FRANCE ASSUREURS

FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE

Livre blanc

Bâtir une économie de la donnée

innovante et protectrice en faveur des Français

ÉLECTION PRÉSIDENTIELLE 2022

Bâtir une économie de la donnée innovante et protectrice en faveur des Français

Éditorial
de Florence Lustman

Florence Lustman
Présidente de France Assureurs

Engagés pour une économie de la donnée innovante et protectrice

Le mot exponentiel prend ici tout son sens. Près de 90 % des données existantes dans le monde ont été créées au cours des deux dernières années. Chaque jour, plus de 300 milliards de courriels sont échangés et 100 millions de photos et de vidéos sont partagées sur Instagram. Internet, les smartphones et les réseaux sociaux engendrent – ou donnent accès – à une somme considérable d'informations toujours plus fines et granulaires, qui, bien utilisées, permettent de déployer **des services innovants et personnalisés**.

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. C'est la raison pour laquelle les assureurs sont entrés de plain-pied dans cette économie de la donnée. Combiner données et nouvelles technologies leur ouvre la possibilité de **mieux prévenir les risques**, mais aussi **d'optimiser et de fluidifier les processus d'indemnisation de leurs assurés**.

Cette expertise leur confère également une responsabilité particulière. Car l'économie de la donnée a sa part d'ombre. Elle suscite d'ailleurs aujourd'hui de légitimes inquiétudes, relatives au respect de la vie privée, à la sécurité et à la souveraineté des données. Plus nos vies sont connectées, plus nous nous trouvons exposés à de nouvelles menaces, notamment celles des cyberattaques qui n'épargnent ni les particuliers ni les entreprises. Les Français s'en préoccupent à juste titre : 66 % considèrent être exposés de manière importante aux risques numériques[1].

Les assureurs sont donc en première ligne pour tirer le meilleur parti des promesses de cette économie de la donnée en misant **sur l'innovation technologique, tout en veillant à offrir à leurs clients un très haut niveau de protection de leurs informations**.

L'objet de ce livre blanc est de rappeler comment les entreprises d'assurance utilisent les données, **de manière proportionnée et responsable**, et dans quels buts. Il formule un certain nombre de propositions sur les enjeux technologiques, relatifs à la sécurité ou encore à la souveraineté de ces données, qui, au-delà des seuls assureurs, sont l'affaire de toutes et de tous.

1 — Étude *Les Français et les risques numériques*, Harris Interactive pour Assurance Prévention, décembre 2021.

Sommaire

Synthèse
du livre blanc

Une nouvelle ère s'ouvre à nous : l'économie de la donnée

Nos vies et notre activité économique se numérisent à grande vitesse : Internet, commerce en ligne, réseaux sociaux, smartphones et plus récemment télétravail nous ont fait entrer en seulement deux décennies dans l'économie de la donnée. Cette économie repose sur la capacité à déverrouiller des informations jusqu'alors particulièrement complexes à collecter et à analyser, et à les exploiter de façon industrielle. Parce que ces données transitent *via* de multiples réseaux de télécommunication, il est possible de les capter et de les mettre à profit, ce qui nourrit l'innovation et favorise l'émergence de nouveaux acteurs technologiques.

Ces flux massifs de données alimentent le développement de l'intelligence artificielle. Grâce à des réseaux de neurones artificiels, les machines peuvent imiter le raisonnement humain et apprendre. On parle alors de *deep learning*. Désormais, toute information, de la plus simple à la plus complexe, est susceptible d'être digitalisée, convertie en chiffres binaires (0 et 1) et exploitée par des microprocesseurs. Cette capacité à passer de données non structurées, verrouillées et donc inexploitables, à des données normées et structurées, est tout l'enjeu de l'économie de la donnée.

Un cycle vertueux peut alors s'enclencher : plus l'on créée de données, plus les intelligences artificielles se sophistiquent et plus elles permettent de déployer applications et services innovants, qui eux-mêmes alimentent des modèles d'apprentissage en nouvelles données. D'où l'importance pour les entreprises d'assurance de placer la protection des données personnelles au cœur de leurs priorités.

France Assureurs présente ses propositions pour bâtir une économie de la donnée innovante et protectrice

EXPLORER

France Assureurs réunit l'ensemble des entreprises d'assurance et de réassurance opérant en France, relevant du Code des assurances, soit 247 sociétés représentant plus de 99 % de ce marché.

Avec l'économie de la donnée surgissent cependant aussi de nouveaux risques qu'il faut prendre au sérieux : comment garantir la souveraineté et la protection de nos données lorsque les infrastructures *cloud*, qui se généralisent dans les entreprises comme au sein de l'État, sont quasiment toutes maîtrisées par des acteurs non européens ? Comment garantir la fiabilité et la robustesse de nos identités en ligne grâce à des identités dites « fortes » ? Comment s'armer face aux cybermenaces qui se multiplient ? Comment traiter la question de la propriété des données qui émerge des nouveaux usages, comme dans le cas de la voiture connectée ?

Et enfin, comment s'assurer que nos entreprises disposent des compétences indispensables face à ces défis ?

Autant de questions, cruciales pour l'avenir de notre pays, qui nous concernent tous, professionnels comme particuliers, secteur privé et secteur public, assureurs et assurés. Protéger, innover, former : la donnée est le fil conducteur de ce livre blanc et le dénominateur commun de plusieurs propositions, que France Assureurs souhaite porter dans le cadre de l'élection présidentielle 2022.

FABRIQUER

Les 6 propositions de France Assureurs

Mieux protéger les citoyens et les entreprises contre les 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.

PROPOSITION 3

Développer une culture du risque cyber (entreprises, collectivités locales…).

PROPOSITION 4

Amplifier les efforts de prévention des TPE et PME

Favoriser l'innovation et la prévention en ouvrant l'accès aux 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 ses données et l'accès transparent et équitable pour tous les acteurs.

Préparer les embauches de demain dans les métiers digitaux

PROPOSITION 6

Veiller à rendre éligibles à l'apprentissage les compléments de formation aux compétences devenues stratégiques pour la transformation des modèles de développement.

Introduction

Un livre blanc pour une économie de la donnée innovante et protectrice

En 2007, il s'échangeait quelque 2 téraoctets de données chaque seconde[1] sur Internet. Douze ans plus tard, ce chiffre était passé à 77 téraoctets par seconde . Pour les entreprises, Gafa en tête, l'explosion du nombre de ces 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. Tentatives de phishing, piratages, rançongiciels… En 2020, plus de 100 000 personnes sont venues demander assistance sur la plateforme gouvernementale cybermalveillance.gouv.

Dès son origine, **France Assureurs a placé la protection des données et le renforcement de la confiance de l'assuré dans l'utilisation des données personnelles** au cœur de ses réflexions, à travers la création de différentes instances (commission numérique, groupes de travail autour de la protection des données, du cyber, des véhicules connectés…), en vue de mettre en place des dialogues constructifs avec les différentes parties prenantes, aussi bien sur le plan national qu'européen.

Ces instances ont identifié les grands enjeux de ce qu'il est désormais convenu de nommer l'économie de la donnée. La domination du *cloud* par des acteurs extra-européens menace notre souveraineté. Le retard français en matière de vérification de l'identité digitale ouvre la porte aux fraudes, tandis que l'exposition des entreprises aux cybermenaces augmente. Le développement de la voiture connectée entraîne le risque d'un verrouillage des données par un petit nombre d'acteurs. Et, au sein des entreprises et des collectivités ainsi que sur le marché du travail, les compétences « tech » viennent à manquer.

Pour le secteur de l'assurance, l'innovation et la transformation digitale sont des sujets clés. **Les assureurs ont toujours visé l'exemplarité en matière de protection des données**. Ils ont travaillé en étroite collaboration avec le régulateur pour définir et mettre en œuvre des bonnes pratiques, avant même que celles-ci ne deviennent des obligations légales. **L'assurance a ainsi été le premier secteur à mettre en place un pack de conformité assurance avec la Cnil, dès 2014**. Afin de tenir compte des obligations prévues par le règlement général sur la protection des données (RGPD), entré en vigueur en mai 2018, ce pack a été actualisé en collaboration avec la Cnil et a fait l'objet d'une publication au début de l'année 2021.

