FRANCE ASSUREURS
FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE

Livre blanc – résumé

Bâtir une économie de la donnée

innovante et protectrice en faveur des Français

21 avril 2022

Pourquoi un livre blanc, et pourquoi maintenant ?

La donnée est, depuis toujours, au cœur du métier d'assureur. Recueillir les informations est indispensable pour analyser les risques, les réduire grâce à la prévention et les couvrir, afin de protéger nos concitoyens et les entreprises de notre pays. En gérant les risques, les assureurs permettent aux Français d'en prendre, et donc à la société d'avancer.

Notre capacité à créer des données n'a jamais été aussi importante : en 2020, chaque individu a produit 1,7 Mo de données par seconde. Et 90 % des données disponibles sur Internet ont été créées au cours des deux dernières années. Pour les entreprises, l'explosion du nombre des données en circulation représente le moyen de proposer des services ultra personnalisés. Mais parce que leur valeur est de mieux en mieux reconnue, elles attirent aussi les cybercriminels.

Le site cybermalveillance.gouv.fr a vu en 2021 sa fréquentation doubler (+101%) par rapport à 2020, soit 2,5 millions de visiteurs, et 173 000 personnes y ont demandé assistance.

France Assureurs a placé la protection des données personnelles au cœur de ses réflexions. Pour le secteur de l'assurance, l'innovation et la transformation digitale sont des sujets clés à l'origine de nombreuses initiatives visant l'exemplarité.
Sans accès aux données, ni protection efficace de celles-ci, ces initiatives pourraient cependant demeurer vaines. C'est la raison pour laquelle France Assureurs appelle aujourd'hui à bâtir une économie de la donnée à la fois innovante et protectrice.

Si ce livre blanc a vocation à dresser un état des lieux, il vise aussi à formuler plusieurs propositions pour améliorer la protection contre les attaques cyber et construire un cadre d'exploitation des données numériques clair et sécurisé.

Le mouvement de digitalisation a accéléré notre entrée dans une nouvelle ère : l'économie de la donnée

Les données, nouveau carburant de l'économie

Le saut technologique du milieu des années 1990 a eu trois conséquences : l'explosion du nombre de données produites, leur exploitation massive par des entreprises devenues des géants technologiques et enfin l'essor de l'intelligence artificielle (IA).

Les informations telles que les habitudes de consommation ou les profils des clients ont commencé à devenir exploitables à une échelle industrielle. De nombreux entrepreneurs visionnaires ont perçu le potentiel de leur exploitation et se sont saisis de cette opportunité. Des géants technologiques, principalement américains, ont émergé et sont devenus en quelques années les plus grandes capitalisations boursières de la planète. L'augmentation de la puissance de calcul des ordinateurs et de la capacité de stockage informatique ont permis le développement de l'IA.
L'économie de la donnée entre alors dans un cycle vertueux : plus on génère de données, plus les intelligences artificielles se sophistiquent et plus elles permettent de déployer applications et services innovants, qui eux-mêmes génèrent des données pour nourrir les modèles d'apprentissage.

La protection des données est au cœur des priorités et des actions des assureurs

Le concept d'assurance repose sur la notion de risque. Les individus et les entreprises ont besoin, pour vivre sereinement et se développer, de se protéger contre certains risques.
Le métier de l'assureur consiste à protéger, de manière simultanée, un grand nombre d'individus ou d'entreprises, pour une durée déterminée, contre ces risques. Pour pouvoir offrir une telle protection, l'assureur a notamment besoin d'une compréhension et d'une connaissance fines du risque pour l'évaluer et donc de collecter des données.
Les données personnelles sont en effet au cœur des activités du secteur assurantiel, elles sont indispensables pour proposer des produits d'assurance adaptés.
L'utilisation de ces données en assurance est encadrée par une réglementation nationale et européenne :

1. la loi informatique et libertés du 6 janvier 1978 ;
2. le règlement général sur la protection des données (RGPD) ;
3. la directive ePrivacy.

Établir une relation de confiance avec l'assuré au sujet de l'utilisation qui est faite de ses données a toujours été une priorité de la profession.
C'est la raison pour laquelle l'assurance a été le premier secteur à mettre en place à ce sujet un « pack de conformité » assurance avec la Commission nationale informatique et libertés (Cnil) dès 2014.

La domination du *cloud* par des géants technologiques non européens

L'informatique en nuage, ou *cloud computing*, est une technologie puissante, qui permet de stocker et d'exploiter de grandes quantités de données de manière sécurisée.

Le *cloud* est de plus en plus massivement utilisé par les entreprises car ce mode d'hébergement et d'exploitation des données offre l'agilité nécessaire à l'accélération de la conception et de la distribution de produits et services innovants.

Toutefois, ce recours croissant aux infrastructures *cloud* pose la question de la concentration du marché des fournisseurs entre les mains de quelques acteurs – principalement américains – et de leur capacité à garantir la souveraineté des données.

Le gouvernement français a annoncé la mise en place d'un nouveau label, nommé « *cloud* de confiance » dont l'objectif est de sécuriser, à la fois techniquement et juridiquement, les services d'informatique en nuage utilisés par les entreprises françaises.

Les assureurs soutiennent cette stratégie nationale.

Le retard français en matière d'identité digitale

En tant qu'utilisateur de services numériques, chaque citoyen ou entreprise peut avoir besoin de prouver son identité sur Internet. De leur côté, les assureurs cherchent à développer une palette complète de services dématérialisés, simplifiant la vie de leurs clients. Cela peut nécessiter la vérification de leur identité digitale, plus sûre qu'un simple mot de passe.

Dans un contexte d'accroissement des risques cyber, le faible niveau de sécurité de nos identités digitales ouvre la voie à des accès frauduleux, au moyen par exemple d'usurpations d'identité.

