point à un autre (GPS) |

Source : Rapport de la CNIL - Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle (Décembre 2017)

« *AI-enabled future crime* »

Caldwell, Andrews, Tanay & Griffin

2020, University College London (UCL)

- Développement accélérée de l'usage du machine learning dans tous les secteurs d'activités, parfois légitimé par la réglementation
- Travaux réalisés au sein de l'UCL pour identifier les risques et rédiger une compilation de 20 activités illégales perpétrées par IA
 - Classement en 3 groupes : « menaces graves », « menaces de moyenne gravité » et « menaces de faible intensité »
- Classement par ordre
 - de dommages potentiels, de gains ou profits engrangés
 - de facilité à mettre en œuvre
 - et de difficulté à détecter et à stopper les menaces

Classe 1

Menaces graves

- Fausses vidéos
- Piratage de voitures autonomes
- Hameçonnage sur mesure
- Piratage des systèmes contrôlés par IA
- Chantage à grande échelle
- Fausses informations rédigées par IA

Classe 2

Menaces de moyenne gravité

- Robots militaires
- Escroquerie
- Corruption de données
- Cyberattaque basée sur l'apprentissage
- Drones d'attaque autonomes
- Refus d'accès
- Reconnaissance faciale
- Manipulation de marchés financiers

Classe 3

Menaces de faible intensité

- Exploitation de préjugés
- Robots cambrioleurs
- Blocage de détection par IA
- Fausses critiques rédigées par IA
- Traque assistée par IA
- Contrefaçon



De nouveaux risques
pour les entreprises

Profils de risque
Facteurs générateurs de risque
(Deloitte, 2019)

- Qualité, quantité et pertinence des données utilisées
- Opacité de fonctionnement
- Dysfonctionnements possibles

Profils de risque Nouveaux risques pour les entreprises (Deloitte, 2019)

- Bouleversement de l'environnement concurrentiel
- Dépendance à l'égard de tiers
- Défaillance des systèmes de l'IA
- Risques humains
- Risques liés aux compétences
- Risques éthiques
- Risques juridique et conformité

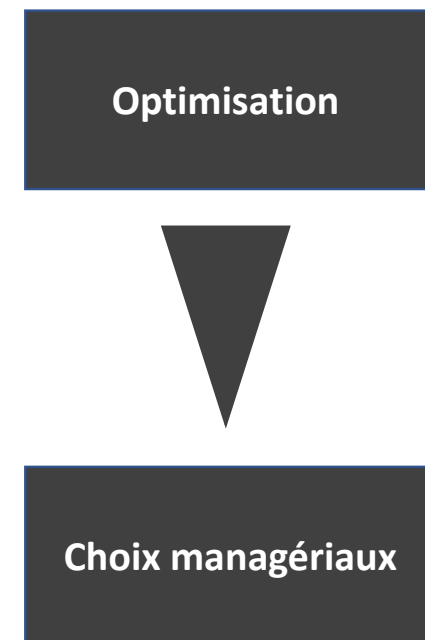
**Business model et
chaîne de valeur**

Modèle social

**Environnement
réglementaire**

Profils de risque
Nouvelles opportunités pour les entreprises
(Deloitte, 2019)

- Automatisation d'une plus grande variété de tâches
- Meilleure exploitation des données disponibles
- Optimisation et objectivisation des prises de décision
- Efficacité opérationnelle accrue





Intégrer les principes de l'ERM dans le déploiement de la data science

| DOMAINES | | TYPES DE PROJETS |
|-------------------|----------------------------------|--|
| AXE DÉVELOPPEMENT | OPTIMISATION DE LA VALEUR CLIENT | <ul style="list-style-type: none"> Analyse de l'élasticité aux majorations Analyse du risque de résiliation Anticipation des évolutions de comportement |
| | CRM, MARKETING ET CIBLAGE | <ul style="list-style-type: none"> Meilleure connaissance des clients et optimisation globale du parcours client Ciblage des campagnes marketing en vue d'en maximiser l'efficacité Optimisation du taux de concrétisation des devis |
| | OFFRE ET SERVICES | <ul style="list-style-type: none"> Conception de nouveaux services rendus possibles par les nouvelles données Intégration des nouvelles technologies dans les offres actuelles Interaction en temps réel |
| AXE TECHNIQUE | SUIVI TECHNIQUE | <ul style="list-style-type: none"> Identification des segments déficitaires et modulation des majorations tarifaires Anticipation des évolutions du risque Aide à la détermination du coût ultime de la sinistralité |
| | TARIFICATION | <ul style="list-style-type: none"> Analyse de l'élasticité au prix d'achat et intégration dans le « competitive pricing » Modification du tarif par l'intégration de « scorings » multicritères Modification du tarif par l'intégration de données externes nouvelles |
| AXE GESTION | FRAUDE | <ul style="list-style-type: none"> Identification des comportements atypiques Aide à la décision sur cas litigieux et aide à la souscription Identification des informations déclaratives falsifiées |
| | SINISTRES | <ul style="list-style-type: none"> Estimation du degré d'urgence et priorisation des dossiers à traiter Contrôle de la bonne gestion et de la correcte liquidation des dossiers Aide à la détection de risques d'erreurs dans le paiement des dossiers |