Sans accès aux données, ni protection efficace de celles-ci, toutes les 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, dans un contexte de transformation digitale s'accélérant sans cesse, il vise aussi, dans le contexte de la campagne présidentielle de 2022, à formuler **plusieurs propositions : mieux protéger les citoyens et les entreprises contre les menaces cyber**, grâce à la sensibilisation des jeunes élèves et au développement de la culture cyber au sein des entreprises et des collectivités locales ; clarifier la position de l'État sur la légalité de l'assurabilité du remboursement des rançons ; **garantir un accès aux données des véhicules connectés**, transparent et équitable pour toutes les parties prenantes ; **mieux préparer les embauches de demain pour les métiers digitaux de l'assurance**.

1 — Société Générale, *Cyber Risk*, 2019.

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

Les données, nouveau carburant de l'économie

Après l'ère du charbon au XIXe et du pétrole au XXe siècle, notre civilisation est entrée depuis le début du XXIe siècle dans l'économie de la donnée.

Cette nouvelle ère a débuté avec la démocratisation d'Internet, au milieu des années 1990. Ce saut technologique a entraîné le passage du format papier au format digital, de la lettre au courrier électronique, de la boutique « *brique et mortier* » au commerce en ligne. Les réseaux de télécommunication et les médias ont commencé à converger. Avec 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.

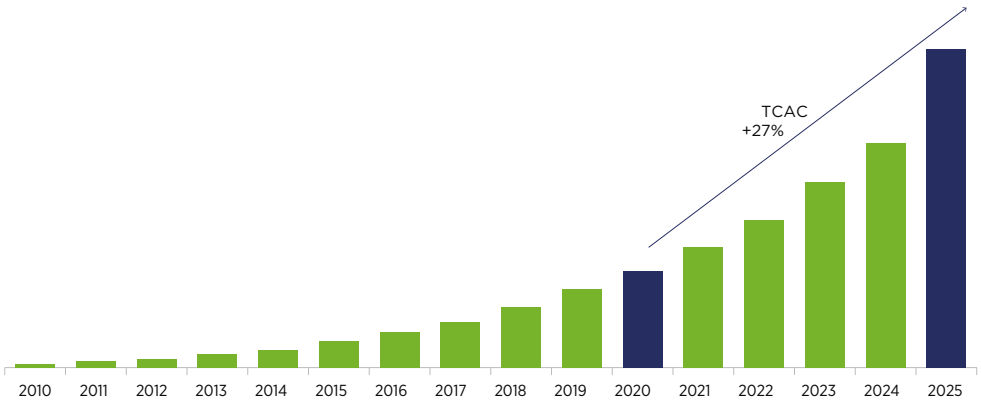
La première conséquence réside dans le fait que des informations telles que les habitudes de consommation ou les profils des clients, qui étaient jusqu'alors complexes à collecter et à analyser, ont commencé à devenir exploitables à une échelle industrielle. Et ce mouvement n'a fait que prendre de l'ampleur au cours des deux dernières décennies. À partir du milieu des années 2000, on a assisté aux premières grandes « disruptions » digitales. En 2007, l'explosion des smartphones dans le sillage de l'iPhone d'Apple a abouti à mettre un terminal dans la poche de très nombreux citoyens. Musique en ligne, échanges par messageries et réseaux sociaux : notre capacité à créer des données n'a jamais été aussi importante. En 2020, chaque individu a ainsi produit 1,7 Mo de données par seconde. Chaque jour, 95 millions de photos et de vidéos sont partagées sur Instagram. Tout va toujours plus vite : 90 % des données disponibles sur Internet ont été créées au cours des deux dernières années [1].

DÉCODER

L'accroissement exponentiel de la production de données

Avec la numérisation et l'utilisation des réseaux sociaux et des smartphones, le monde produit de plus en plus de données avec une multiplication par 25 en une décennie et un triplement à venir au cours des cinq prochaines années.

INFORMATION DIGITALE GLOBALE CRÉÉE PAR AN



TCAC : taux de croissance annuel composé.

1 — Information overload research group (Iorg).

Dès lors que ces informations transitent sur des réseaux, elles peuvent être captées et utilisées. De nombreux entrepreneurs visionnaires ont perçu le potentiel de leur exploitation et se sont saisis de cette opportunité.

La deuxième conséquence de la digitalisation a donc été l'émergence de géants technologiques, principalement américains, devenus en quelques années les plus grandes capitalisations boursières de la planète, supplantant groupes pétroliers, chimiques ou industriels. Ces géants technologiques ont pour caractéristique commune d'être les plus grands collecteurs et analystes de données, à une échelle inédite dans l'histoire de l'humanité.

La troisième conséquence de la digitalisation a été le grand réveil de l'intelligence artificielle. Avec l'augmentation de la puissance de calcul des ordinateurs et de la capacité de stockage informatique (développement du *cloud computing*), les chercheurs ont pu faire sortir l'intelligence artificielle du long « sommeil » dans lequel elle était plongée depuis les années 1970. Ils ont pu tirer parti de la capacité des machines à imiter le raisonnement humain en tissant des connexions entre des millions d'informations différentes, à travers un réseau de neurones artificiels. Cette capacité d'apprentissage automatique se nomme *deep learning*.

Désormais, toute information, de la plus simple à la plus complexe, est susceptible d'être digitalisée, convertie en chiffres binaires (0 et 1) qu'un ordinateur peut analyser et exploiter. Bardés de capteurs reliés à un ordinateur de bord capable d'intelligence artificielle, les véhicules autonomes roulent ainsi déjà à titre expérimental. Il devient également possible pour une machine de comprendre et d'interpréter le langage humain, voire de mener une conversation en répondant à certaines questions basiques, formulées en langage naturel.

C'est cette capacité relativement récente dans l'histoire à normer et organiser une myriade d'informations à l'aide de microprocesseurs qui est au cœur de l'économie de la donnée. Dès qu'il devient possible d'alimenter une intelligence artificielle avec ce nouveau carburant, un processus d'apprentissage peut être mis en route. Elle va alors progressivement se doter de capacités cognitives : raisonnement, déduction, résolution de problèmes, émission de recommandations ou prises de décisions.

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 besoin entre autres prérequis :

- d'une multiplicité d'assurés pour mutualiser les risques. L'assurance fonctionne de manière efficace quand un petit nombre de sinistres, sur une période donnée, sont financés par la masse des cotisations d'un grand nombre d'assurés à qui il n'est rien arrivé ;

- d'une compréhension et d'une connaissance fines du risque pour l'évaluer. L'assureur a besoin de connaître et comprendre la nature du risque qu'il couvre et de le comparer à des tendances passées. Ce travail d'actuariat

aboutit à la tarification du risque et donc au calcul de la cotisation d'assurance. Il s'agit en définitive de répondre à une question : quel niveau de cotisation doit-on demander à un nombre déterminé d'assurés, pour une période donnée, afin de s'engager à couvrir un nombre de sinistres susceptibles de survenir durant cette période ?

Cette collecte de données obéit à des règles strictes, établies au niveau européen et français, à commencer par celles du règlement général sur la protection des données (RGPD), et répond à des finalités très précises.

EXPLORER

Assurance et données : la position de la Commission nationale informatique et libertés (Cnil)

« Les données traitées dans le cadre d'un contrat d'assurance doivent être pertinentes et nécessaires au regard de l'objectif de celui-ci. […] Le traitement de données de santé est possible lorsque que celui-ci 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 à la protection sociale. Dès lors, les organismes d'assurance pourront se prévaloir de cette exception pour les contrats relevant de ce périmètre (exemple : contrats de complémentaire santé, contrats de prévoyance, retraite supplémentaire). »

Source > Cnil, « Les grands traitements du secteur de l'assurance et leurs bases légales », 16 juillet 2021.

DÉCODER

Assurance et protection des données de santé

Les assureurs n'utilisent que les données strictement nécessaires pour la conclusion et l'exécution du contrat, conformément à la règlementation.

Qu'est-ce qu'une donnée de santé ?

Selon l'article 4 du RGPD, il s'agit des données personnelles concernant la **santé physique ou mentale des personnes physiques** y compris la **prestation de services de soins de santé** qui révèlent des informations sur l'état de santé.

Quelles utilisations ?

Les données de santé font lobjet de traitements lorsqu'elles sont **nécessaires à la souscription, la gestion et l'exécution d'un contrat d'assurance**.

Exemple 1 : Complémentaire santé

Dans le cadre d'une demande de remboursement, l'assureur traite des documents sur lesquels figurent des données de santé, comme par exemple :

- le numéro de la catégorie d'acte médical réalisé,
- le décompte de la sécurité sociale.

Exemple 2 : Assurance corporelle IARD*

Dans le cadre de l'évaluation des préjudices corporels et de l'indemnisation, les assureurs ont besoin de collecter des informations, comme par exemple :

- les conclusions d'une expertise médicale,
- des certificats médicaux.