C'est pourquoi les entreprises d'assurance attendent que la France se dote d'un ou plusieurs dispositifs d'identification numérique forte.

L'accroissement de notre exposition aux cybermenaces

Notre basculement progressif vers un monde de plus en plus digital a pour conséquence logique et inéluctable l'accroissement de notre exposition aux risques cyber.

L'attaque en réseau, autrement dit l'attaque simultanée par plusieurs centaines ou milliers d'objets connectés, pourrait même engendrer des réactions en chaîne potentiellement catastrophiques.

Ces attaques peuvent aussi prendre d'autres formes. L'une des plus courantes est le rançongiciel qui a représenté près de 80% des attaques cyber en 2020.

Cette modalité de piratage informatique est devenue très rentable car aucun texte national ou européen n'interdit le paiement d'une rançon par une entreprise ni l'assurabilité de ce genre de couverture, à l'exception des cas particuliers de financement du terrorisme et de blanchiment de capitaux. Dans le cadre de l'accompagnement par les assureurs, les solutions alternatives au paiement de la rançon sont toujours privilégiées lorsqu'elles existent.

Face à ces nouveaux risques, en perpétuelle évolution, les assureurs ont engagé des travaux de recherche et de formation afin de mieux quantifier le risque cyber pour mieux le prévenir et développer les contrats d'assurance incluant des garanties adéquates.

Tous ces travaux pointent systématiquement la nécessité d'améliorer la prévention, et tout particulièrement au niveau des petites et moyennes entreprises (TPE/PME). En effet, nombre d'entre elles n'ont pas suffisamment conscience de la dangerosité des cyberattaques, qui font peser des risques sur leur continuité opérationnelle, leur image et leurs finances.

La montée en puissance des véhicules connectés

D'ici à 2025, près de la moitié des véhicules en circulation en Europe seront des véhicules connectés. La connectivité des véhicules permet d'améliorer les services existants, de proposer un grand nombre d'innovations et permet aux assureurs de renforcer leurs offres en matière de prévention.

Il est important de garantir la maîtrise par chaque utilisateur de ses données et d'aider les professionnels à intégrer une dimension de protection pour éviter le risque de verrouillage des données par certaines entreprises.

La pénurie de compétences « tech »

Progressivement, le fossé se creuse, sur le marché de l'emploi mondial comme dans les organisations, entre les compétences disponibles et celles devenues incontournables.

En France, la pénurie de main-d'œuvre dans le numérique se traduit par une tension forte sur le marché de l'emploi. Cette tension ralentit le rythme de la transformation digitale des entreprises, qui peinent à recruter.

Les assureurs proposent des actions fortes en faveur de la protection des données

Les assureurs font plusieurs constats…

- les risques cyber constituent une menace grandissante pour notre économie ;
- la connectivité croissante des véhicules engendre des risques de verrouillage du marché ou de mise en place de mécanismes de péage sur les données de ces véhicules ;
- la pénurie de main-d'œuvre dans le numérique génère une tension forte sur le marché de l'emploi, notamment dans le secteur de l'assurance.

…et soumettent six propositions qui se structurent en trois axes :

- mieux protéger les citoyens et les entreprises contre les nouvelles menaces cyber ;
- favoriser l'innovation et la prévention en ouvrant l'accès aux données des véhicules connectés ;
- préparer les salariés aux métiers digitaux de l'assurance.

Axe 1 : nouvelles menaces cyber

Proposition 1

Inclure une sensibilisation cyber dans le parcours des jeunes élèves (primaire, collège, lycée) sous l'égide du ministère de l'Éducation Nationale, de la Jeunesse et des Sports, sur le modèle des actions de la Prévention routière.

Proposition 2

Clarifier la position de l'État français et de l'Union européenne concernant le cadre légal de l'indemnisation du paiement des rançons. Il semble qu'un chemin pourrait exister permettant de protéger sans inciter. Une amélioration du dispositif actuel, tant du côté des pouvoirs publics que du côté des assureurs, pourrait en effet permettre de sécuriser le cadre légal dans lequel la rançon peut être indemnisée en dernier ressort. Par exemple, une collaboration étroite entre assureurs et autorités judiciaire et policière pourrait être mise en place afin d'encadrer au mieux le paiement de rançons (information systématique d'une entité de la police judiciaire, du parquet de Paris, communication des adresses IP de paiement...).

Proposition 3

Développer une culture des risque cyber au sein des entreprises et des collectivités territoriales afin d'accélérer la résilience cyber de l'économie française et de permettre le développement des couvertures assurantielles.

Proposition 4

Amplifier les efforts de sensibilisation spécifiques auprès des TPE et PME

Les PME sont les principales cibles des cyberattaques et peuvent servir de porte d'entrée pour cibler les grands groupes dans le cadre de relations de sous-traitance. Par ailleurs, deux autres mesures permettraient de mieux protéger les entreprises contre les conséquences de la survenance d'une attaque cyber :

- l'élaboration d'un socle minimum de prévention/protection cyber ;
- le développement des prestataires informatiques labellisés.

Axe 2 : données des véhicules connectés

Proposition 5

Mettre en place au niveau européen un cadre qui garantisse le respect de deux principes clés :

- le libre choix de l'utilisateur de partager ou non les données de son véhicule connecté ;
- l'accès transparent et équitable pour tous les acteurs de la filière automobile en France.

Axe 3 : métiers digitaux de l'assurance

Proposition 6

Rendre éligibles à l'apprentissage les compléments de formation essentiels pour certaines compétences rares recherchées dans le cadre des activités numériques, en les finançant par une majoration du coût du contrat.

Dans un environnement de travail en perpétuelle évolution, **renforcer l'accompagnement des salariés**.