Données : quels types de nouveaux risques ?

- La data science s'appuie souvent sur des données réorganisées, rassemblées, complétées.
- Les données sont analysées à travers la constitution d'un échantillon, lorsqu'elles sont très volumineuses.
 - ➔ La qualité de prédiction du modèle obtenu dépend de la représentativité de cet échantillon : risque de biais de sélection.

Données : quels types de nouveaux risques ?

- Dans la base reconstituée pour la data science,
 - Des variables très peu utilisées dans le passé ont été reprises : peu connues et moins testées par les travaux successifs.
 - Des données provenant de plusieurs sources : la connaissance et la compréhension globales sont des points d'attention.
 - Des données non structurées éparpillées ont été rassemblées : gestion manuelle dans le passé avec le risque d'anomalie associé.




Ces données ont, bien entendu, été recettées. Néanmoins, elles restent non éprouvées et avec un risque de biais plus élevé.

Données : quels types de nouveaux risques ?

- Les risques de biais associés aux données externes sont encore plus élevés, l'utilisation de données externes étant encore moins habituelle.
- Au-delà :
 - Risque RGPD en franchissant potentiellement les autorisations obtenues pour l'utilisation des données
 - Augmentation du **risque cyber** dans un contexte de forte valorisation des données

Algorithmes : quels sont les risques ?

- Aux datas sont appliqués les algorithmes, une bonne connaissance métier conditionne la qualité et la pertinence des analyses réalisées.
 - Le choix des variables à retenir gagne à être orienté par des compétences métiers (entre variables fortement corrélées, choisir les plus appropriées selon l'objectif de l'analyse)
 - Le traitement des données manquantes doit aussi être réalisé selon la finalité de l'analyse (ex : prudence si finalité tarifaire)
 - ...
-  Une étude réalisée sans suffisamment comprendre la matière et la finalité introduit des risques techniques (ex : sous-tarifcation, sous-provisionnement, loi de rachats biaisée, ...)

Algorithmes : quels sont les risques ?

- Chaque modèle ou combinaison de modèles revêt des points forts et des points d'arbitrages.
 - Le choix dépend de l'objectif.
 - La maîtrise des méthodes est essentielle.
- ➔ La mise en place d'un modèle trop élaboré comparé au besoin ressort trop coûteux. Mais de mauvaises décisions pourraient être prises sur la base d'un modèle trop simplifié intégré dans un processus de décision automatisé. **Risque de modèle.**

Informations extraites : pourquoi ça peut générer des risques ?

- La justesse des informations extraites d'une analyse data science est essentielle.
 - Un travail peut être très juste au niveau théorique mais ressortir des résultats sujets à (mauvaises) interprétations, avec les **biais d'utilisation** associés.
 - Certains modèles « boîtes noires » peuvent ressortir des résultats très informatifs, sans possibilité de rationaliser. Les utiliser sans analyses croisées augmente le **risque décisionnel** par la difficulté d'un second regard « humain ».