*IARD : incendies, accidents et risques

Des utilisations interdites

L'utilisation des résultats des tests génétiques est formellement interdite aux assureurs à la fois par le Code pénal, le Code des assurances et le Code de la Santé publique.

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.
Les « packs » définissent les bonnes pratiques pour un secteur en matière de traitement de la donnée. Ils représentent, pour la Cnil, un mode de régulation. Le pack de l'assurance a été complété en 2021 par un guide d'actualisation, rédigé par France Assureurs, la Fédération Nationale de la Mutualité Française (FNMF), Planète CSCA et le Centre Technique des Institutions de Prévoyance (CTIP), toujours en collaboration avec la Cnil.

Ce guide d'actualisation présente :

- **les différentes qualifications des acteurs du secteur de l'assurance** dans le cadre du traitement des données personnelles. Il s'agit de savoir qui détermine les finalités et les moyens mis en œuvre pour ce traitement, dans un grand nombre de modèles d'organisation différents ;

- **les bases légales de traitement en fonction des finalités** (que sont d'une part la passation, gestion et exécution du contrat et d'autre part, les opérations de prospection commerciale). Ainsi, par exemple, le traitement des données à caractère personnel strictement nécessaires est légitime pour le responsable concerné lorsque celui-ci vise à prévenir des fraudes. Le traitement de la lutte contre la fraude est ainsi indissociable de la gestion et de l'exécution des contrats ;

- **les types de données personnelles traitées en fonction de la finalité retenue**. Pour rappel, il est interdit de traiter des données sensibles (dont les données de santé) sauf cas prévus par l'article 9 du RGPD[1] ;

- **les cas d'utilisation du numéro de sécurité sociale (NIR) selon le décret du 19 avril 2019**. Le NIR peut en effet être utilisé par les Organismes d'assurance dans les conditions prévues par le décret du 19 avril 2019 ;

- **le traitement des données relatives à la santé**. Les données médicales sont couvertes par le secret professionnel et le traitement des données génétiques par les responsables de traitement, ou pour leur compte, est interdit à la fois par le Code de la santé publique (article L. 1141-1), par les trois Codes assurantiels (article L. 133-1 du Code des assurances, article L. 932-39 du Code de la Sécurité sociale et article L. 110-6 du Code de la mutualité) et par le Code pénal (Article 225-3) ;

- **les droits des personnes concernées** prévus par le chapitre III du RGPD (droit d'accès, de rectification, d'opposition…) ;

- **les destinataires**. On distingue des destinataires communs à tous les traitements et des destinataires spécifiques dans le cadre de certains traitements de données ;

- **les durées de conservation**. Les données personnelles doivent être conservées pour la seule durée nécessaire au traitement visé par le responsable. Ces durées diffèrent en fonction de la conclusion ou non d'un contrat d'assurance ;

- **les mesures de sécurité**. Le responsable de traitement prend toutes précautions utiles, notamment techniques et organisationnelles, pour préserver la sécurité, l'intégrité, la disponibilité et la confidentialité des données traitées. Une fois encore, les données médicales bénéficient de mesures de sécurité spécifiques ;

1 — Ainsi l'article 9 point b) du paragraphe 2 du RGPD peut s'appliquer aux organismes d'assurance 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 de la protection sociale. Également, l'article 9 point a) du paragraphe 2 indique que le consentement peut être utilisé dès lors que le traitement des données de santé est « nécessaire à l'exécution d'un contrat, y compris la fourniture d'un service, si cette exécution est subordonnée au consentement explicite ».

EXPLORER

La protection des données personnelles en assurance

Les données personnelles sont 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 de protection des données (RGPD)

3. la directive ePrivacy

Seules les données **strictement nécessaires** sont connectées dans un **but précis et légitime**.

Les données sont conservées pour une **durée déterminée**.

Les assurés disposent d'un **droit d'accès, de rectification, d'opposition**.

Les assureurs mettent en œuvre les **mesures de sécurité et de confidentialité appropriées**.

DÉCODER

Renforcer la confiance autour de l'utilisation des données personnelles par les assureurs

Vous connaître

Vos données sont indispensables pour bien vous assurer. Nous ne collectons et conservons que les données nécessaires pour vous proposer des produits et services adaptés, vous indemniser au mieux, et mener des actions de prévention ciblées et efficaces.

Vous faciliter l'exercice de vos droits

Vos données sont protégées par la loi. Nous nous engageons à ce que vous puissiez à tout moment et par tout moyen y accéder, vous opposer, rectifier ou faire supprimer vos données personnelles.

Vous rassurer

Vos données sont précieuses : nous mettons tout en œuvre pour garantir leur sécurité et leur intégrité.

Vous informer

Vos données sont personnelles. C'est à vous de choisir à qui vous les communiquez. Quand vous nous confiez vos données, nous vous informons de leur utilisation et à qui elles sont transmises. Et nous vous expliquons à quelles fins et combien de temps nous devons les conserver.

Vous accompagner

Les données sont partout, les technologies avancent vite, il est parfois difficile de s'y retrouver.

Parce que les évolutions numériques doivent profiter à chacun d'entre vous, nous vous accompagnons à chaque étape, dans toutes vos démarches, pour vous faciliter l'assurance au quotidien.

Pour consulter ce document, rendez-vous sur franceassureurs.fr, rubrique « L'assurance protège » / « L'assurance en pratique pour les particuliers » / « L'assurance et vos données personnelles ».

Source > Extrait du guide France Assureurs « Bien vous connaître, c'est bien vous assurer », 2017.

Les grands enjeux de l'économie de la donnée pour la société française et les assureurs

Les données sont au cœur de nos vies : elles méritent d'être protégées à tout prix contre les risques cyber, les risques d'usurpation d'identité digitale ou les risques liés à la souveraineté des données dans le *cloud*... Il est pour cela essentiel de garantir que tous les acteurs respectent les mêmes règles du jeu et que les citoyens comme les entreprises, puissent être informés et formés sur ces enjeux.

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.

Grâce à lui, plusieurs assureurs envisagent par exemple de déployer des capteurs connectés (détecteurs de fumée, détecteurs de fuites d'eau...) pour prévenir les sinistres les plus fréquents. Les données de ces capteurs remonteraient dans le *cloud* pour y être analysées et comparées avec d'autres sources d'information. Le déclenchement d'une intervention deviendrait alors possible à la moindre anomalie, avant qu'elle ne se transforme en sinistre important, en prévenant l'assuré sur son smartphone, voire en coupant directement l'eau ou l'électricité.

Le recours au *cloud* s'est notamment révélé indispensable durant les épisodes de confinements successifs de 2020 et 2021. Il a permis la continuité des opérations de nombreuses entreprises dont les collaborateurs ont vu leur activité intégralement basculée en télétravail quasiment du jour au lendemain.

L'utilisation du *cloud* par les entreprises a donc vocation à croître fortement dans les années à venir.

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.

Ainsi, lorsque les assureurs souhaitent travailler avec des prestataires de *cloud* américains par exemple, ils doivent consacrer énormément de temps et de ressources à définir, par voie contractuelle, l'ensemble des garanties nécessaires demandées à leurs fournisseurs.

Conscient de ces difficultés, le gouvernement français a annoncé le 17 mai 2021, lors de la présentation de la stratégie nationale pour le *cloud*, 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. « La constitution d'une offre de *cloud* de confiance à l'échelle européenne représente un enjeu majeur. Ce partenariat montre que La France, comme d'autres pays européens, est en mesure d'imposer des conditions strictes aux géants du numérique, conformément à la doctrine *cloud* du Gouvernement. », a déclaré Bruno Le Maire, ministre de l'Économie, des Finances et de la Relance, le 6 octobre 2021. Cédric O, secrétaire d'État chargé de la Transition numérique et des Communications électroniques a, quant à lui, déclaré le lendemain : « notre objectif est de faire émerger des champions européens du *cloud* ».

Les assureurs soutiennent la stratégie nationale et la création du label « *cloud* de confiance », qui offrira les conditions de confiance nécessaires au développement des services dans le *cloud,* et souhaitent que les pouvoirs publics encouragent le lancement d'offres de *cloud* souveraines, au niveau français et européen.