Maitriser le
risque de perte de
contrôle

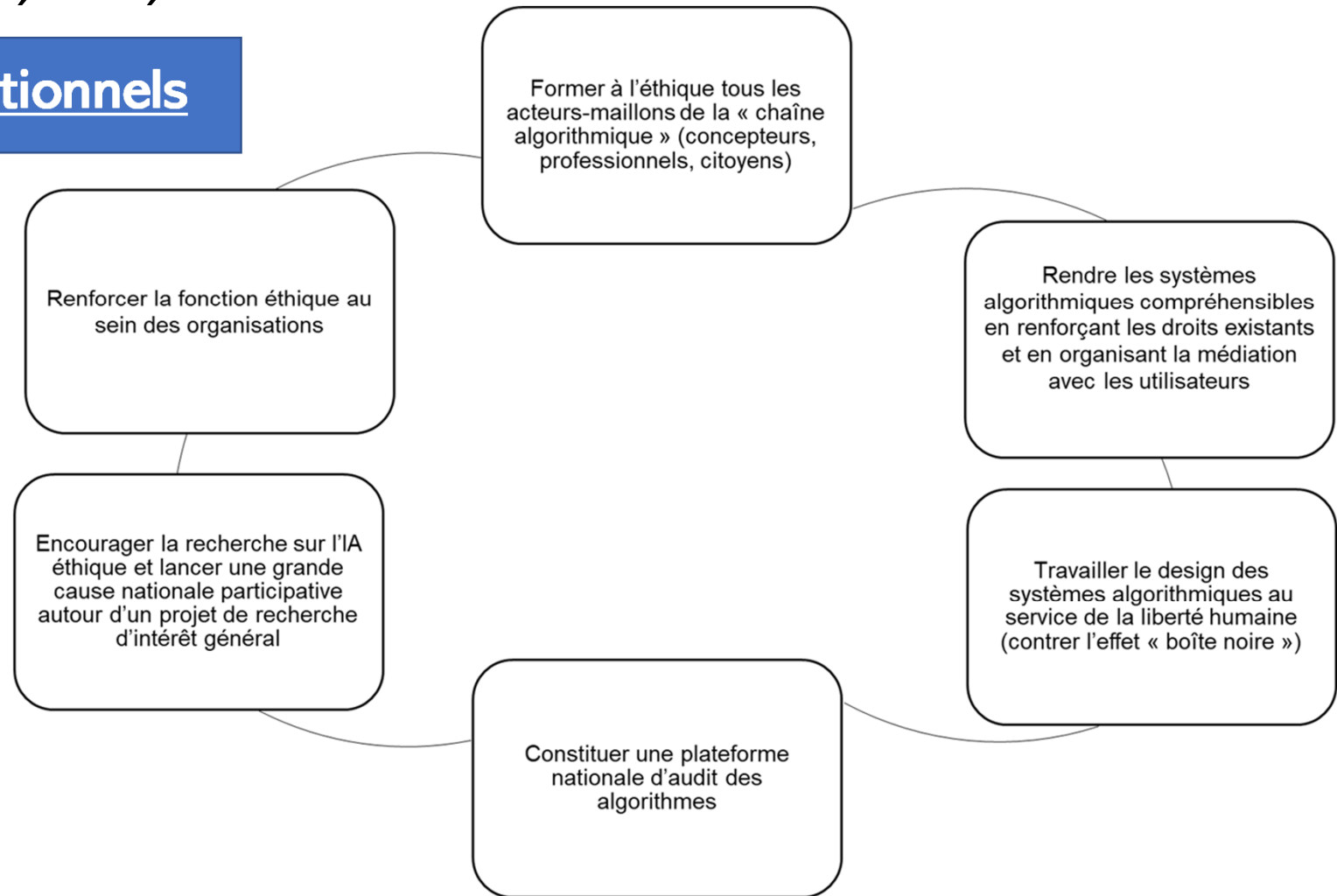
« Comment permettre à l'homme de garder la main ? Enjeux éthiques des algorithmes de l'IA », CNIL, 2017

Subqf1shv#irggdwhxuv

- **Principe de loyauté** : le traitement des données, à caractère personnel ou non, par un algorithme doit mener à des résultats loyaux envers les utilisateurs non seulement dans une optique individuelle (pour les utilisateurs en question) mais aussi plus largement dans les effets possibles sur la collectivité. Ce principe questionne largement la manière avec laquelle l'algorithme sera mis en œuvre opérationnellement au sein de la chaîne de valeur des organisations ;
- **Principe de vigilance (ou de réflexivité)** : un questionnement régulier, méthodique et délibératif à l'égard des algorithmes doit être mis en place visant à contrer la confiance excessive qui leur est parfois donnée. Ce principe suppose que des procédures concrètes soient appliquées tout au long de la chaîne algorithme depuis sa conception.