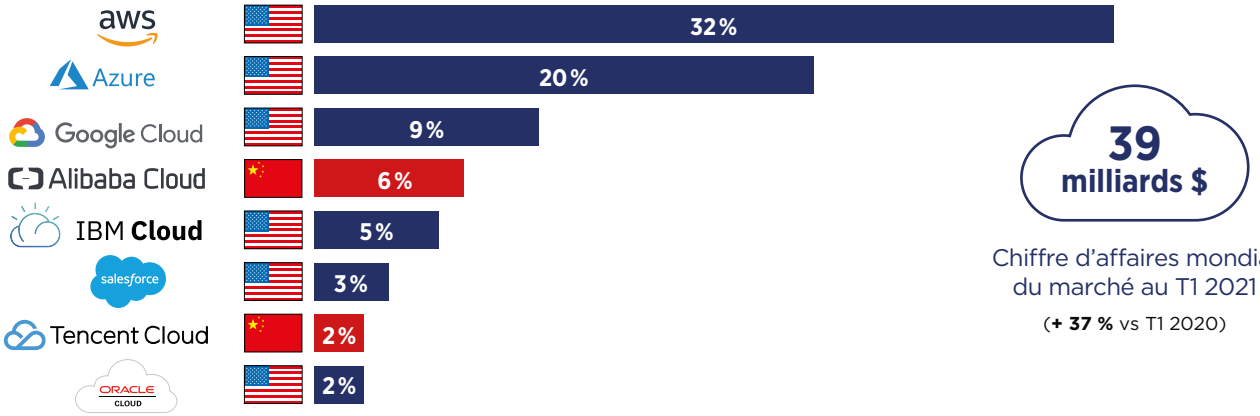
EXPLORER

Le marché mondial du *cloud*

Amazon a été pionnier sur le marché du *cloud* en proposant de mettre à disposition une partie de ses infrastructures à travers sa filiale Amazon Web Services. Très vite, les autres géants technologiques américains (Microsoft avec Azure et Google avec Google *cloud*) lui ont emboîté le pas. Le marché du *cloud* est aujourd'hui dominé par une poignée d'acteurs américains et chinois. Cette domination est encore plus marquée en Europe, puisque selon une étude de la société de conseil américaine Oliver Wyman[1], **92% des données numériques des pays européens sont hébergées aux États-Unis**.

CLOUD : LES GÉANTS SE PARTAGENT LE MARCHÉ

Part du marché mondial des principaux fournisseurs de services de cloud d'infrastructure (1er trimestre 2021)*



* Inclut les modèles "Plateforme en tant que service (PaaS)" et "Infrastructure en tant que service (IaaS)", ainsi que les services de *cloud* hébergé.

Source > Synergy Research Group.

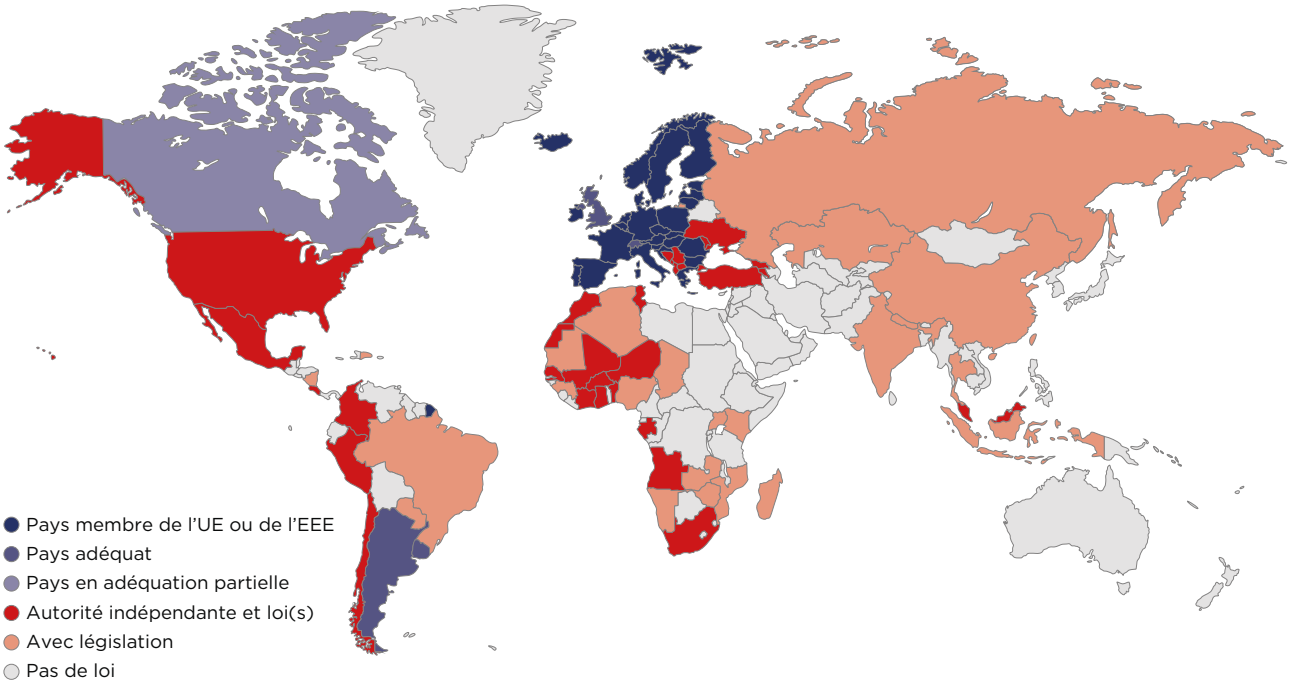
1 — *European digital sovereignity*, octobre 2020

DÉCODER

Les transferts ou hébergement de données selon les pays

Un petit nombre de pays dits « adéquats » offrent des niveaux de protection des données personnelles au moins équivalents à ceux de l'Union européenne. Le transfert ou l'hébergement de données chez eux ne pose donc pas de problème spécifique.

Avec les pays situés en dehors de l'Union européenne ou de l'espace économique européen, et non « adéquats » – le niveau de protection des données personnelles étant jugé insuffisant ou partiel –, une vigilance particulière s'impose. Il faut, par exemple, négocier des clauses spécifiques avec les fournisseurs de *cloud*. Cela s'avère le plus souvent complexe et coûteux.



Source > CNIL – 23/11/2020 : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde.

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) soit au moment de l'entrée en relation soit au cours de la réalisation de certaines opérations.

En France, chaque citoyen bénéficie d'un dispositif d'identification avec France Connect pour effectuer ses démarches administratives, avec deux niveaux :

- France Connect, la version de base utilisée par près de 35 millions de Français, très simple d'utilisation mais qui n'est pas une solution d'identité numérique forte ;

- France Connect+, une version d'identité numérique forte, proposée en conjonction avec l'Identité Numérique de la Poste et nécessitant une procédure de vérification en bureau de Poste ou *via* son facteur.

France Connect+ permet, en plus de la connexion à ses services administratifs habituels, d'effectuer des démarches plus complexes, sans avoir à transférer de pièce d'identité.

DÉCODER

Qu'est-ce que l'identité numérique forte ?

On parle d'identité numérique forte lorsqu'au moins deux des trois facteurs d'authentification suivants sont utilisés :

- quelque chose que l'on possède : téléphone portable, jeton d'authentification ;

- quelque chose que l'on connaît : mot de passe, code PIN ;

- quelque chose que l'on est ou que l'on fait : authentification biométrique *via* le visage ou les empreintes digitales...

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, comme un grand nombre d'autres acteurs économiques, les entreprises d'assurance attendent que la France se dote d'un ou plusieurs dispositifs d'identité numérique forte.

Plusieurs voies semblent envisageables, entre autres :

- soit l'État encourage le déploiement du dispositif France Connect+ en conjonction avec l'Identité Numérique de la Poste ;
- soit l'État diffuse un outil d'identification utilisable par chaque consommateur : une carte d'identité électronique, comme c'est le cas au Danemark, en Belgique ou en Estonie ;
- soit certains dispositifs d'identification mis à la disposition des consommateurs deviennent interopérables, comme les cartes de paiement et de retrait d'espèces, afin qu'ils puissent être utilisés par l'ensemble des professionnels, comme c'est le cas en Norvège.

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.

Pendant plusieurs décennies, après l'émergence des premiers ordinateurs personnels, les risques cyber étaient naturellement contenus par l'absence de mise en réseau massive. L'arrivée d'Internet, puis des réseaux sociaux, des smartphones, des objets et véhicules connectés a considérablement changé la donne. Tout objet doté d'un cœur numérique, c'est-à-dire d'une puce et d'une connectivité (3G, 4G ou 5G, Wifi, Bluetooth, NFC, IoT…) est désormais susceptible de faire l'objet d'une attaque cyber.

L'attaque de réseaux, ou l'attaque simultanée de plusieurs centaines ou milliers d'objets connectés (comme des feux de circulation, par exemple), pourrait même engendrer des réactions en chaîne potentiellement catastrophiques.

Face à ces nouveaux risques, en perpétuelle évolution et difficilement maîtrisables, les assureurs ont engagé des travaux de recherche, de formation, de quantification et de prévention du risque cyber afin de développer les contrats d'assurance incluant des garanties adéquates.

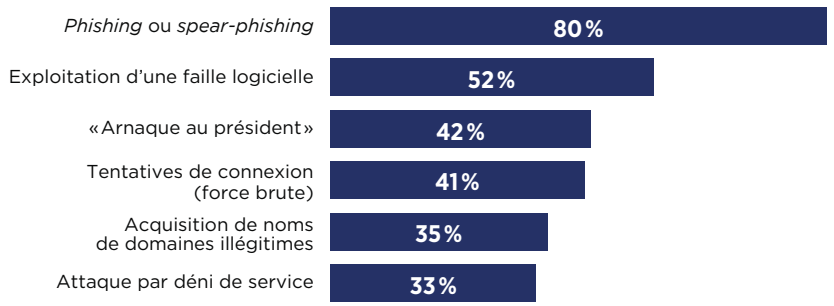
> **« Seul un quart des dirigeants de TPE/PME françaises estiment que leur entreprise est concernée par le risque de subir une attaque cyber »**

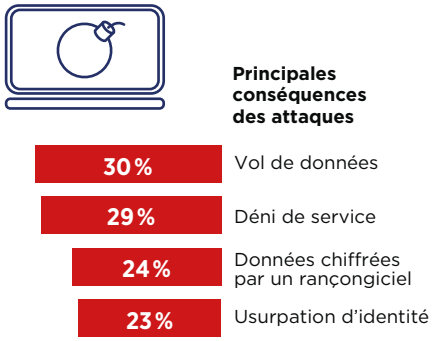
Tous ces travaux pointent systématiquement la nécessité d'améliorer la prévention, et tout particulièrement au niveau des petites et moyennes entreprises (TPE/PME). En effet, nombre d'entre elles n'ont pas suffisamment conscience de la dangerosité des cyberattaques, qui font peser des risques sur leur continuité opérationnelle, leur image et leurs finances. Seul un quart des dirigeants de TPE/PME françaises estiment que leur entreprise est concernée par le risque de subir une attaque cyber[1].

EXPLORER

Les entreprises face aux cyberattaques

TYPES D'ATTAQUES LES PLUS COURANTS CONSTATÉS PAR LES ENTREPRISES EN 2020*





* Plusieurs réponses possibles, sélection des plus fréquentes.
Les entreprises ciblées ayant répondu à l'enquête ont subi en moyenne **3,6 attaques et 2,3 conséquences.**

Source > Cesin, OpinonWay, Statista.

1 — Enquête *Les TPE / PME et la cybersécurité*, Ifop, 2021.

Parmi les risques cyber, ces dernières années ont vu le développement d'une forme d'attaque particulièrement grave pour les entreprises : le « rançongiciel », contraction de « rançon » et de « logiciel ». Celui-ci infecte un système informatique à l'aide d'un virus qui va rendre les données inaccessibles et appuyer la demande de paiement d'une rançon. Certaines attaques combinent ce cryptage avec un chantage à la fuite de données vers l'extérieur, afin d'exercer une pression additionnelle sur l'entreprise. Cette forme de piratage informatique est devenue tellement rentable qu'elle pourrait éclipser d'autres modes opératoires plus complexes (« arnaque au président », phishing…). On trouve désormais sur le Dark Web des développeurs proposant des logiciels de rançons à louer à des groupes mafieux ne disposant pas des compétences techniques. Le phénomène « rançongiciel » a représenté près de 80 % des attaques cyber en 2020[1].

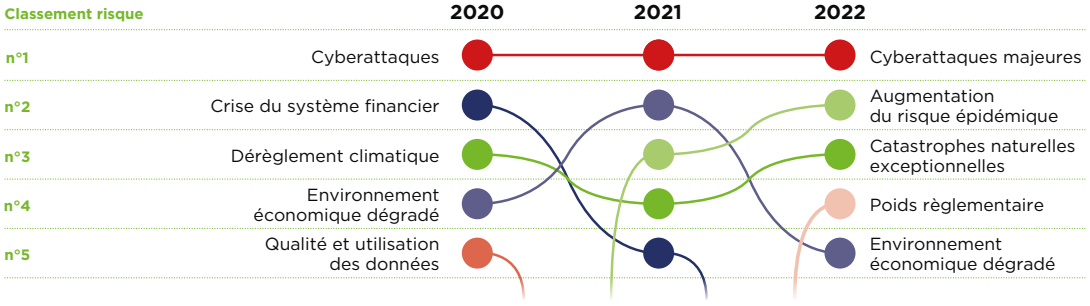
Les cyberattaques létales sont des cyberattaques de grande ampleur avec mise à l'arrêt du système d'information de l'entreprise (rançongiciel avec blocage du système d'informations ou menace de publication de données, attaque par déni de service capable de submerger un serveur pour le rendre inopérant…). Les conséquences sont d'ordre économique – au niveau de l'individu, de la société comme du pays – et géopolitiques.

Aucun texte national ou européen n'interdit le paiement d'une rançon par une entreprise ni le remboursement des rançons par un assureur, à l'exception des cas particuliers de financement du terrorisme et de blanchiment de capitaux.

DÉCODER

Les risques cyber dans la cartographie prospective de l'assurance

Les directions des risques des assureurs et réassureurs français sont sondées chaque année pour établir une cartographie des risques. En 2022 comme en 2020 et 2021, ce sont les risques cyber qui s'installent en tête du classement.



Source > France Assureurs, *Cartographie prospective 2022 de l'assurance*, janvier 2022

Pour consulter ce document, rendez-vous sur franceassureurs.fr, rubrique « Nos positions » / « L'assurance protège ».

Dès lors, certains assurés ont pu faire le choix de souscrire une garantie couvrant le remboursement de la rançon en cas de cyberattaque afin d'éviter un blocage complet de leur système d'information. L'objectif premier est de couvrir les pertes pécuniaires. Pour un entrepreneur dont l'outil de travail est totalement bloqué, et en l'absence de sauvegardes fiables, il n'y a parfois pas d'autres choix. Les assureurs sont là pour les accompagner dans ces situations souvent dramatiques. Mais ces situations exposent à des dilemmes. Pour un directeur de clinique ou d'hôpital, par exemple, que faire si la survie de patients est

1 — Sophos 2022 Threat Report.

mise en cause en raison d'un cryptage de données ? Payer ou bien mettre en danger la vie de ses patients ? Sachant que le paiement n'offre jamais la garantie que le système sera débloqué.

Dans le cadre de l'accompagnement par les assureurs, les solutions alternatives au paiement de la rançon sont toujours privilégiées lorsqu'elles existent. En Europe, l'assurance cyber demeure encore peu répandue. Par ailleurs, tous les contrats cyber ne contiennent pas une garantie couvrant l'assuré contre le risque de rançongiciel.

« 47 % des Français disent être mal informés sur les risques numériques et 51 % méconnaissent les mesures permettant de limiter ces risques »

Les particuliers sont aussi susceptibles d'être visés par des cybermenaces, a fortiori dans le contexte du télétravail, qui brouille les frontières entre ressources informatiques privées et professionnelles. Or, 47 % des Français disent être mal informés sur les risques numériques et 51 % méconnaissent les mesures permettant de limiter ces risques[1].

Le site www.cybermalveillance.gouv.fr propose un kit de sensibilisation, élaboré en collaboration avec France Assureurs, aux 4 risques numériques majeurs auxquels sont exposés les utilisateurs :

- l'hameçonnage (*phishing*) ;
- la gestion des mots de passe ;
- l'utilisation des appareils mobiles (téléphones et tablettes) ;
- la sécurité des usages professionnels et personnels.

Il met également à disposition des particuliers des diagnostics en ligne, donne des conseils et des solutions. Le site facilite également le dépôt de plainte après une cybermalveillance.

Le site www.cybermalveillance.gouv.fr est piloté par le Groupement d'intérêt public (GIP) Action contre la cybermalveillance (Acyma) dont France Assureurs est membre fondateur et auquel de nombreux assureurs participent.