« Comment permettre à l'homme de garder la main ? Enjeux éthiques des algorithmes de l'IA », CNIL, 2017

Subsidiarités organisationnelles



« Lignes directrices pour une IA responsable » Commission européenne, juin 2018

- 4 principes éthiques ancrés dans les droits fondamentaux auxquels les praticiens de l'IA devraient s'efforcer de s'y conformer :
 - Le respect de **l'autonomie humaine** en gardant un contrôle sur l'IA sans risque de contrainte ou de manipulation sur les êtres humains
 - La **prévention de toute atteinte ou nuisance** de quelque façon que ce soit aux êtres humains (risque d'asymétrie de pouvoir ou d'informations)
 - **L'équité dans le partage des coûts et des avantages** liés à l'IA (éviter les discriminations et les biais, mettre en place des mécanismes de recours efficaces contre les décisions prises par l'IA)
 - **L'explicabilité des procédés et des décisions** en fonction du contexte et de la gravité des conséquences d'un résultat erroné.

« IA digne de confiance » : cadre juridique / approche par les risques

Commission européenne, avril 2021

Risque inacceptable

menace évidente pour la sécurité, les moyens de subsistance et les droits des personnes

systèmes ou applications qui manipulent le comportement humain pour priver les utilisateurs de leur libre arbitre

systèmes qui permettent la notation sociale par les États.

Risque élevé

infrastructures critiques (par exemple les transports) avec risque de mise en danger la vie et la santé

éducation ou formation professionnelle (accès et parcours)

domaine de l'emploi, de la gestion de la main d'œuvre et de l'accès à l'emploi indépendant

...

Risque limité

Obligations strictes en matière de transparence

(ex : informer que l'interaction avec chatbot est basée sur l'IA)

Risque minime

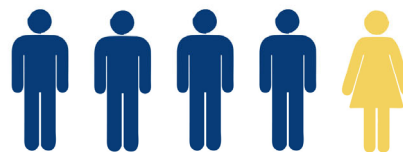
risque minime, voire nul, pour les droits ou la sécurité des citoyens.

utilisation libre d'applications

Conformité à des obligations strictes

(évaluation et atténuations des risques, qualité des données, traçabilité, informations claires ...)

« Recommandation
sur l'éthique de
l'intelligence
artificielle »
UNESCO



Seulement 22%
des professionnel.le.s de l'IA
sont des **FEMMES**

Source: World Economic Forum

11  **MILLIONS**
d'étudiant.e.s

pourraient 
bénéficier de l'IA
pour terminer leurs


ÉTUDES SECONDAIRES

Source: Accenture

L'IA  **devrait**
générer
près de US\$4 trillions
de valeur ajoutée d'ici
2022

Source: Gartner



**L'EXTRACTION
DE DONNÉES**


consomme près de
10% de l'énergie
mondiale

Source: Anders S.G. Andrae et al.

Projet « Recommandation sur l'éthique de l'intelligence artificielle » UNESCO, 2020

- « Nous avons besoin d'une IA centrée sur l'humain, qui servirait l'intérêt supérieur des citoyens, et non pas l'inverse » (éthique moralisante choisie par l'UNESCO)
 - Besoin de politiques et de cadres réglementaires internationaux de même que nationaux pour faire en sorte que ces technologies émergentes profitent à l'humanité tout entière
 - Besoin d'une IA centrée sur l'humain, qui servirait l'intérêt supérieur des citoyens, et non pas l'inverse
- Proposition d'élaborer un instrument normatif mondial visant à doter l'IA d'une base éthique solide, qui non seulement protégera mais aussi promouvra les droits et la dignité humains
 - Boussole éthique et base normative globale permettant de faire respecter l'État de droit dans le monde numérique

Impacts pour les entreprises en termes d'ERM

Le déploiement de l'IA impose ...

- Suivi des évolutions réglementaires et la mise en conformité (y compris sur soft law)
- Mise en place d'une gouvernance et questionnement permanent

Attention à la surestimation de la maturité sur le sujet (étude BCG, mars 2021)

- Gouvernance des données et respect de la vie privée : OK majoritairement
- Justice et équité, impact social et environnemental, approche « Humain augmenté sans s'y substituer » : KO

La responsabilité
comme nouvelle
source de risque



Principe général posé par la réglementation : Protéger toute personne physique identifiable

- Deux dispositions de la loi Informatique et Libertés de 1978
 - Principe d'interdiction de décision sur le seul fondement d'un traitement automatisé
 - Droit à une explication en cas de décision automatisée
- Renforcé dans la loi pour une République numérique (2016) et le règlement général pour la protection des données personnelles (RGPD)

La tentation de déporter une décision humaine vers l'algorithme existe et le risque associé est difficile à évaluer : [Comment s'assurer de l'effectivité de l'intervention humaine ?](#)



Obligations de conformité au RGPD Cartographie des risques « données »

- Exigence de transparence et d'expression du consentement
- Droit à l'effacement
- Droit à la portabilité des données
- Sécurisation des données
- Conservation limitée dans le temps
- Tenue d'un registre des traitements
- ...