La montée en puissance des véhicules connectés et le risque d'un verrouillage des données

La connectivité des véhicules ouvre un champ extrêmement étendu de création de services digitaux innovants et de nouvelles solutions pour le grand public. Ces nouveaux services favoriseront une conduite apaisée et contribueront à améliorer le confort et la vie des conducteurs et des passagers. Certains auront une portée plus large, en participant notamment à la sécurité routière, à l'optimisation des infrastructures, à la transition écologique et à la conversion du parc à l'électrique.

La connectivité des véhicules est en train de donner naissance à un écosystème complet permettant aux constructeurs, mais aussi à la filière automobile dite « aval » (assureurs, réparateurs, experts, loueurs, fournisseurs d'électricité…), d'améliorer leurs services existants et de proposer un grand nombre d'innovations.

Avec des véhicules connectés à Internet, il devient ainsi possible pour les assureurs de renforcer leurs offres en matière de prévention : services d'alertes trafic géolocalisées et en temps réel (météo, accidents…), dispositifs d'amélioration du comportement de conduite ou de formation intuitive à l'écoconduite, maintenance prédictive (faire remplacer une pièce avant la survenance d'une panne).

1 — Étude *Les Français et les risques numériques*, Harris Interactive pour Assurance Prévention, décembre 2021.

Afin que l'ensemble des acteurs puissent développer ces nouveaux services dans des conditions techniques et économiques équitables, il est indispensable de veiller au respect de principes clés :

- le libre choix de l'utilisateur ou du propriétaire du véhicule de partager ou non ses données ;
- l'accès transparent et équitable pour tous les acteurs de la mobilité connectée.

« C'est à l'utilisateur ou au propriétaire du véhicule de décider avec qui et pour quels usages il souhaite partager ses données »

Rappelons en effet que les données automobiles sont principalement des données personnelles. C'est donc à l'utilisateur ou au propriétaire du véhicule de décider avec qui et pour quels usages il souhaite partager ses données : son assureur, son réparateur, son fournisseur d'électricité…

DÉCODER

Les véhicules connectés et les mutations du secteur de l'automobile

« D'ici à 2025, près de la moitié des véhicules en circulation en Europe seront des véhicules connectés »

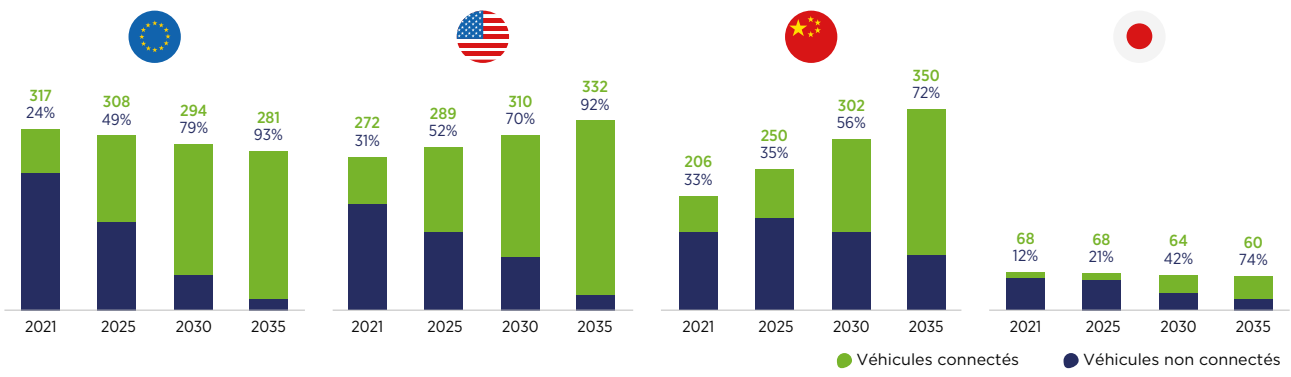
La révolution numérique, la concurrence de nouveaux entrants et des régulations environnementales toujours plus strictes ont engendré **trois mutations profondes** pour le monde de l'automobile :

- l'**automatisation** progressive (aide à la conduite aujourd'hui, délégation partielle ou totale de conduite demain) ;
- l'**électrification** ;
- le déploiement d'une **connectivité** de plus en plus aboutie (depuis le véhicule vers son environnement proche ou depuis le véhicule vers des prestataires de services).

D'ici à 2025, près de la moitié des véhicules en circulation en Europe seront des véhicules connectés.

NOMBRE TOTAL DE VÉHICULES CONNECTÉS RAPPORTÉ AU PARC TOTAL DE VÉHICULES

En millions d'unités et %



Source > Digital Auto Report, PwC, 2021.

Or, il existe un risque de verrouillage de ces données par certaines entreprises, qui pourraient devenir des points de passage obligés et/ou mettre en œuvre des formes de « péage » sur l'accès aux données, limitant ainsi la liberté de choix des automobilistes et freinant le développement de services innovants.

Afin de garantir la maîtrise par chaque utilisateur de ses données et d'aider les professionnels à intégrer cette dimension de protection dès la création de leurs produits ou services, les assureurs ont contribué dès 2017 à l'élaboration du pack de conformité Cnil « véhicules connectés et données personnelles[1] ».

La Cnil rappelle que les données personnelles comprennent les données directement identifiantes, comme le nom du conducteur, mais également les données indirectement identifiantes, telles que le détail des trajets effectués, les données d'usage du véhicule (par exemple, les données relatives au style de conduite ou au nombre de kilomètres parcourus) ou encore les données techniques du véhicule (relatives, par exemple, à l'état d'usure des pièces) qui, par croisement avec d'autres fichiers, peuvent être rattachées à une personne physique.

La Cnil identifie trois scénarios de collecte de données :

- les données collectées dans le véhicule restent dans celui-ci sans transmission aux fournisseurs de services ;

Exemple : une solution d'éco-conduite traitant les informations directement dans le véhicule afin d'afficher des conseils en temps réel sur l'ordinateur de bord.

- les données collectées dans le véhicule sont transmises à l'extérieur pour fournir un service à la personne concernée ;

Exemple : un contrat de « *Pay as you drive* » souscrit auprès d'une société d'assurance.

- les données sont transmises à l'extérieur pour déclencher une action automatique dans le véhicule.

Exemple : « Info-trafic » dynamique avec calcul d'un nouvel itinéraire après un incident sur la route.

Ce pack propose des lignes directrices permettant, pour chaque type de traitement identifié, de préciser leurs finalités, les catégories de données collectées, leur durée de conservation, les droits des personnes, les mesures de sécurité à mettre en place et les destinataires des informations.

La pénurie de compétences « tech »

La digitalisation des entreprises s'inscrit dans une double tendance mondiale : l'apparition de nouveaux emplois numériques d'une part, la numérisation des emplois dits traditionnels d'autre part. En effet, les modes et outils de travail évoluent au gré de l'introduction de nouvelles technologies visant à simplifier, optimiser, voire automatiser les processus existants.

La digitalisation des emplois est générale et s'observe dans le monde entier, indépendamment du secteur et du niveau de qualification du poste. Selon une étude de la Commission européenne[2], les métiers de cadre requièrent aujourd'hui des compétences numériques de base dans 98 % des entreprises de l'Union européenne.

« Le fossé se creuse entre les compétences disponibles et celles devenues incontournables »

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 effet, alors que dans les entreprises

1 — Document consultable sur www.cnil.fr.

2 — *ICT for Work* : *Digital Skills in the Workplace*, mai 2017.

américaines, un tiers des collaborateurs manqueraient de compétences digitales[1], la pénurie de talents « tech » est telle que 1,2 million d'ingénieurs informatiques pourraient manquer en 2026 aux États-Unis[2].

En France, la pénurie de main-d'œuvre dans le numérique se traduit par une tension forte sur le marché de l'emploi. En 2018, les candidats pour des postes en informatique étaient seulement 1,5 fois plus nombreux que les offres d'emploi, un ratio très faible[3], avec un nombre relativement modeste de candidatures répondant à l'ensemble des exigences en matière de compétences numériques. **Cette tension ralentit le rythme de la transformation digitale des entreprises, qui peinent à recruter**. Les trois quarts des dirigeants interrogés dans le cadre d'une étude menée par le cabinet Gartner en 2021 considéraient ainsi la faible disponibilité des talents comme le premier facteur de risque au moment de lancer un plan de transformation digitale au sein de leur organisation[4].