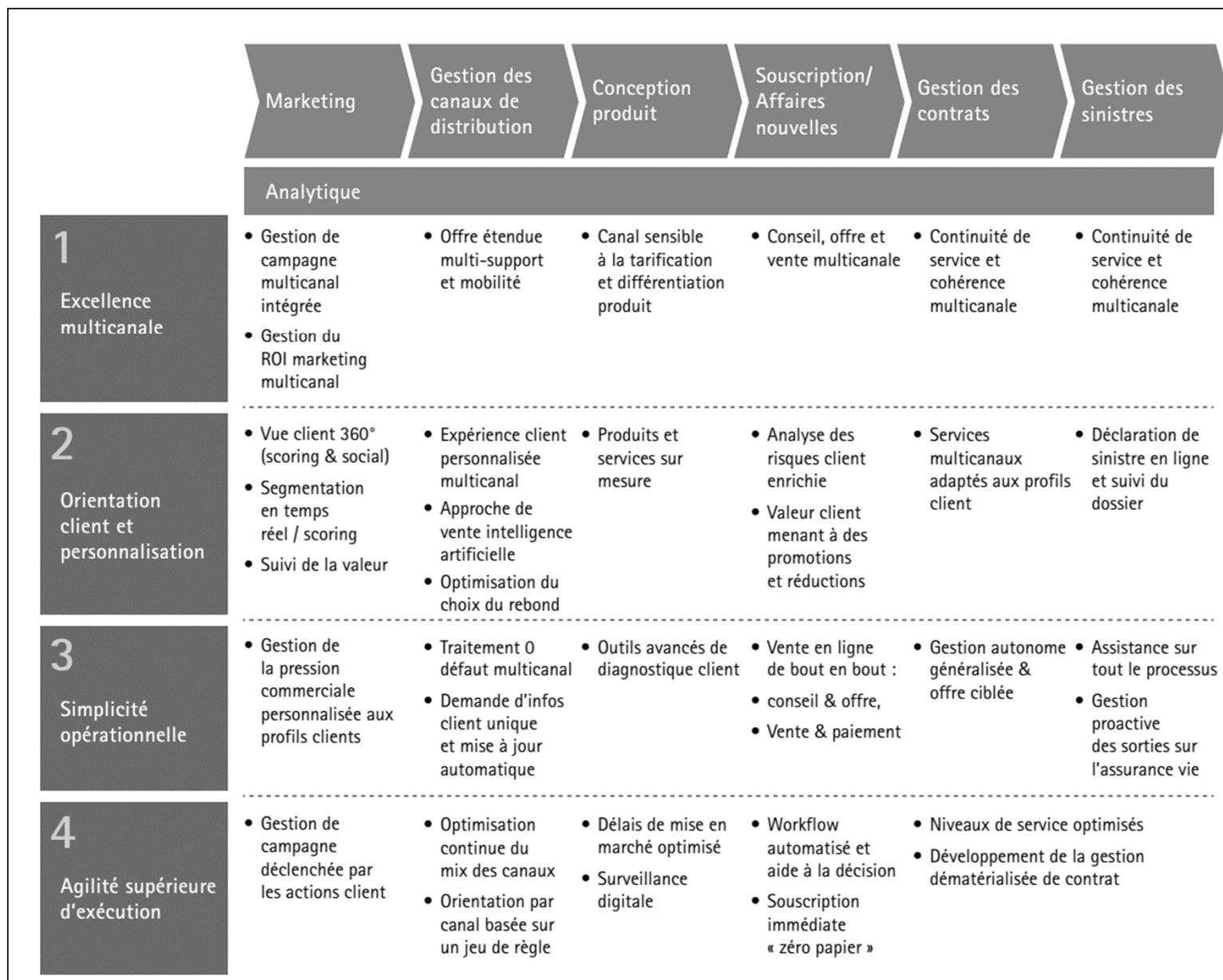
Qui peut être responsable en cas de dommages ?

La machine, les concepteurs de l'algorithme, ceux qui l'utilisent ...