Parmi les **compétences rares** les plus demandées, **cybersécurité** et **intelligence artificielle (IA)** arrivent en tête. La complexification croissante des systèmes d'information induit, on l'a vu, un risque accru d'attaques cyber. Conséquence : plus des deux tiers des entreprises dans le monde manquent de spécialistes **de la sécurité informatique**. À l'échelle mondiale, 4 millions de collaborateurs supplémentaires devraient être formés pour répondre à la demande[5]. Quant à l'intelligence artificielle, la pénurie de profils en France trouve deux explications : une offre de formation diplômante relativement faible, d'une part, et l'attractivité des géants nord-américains et chinois du numérique auprès de la main-d'œuvre hautement qualifiée d'autre part. Cette rareté des ressources crée une tension particulièrement forte sur certains métiers de l'intelligence artificielle : programmation, *machine learning* et modélisation, Big Data, robotique…

La pénurie de compétences « tech » est tout aussi palpable dans le secteur de l'assurance. Si l'assurance est *data native* (la donnée fait partie de son ADN), elle n'est pas *digital native* (née avec l'essor du numérique). Elle doit donc aussi se doter des moyens de développer, capter et retenir les talents et compétences stratégiques.

1 — National Skills Coalition, *The New Landscape of Digital Literacy*, mai 2020.

2 — « La guerre des talents est déclarée dans la tech », *Les Échos*, octobre 2021.

3 — « La pénurie de main d'œuvre dans le numérique est d'abord un besoin de compétences », *Les Échos*, décembre 2018.

4 — The 2021-2023 *Emerging Technology Roadmap Survey*, septembre 2021.

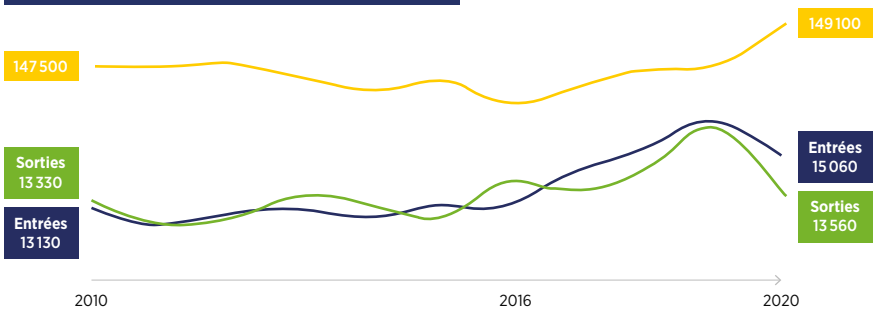
5 — Enterprise Strategy Group ISSA, *The life and times of cybersecurity professionals*, décembre 2019.

DÉCODER

Les recrutements dans le secteur de l'assurance face aux besoins digitaux

- Le secteur de l'assurance est caractérisé par une stabilité de ses effectifs : **+1% entre 2019 et 2020, soit 1500 salariés supplémentaires** ;

ÉVOLUTION DES EFFECTIFS DE 2010 À 2020



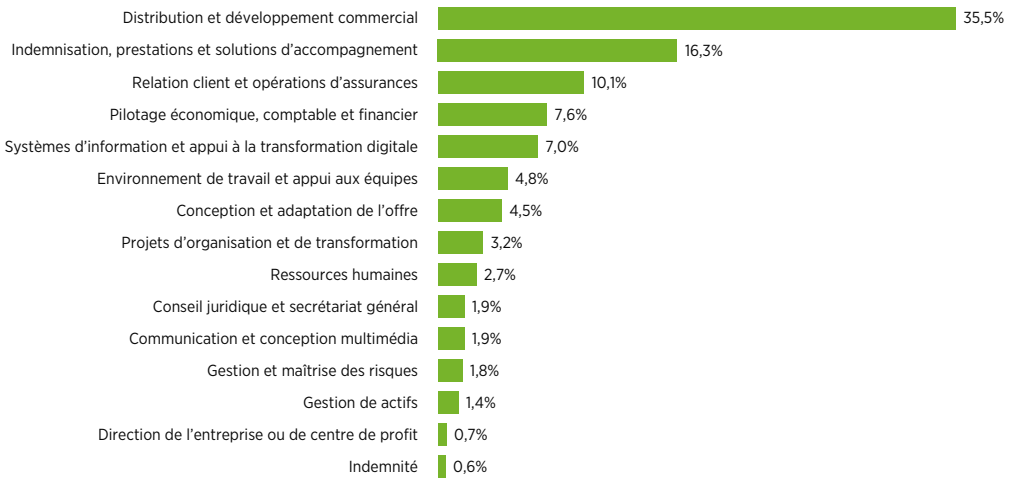
- Le niveau de qualification est en croissance depuis plusieurs années : la **part des recrutements de bac+5 est en hausse de +3,4 points de pourcentage entre 2015 et 2020** ;

ÉVOLUTION DE LA STRCUTURE DES RECRUTEMENTS

	2015	2016	2017	2018	2019	2020
Femme	58,9 %	58,9 %	59,9 %	60,7 %	60,0 %	**59,3 %**
Cadres	26,4 %	30,6 %	28,7 %	31,2 %	32,8 %	**29,9 %**
Âge moyen	30,0 ans	30,5 ans	30,7 ans	30,9 ans	31,2 ans	**30,9 ans**
< 30 ans	58,6 %	56,5 %	55,4 %	53,5 %	52,1 %	**53,9 %**
≥ 55 ans	1,2 %	1,7 %	2,0 %	1,6 %	1,8 %	**1,4 %**
CDI	49,8 %	51,5 %	52,3 %	52,8 %	56,7 %	**54,0 %**
Alternants	25,1 %	23,3 %	26,2 %	23,9 %	23,6 %	**24,9 %**
≤ Bac +2	20,4 %	18,9 %	19,4 %	18,5 %	20,9 %	**17,8 %**
Bac +2	34,5 %	29,5 %	30 %	28 %	25,8 %	**26,5 %**
Bac +3	19,3 %	21,9 %	23,7 %	23,1 %	22,9 %	**26,5 %**
≥ Bac +5	25,8 %	29,7 %	26,9 %	30,4 %	30,4 %	**29,2 %**

- Plus de 10 % des nouvelles embauches dans l'assurance sont consacrées aux systèmes d'information, à l'appui à la transformation digitale ainsi qu'aux projets d'organisation et de transformation.

VENTILATION DES NOUVEAUX ENTRANTS EN 2020



Source > Observatoire de l'évolution des métiers de l'assurance, ROMA 2021.

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

Mieux protéger les citoyens et les entreprises contre les nouvelles menaces cyber

À la suite de la crise sanitaire et face à l'augmentation des cyberattaques en 2021, constatée par l'Agence nationale de la sécurité des systèmes d'information (Anssi), dont ont été victimes des entreprises de taille significative, des hôpitaux ou encore des collectivités territoriales, il n'est plus possible d'en douter : les risques cyber constituent une menace grandissante pour notre économie.

C'est la raison pour laquelle **France Assureurs propose de faire de la lutte contre les risques cyber une grande cause nationale** sous l'égide des pouvoirs publics, démarche à laquelle les assureurs pourraient s'associer autour de plusieurs axes.

FABRIQUER

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.

Par ailleurs, l'ensemble des acteurs souhaitent que l'État français et l'Union européenne se positionnent clairement sur le sujet. Des avis se sont exprimés sur le fait qu'assurer le remboursement des rançons pourrait être un facteur d'incitation aux cyberattaques.

FABRIQUER

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…).

DÉCODER

Les réponses apportées par le Hcjp sur le cadre légal de l'indemnisation du paiement des rançons

Le Haut Comité juridique de la place financière de Paris (Hcjp) promeut une stabilité juridique et un cadre clair permettant à la fois aux assureurs et aux assurés de bien cerner la portée de leurs engagements respectifs et la portée des couvertures souscrites. Dans son rapport, il prend position sur trois questions, restées à ce jour sans réponse :

Les sanctions administratives, notamment pécuniaires, peuvent-elles faire l'objet d'une couverture assurantielle ?

Le rapport répond par la négative s'agissant des sanctions administratives de nature pécuniaires, mais ouvre la voie d'une possibilité d'assurer des mesures correctrices imposées par l'autorité compétente.

Le paiement des rançons et leurs indemnisations par des assurances sont-elles licites ?

Le rapport se prononce de façon affirmative sur la licéité du paiement des rançons et la possibilité de leur couverture assurantielle, tout en rappelant les limites fixées par la règlementation relative au financement du terrorisme.

Le risque de cyberguerre est-il en droit positif français un cas d'exclusion légal de l'assurance ?

Le rapport conclut à la nécessité de clarifier la définition légale du risque de guerre pour y intégrer le risque de guerre cybernétique.

Source > Hcjp, *Rapport sur l'assurabilité des risques cyber*, 28 janvier 2022. À consulter sur www.hcjp.fr.

FABRIQUER

PROPOSITION 3

Développer une culture du risque cyber au sein des entreprises et des collectivités locales

Dans cette optique, France Assureurs salue la création par les pouvoirs publics du « Campus Cyber » dont les priorités incluront la formation et le développement de la culture du risque cyber. Cette création devrait contribuer au nécessaire renforcement des moyens de lutte contre la cybercriminalité.

Afin d'accélérer la résilience cyber de l'économie française et le transfert du risque aux assureurs, la culture du risque cyber doit davantage être prise en compte au sein de l'ensemble des acteurs économiques. Tant les dirigeants que leurs collaborateurs en entreprise, mais également les élus locaux, les agents publics et leurs services techniques, doivent être conscients de la gravité de ces risques, connaître et appliquer les règles de sécurité informatique.

FABRIQUER

PROPOSITION 4

Amplifier les efforts de sensibilisation spécifiques auprès des TPE et PME

Les efforts de pédagogie auprès des TPE et PME devraient être amplifiés et systématisés. 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 par typologie d'entreprise (TPE, PME, ETI) et par niveau d'exposition aux risques cyber ;
- le développement des **prestataires informatiques labellisés** Experts Cyber[1].

Favoriser l'innovation et la prévention en ouvrant l'accès aux données des véhicules connectés

Face aux risques de verrouillage de marché ou de mise en place de mécaniques de péage sur les données des véhicules connectés, France Assureurs a œuvré à la constitution de l'**Alliance mobilité connectée pour tous**, qui rassemble la plupart des acteurs de la filière aval de l'automobile en France : automobilistes (ACA), sociétés d'assistance (Snsa), experts (Anea), réparateurs (Cnpa et Mobivia), loueurs longue durée (SesamLLD) et fournisseurs d'énergie (UFE) et bien entendu France Assureurs, au titre des assureurs.

L'Alliance mobilité connectée pour tous a pour objectifs :

- de réaliser un état des lieux technologique ;
- d'adopter l'approche la plus didactique possible sur des sujets ardus pour les non-initiés ;
- de formuler des propositions constructives permettant de garantir un accès aux données des véhicules connectés transparent et équitable pour toutes les parties prenantes ;
- de préserver la liberté de choix pour les clients (automobilistes, utilisateurs ou propriétaires de véhicules) et de permettre l'émergence de services innovants autour de la mobilité connectée.

1 — Label Expert Cyber de cybermalveillance.gouv.fr.

EXPLORER

8 principes pour un écosystème équilibré et accessible à tous

Dans le cadre de l'Alliance mobilité connectée pour tous, France Assureurs et ses partenaires ont identifié huit principes essentiels à une structuration équilibrée de l'écosystème des véhicules connectés. **Ces huit principes, ainsi qu'un récapitulatif des enjeux juridiques, techniques et économiques autour de l'accès aux données, sont exposés dans un document pédagogique.**

1. L'ensemble des données, quelle que soit leur nature et sous réserve du consentement de l'utilisateur, doit être accessible de façon équitable à toutes les parties prenantes. Cela implique également une parfaite transparence sur les données disponibles.
2. Les choix des utilisateurs du véhicule doivent être rendus réellement effectifs grâce à des modalités fluides et réversibles du recueil de leur consentement.
3. Plusieurs modalités d'accès doivent être prévues afin de préserver la neutralité technologique et d'éviter les verrouillages de marché.
4. Ces accès doivent s'opérer dans des conditions techniques et économiques identiques pour tous les acteurs, du constructeur à l'opérateur indépendant. Les conditions financières doivent être raisonnables et compatibles avec le développement de services digitaux innovants.
5. L'accès aux données et aux ressources du véhicule (y compris l'interface homme - machine) doit être direct et, si nécessaire en temps réel (c'est-à-dire sans délai).
6. Les parties prenantes doivent dans le cadre d'un besoin métier pouvoir accéder aux données essentielles contenues au niveau même des calculateurs.
7. Une approche intersectorielle et coopérative doit permettre de concourir à un objectif partagé de sécurité et cybersécurité des véhicules.
8. Une règlementation européenne est primordiale, notamment en termes de standards, afin d'asseoir ces principes et une gouvernance neutre.

Source > France Assureurs, *Véhicule connecté : 8 principes pour un écosystème équilibré et accessible à tous*, février 2021.

Pour consulter ce document, rendez-vous sur franceassureurs.fr, rubrique « Nos positions » / « L'assurance protège ».

FABRIQUER

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 ses données ;
- l'accès transparent et équitable pour tous les acteurs.

Préparer les salariés aux métiers digitaux de l'assurance

France Assureurs propose le **renforcement des filières d'excellence en matière d'apprentissage et d'alternance en assurance, avec une attention toute particulière portée aux métiers du digital**.

— Ouvrir l'apprentissage aux compléments de formation

Certaines compétences rares en matière de numérique, de transition énergétique et écologique font l'objet de compléments de formation sous forme d'une certification à l'issue de la formation initiale. De la même façon, certaines certifications (Certificat de qualification professionnelle, etc.), formations ou habilitations réglementaires sont nécessaires pour pouvoir exercer les métiers en complément des diplômes.

Or, à ce jour, seules les formations diplômantes de l'enseignement supérieur ou les titres d'école inscrits au Registre national des certifications professionnelles sont éligibles à l'apprentissage. Les formations de courte durée (inférieures à 150 heures) sont aujourd'hui souvent essentielles à une bonne insertion dans l'emploi mais ne rentrent pas dans le périmètre de l'apprentissage.

— Accompagner les salariés dans un contexte de digitalisation des activités

Dès 2017, dans un contexte de digitalisation des activités du secteur de l'assurance, le Certificat digital assurance (CDA) a été déployé auprès des salariés des sociétés d'assurance, dans l'objectif d'attester des compétences digitales essentielles à l'exercice de leur métier. Issu de travaux menés dans le cadre de la Commission paritaire nationale de la formation professionnelle et de l'emploi de la branche des sociétés d'assurance, le CDA a fait l'objet d'un enregistrement à l'inventaire des certifications professionnelles.

Le jury paritaire a validé près de 70 000 certificats, garantissant ainsi des compétences détenues par les salariés de l'assurance : « l'intégration de la digitalisation des activités et les apports des outils numériques dans la pratique professionnelle » et « la maîtrise des outils du poste de travail connectés ».

Les entreprises ont accompagné les montées en compétence des salariés grâce aux actions de formation établies en amont, ou bien en aval, du passage de la certification.

FABRIQUER

PROPOSITION 6

Rendre éligibles à l'apprentissage les compléments de formation

(Certifications, habilitations professionnelles…) essentiels pour certaines compétences rares recherchées dans le cadre des activités numériques, en les finançant par une majoration du coût du contrat à chaque fois qu'ils sont mis en œuvre ;

Renforcer l'accompagnement des salariés

Dans un environnement de travail en perpétuelle évolution.

Le traitement des données à caractère personnel : guide d'actualisation du pack de conformité assurance

Depuis 2014, les organismes d'assurance disposent d'un référentiel fixant un cadre au traitement des données à caractère personnel : le pack de conformité assurance. L'entrée en application du règlement général sur la protection des données (RGPD), le 25 mai 2018, a nécessité sa mise à jour. Afin de clarifier les règles applicables depuis 2018, France Assureurs, le Centre technique des institutions de prévoyance (CTIP), la Fédération nationale de la Mutualité Française (FNMF) et Planète CSCA ont ainsi élaboré ensemble à un guide actualisant ce pack de conformité. Ce guide a été rédigé en association avec les services de la Cnil.

Pour consulter ce guide, rendez-vous sur franceassureurs.fr, rubrique « Nos positions » / « L'assurance protège ».

FRANCE ASSUREURS

FAIRE AVANCER LA SOCIÉTÉ EN CONFIANCE

France Assureurs – Faire avancer la société en confiance est une marque de la Fédération Française de l'Assurance.
Conception/réalisation : agence Pastelle.

26, boulevard Haussmann
75009 Paris

Rue du Champ de Mars 23
1050 Ixelles
Bruxelles-Capitale

franceassureurs.fr
@FranceAssureurs