- « quelles responsabilités pour les algorithmes », A. Charpentier, 2020 (<https://freakonometrics.hypotheses.org/59715>)
 - Un homme est fondamentalement responsable de ses actes
 - Il est censé comprendre que ses actions ont des causes et des conséquences (principe d'abstraction)
- Les algorithmes d'apprentissage « apprennent » par inductions, en cherchant des corrélations permettant d'améliorer la prévision
 - Processus itératif qui rend difficile la compréhension du cheminement (principe d'induction)
 - Ni volonté propre, ni de libre arbitre des algorithmes : maximisation d'une fonction dite « objectif »



Prendre en compte
les impacts sur les
emplois



Source : Accenture

15 ans de prospective sur les métiers dans l'assurance

- Baromètre des métiers 2007 : **Anticiper, attirer, retenir, fidéliser les nouveaux talents d'une part, valoriser les salariés en place**, gérer et promouvoir la mobilité en renforçant l'employabilité d'autre part, sont deux enjeux majeurs pour répondre aux défis de l'évolution de l'assurance, des métiers et de ses compétences » -
- L'Argus de l'assurance – Juin 2012 : **Crise économique, évolution technologique, papy-boom et nouvelles exigences réglementaires**, le secteur de l'Assurance vit plusieurs révolutions. Les métiers de l'Assurance sont en pleine mutation. Le secteur, hier ronronnant, affronte des révolutions aux conséquences majeures sur la manière dont sont pratiqués les métiers.
- L'Argus de l'assurance – Juin 2015 : **La transformation digitale redistribue les cartes dans le monde de l'assurance**. Elle amène avec elle de nouveaux leviers de croissance, change les manières de faire et redéfinit la relation assureur-assuré. Certains métiers et services profitent largement de cette redistribution.
- Baromètre des métiers 2017 - **Pour tous les salariés, c'est surtout une mutation qualitative qui s'annonce, avec une densification de la valeur ajoutée attendue de chaque emploi**. Dans toutes les familles de métiers, il devient plus difficile de bien faire son travail en se reposant sur des routines de l'activité. Si le digital était au cœur de l'actualité au cours de la période récente, l'introduction de nouvelles normes professionnelles vient nous rappeler la place centrale du réglementaire dans le secteur de l'assurance.

1^{ère} conséquence

Métiers dépassés

- Vagues de licenciements se multiplient alors même que les entreprises font face à un manque sur les métiers nécessaires à leur transformation digitale
- Consensus face aux profondes mutations
 - Les actifs doivent pouvoir accéder à une formation tout au long de leur vie
 - Créer la compétence manquante en interne coûte 3 à 6 fois moins cher que de recruter
 - Augmentation de la productivité : automatisation des tâches les plus répétitives
- Pour certains secteurs
 - Ce ne sont plus les compétences qui sont dépassées mais bien les métiers
 - Les emplois moyennement qualifiés se transforment au profit de travaux plus intellectuels, les emplois faiblement qualifiés sont peu à peu remplacés par des outils numériques plus économiques et plus performants
 - Fait écho à ce qui s'est passé au cours des précédentes révolutions industrielles : touche tous les métiers comportant des tâches répétitives

2^{ème} conséquence

Obsolescence des compétences

- Obsolescence : « insuffisance des savoirs ou compétences nécessaires à un travailleur pour continuer d'être parfaitement performant dans son activité professionnelle actuelle ou future ».
 - Là où il fallait une vie professionnelle pour voir ses compétences devenir obsolètes, le progrès technique accélère le phénomène
 - Près d'un quart des salariés européens (CEDEFOP)
 - Sentiment d'être dépassé et pas uniquement pour les seniors (*plus de 20% des 30-39 ans estiment que l'évolution technologique a rendu leurs compétences obsolètes ces deux dernières années contre 31% des 50-55 ans*)
 - Terrain des « *hards skills* » plus impacté par l'obsolescence
- Précipitation avec la Covid19 : « tout digital »

3^{ème} conséquence

Pénurie de compétences numériques

- Monde numérique : enjeu de compétitivité à long terme des entreprises, frein à l'innovation et à la transformation numérique
 - 80 000 emplois non pourvus en France (pole emploi)
 - 66% des entreprises cherchant à embaucher font face à une pénurie
- Secteur les plus touchés : cybersécurité - 3,5 millions de postes non pourvus dans le monde, en France, seules 25% des offres sont pourvues par manque de candidats ou de professionnels qualifiés
- Autre aspect :
 - certains métiers hyper qualifiés du secteur numérique arrivent plus rapidement à maturité et perdent rapidement leur valeur à cause d'un certain dumping social (intégration des nouvelles compétences plus rapide chez les plus jeunes / dans certains pays)

Merci de votre attention