OPTIC

Artificial intelligence, solidarity and insurance in Europe and Canada

Roadmap for international cooperation

January 20, 2020

OPTIC

Artificial intelligence, solidarity and insurance in Europe and Canada

Roadmap for international cooperation

HUMAN TECHNOLOGY FOUNDATION

INSTITUT DE LA TECHNOLOGIE POUR L'HUMAIN MONTREAL

Report produced in partnership with:

Allianz

BCF AVOCATS D'AFFAIRES

CNP assurances

EY Building a better working world

SwissLife

GROUPE VYV

OBSERVATOIRE INTERNATIONAL SUR LES IMPACTS SOCIÉTAUX DE L'IA ET DU NUMÉRIQUE

ICO INSTITUT DE LA CONFIANCE DANS LES ORGANISATIONS

Table of Contents

Summary 6
Introduction 12

Chapter 1 - Main uses 15
What is insurance? 16
The impact of IA on the industry 18

Chapter 2 - Mutualization: the challenge of solidarity 27
From prediction to foresight: individual responsibility of insureds and insurer commitments 29
AI and the temptation to hypersegment 32

Chapter 3 - Ensuring responsible AI 35

Chapter 4 — Expected technical characteristics 39
Making AI understandable for all 40
Better managing new and existing biases 42

Chapter 5 — For enhanced performance 45
AI and client relationships: Humans in the loop 48
Nudging insureds in the right direction 52

Chapter 6 — Personal data 57
Improving Canada's regulatory framework 58
Better managing the impacts of emerging new data 60

Chapter 7 — Governance 65

In conclusion 68

Glossary 70
Participants 73
footnotes 74

Summary

Artificial intelligence (AI), defined here as a set of computer-based automatic learning techniques enabling the performance of more or less general cognitive tasks associated with human intelligence, is already permanently transforming the way the insurance industry operates. In other words, the rise of AI is impacting — and will continue to impact — the ways insurers use the data they have, how they manage insurance contracts and the relationship between insurers and insureds, to name only a few areas. For this reason, oversight of insurance industry AI creation and development practices appears crucial to maximizing positive impacts and minimizing potential negative effects.

Produced by European and Canadian insurance stakeholders, this report aims to spark in-depth discussion on the nature of such oversight and how it might be implemented, whether it should take the form of regulations or consist of standards set by the profession.

To begin such a discussion, we must first of all set out the principles that will enable insurance stakeholders to use AI responsibly. For individuals, mutualization and solidarity provide the means for insuring each other against social risks. Individuals are held to be responsible for some (but not all) of the risks they incur, while insurance companies seek to segment the market in the most relevant way possible, i.e., to assign different levels of risk to their current and potential clients and price each level accordingly. The increased potential of technology and AI is forcing us to reflect on these practices and their future. For example, insurers' use of connected devices, which provide valuable information about insureds' behaviour, may conflict with the fundamental right of people to live their lives according to their own ideas of the good life. And hyper-segmentation, when extended to its logical conclusion of fully personalized pricing, could call into question the principle of mutualization between insureds. Clearly, it becomes desirable to anticipate the risks associated with deploying AI in order to leverage all of its potential.

We therefore propose the following seven principles to support the adoption and deployment of ethical, trustworthy and human-centric AI in the insurance industry:

► SOLIDARITY: The development and use of artificial intelligence systems (AIS) must be compatible with maintaining solidarity between people and generations.

► EQUITY: The development and use of AIS must contribute to achieving a fair and equitable society.

► RESPONSABILITY: The development and use of AIS must not contribute to lessening the responsibility of insurance professionals or their clients.

► TRANSPARENCY AND JUSTIFICATION: AIS must be intelligible and their recommendations justifiable and accessible to professionals and users.

► AUTONOMY: The use of AIS must respect people's autonomy, with the goal of increasing their control over their lives and their surroundings.

► PRIVACY AND INTIMACY: Privacy and intimacy must be safeguarded from the intrusion of AIS and personal data acquisition and archiving systems (DAAS).

► WELL-BEING: The deployment of AIS must not be prejudicial to the individuals, professionals and users affected by them and must, as far as possible, contribute to their well-being.

To comply with these principles, AIS should have certain characteristics: all individuals, regardless of the many particular factors that may have influenced them, should be able to understand the decisions made by the AI systems implemented by insurers. These tools should also be designed so as not to duplicate or reinforce some of the biases already experienced by certain members of society (whether contamination by social biases originates in the data used, the algorithms or the lack of diversity of the teams that developed them). Accordingly, insurance professionals must work with their technology providers to develop systems and procedures that promote AIS auditability and explainability so they are able to explain their decisions in a way that is understandable to the individual concerned. Clients should systematically have the option of requesting an explanation from a human representative. Insurers should take all necessary actions to sustainably prevent the AIS they deploy from unwittingly creating or reinforcing discrimination.

AI's contribution to insurers' performance is already real in some areas, but many of the systems implemented still rely very little on machine-learning technologies. Although they draw on insurers' databases, they are often based on traditional algorithms and statistics. It must be noted that AI only produces the expected results if insurance professionals have the appropriate knowledge. Accordingly, we propose to:

► Encourage the implementation of AIS, consistent with the recommended ethical framework, in all sectors of the insurance business where the deployment of AI is beneficial to insurers and insureds;

► Carry out an inventory of current educational

program and workplace AI training for insurance professionals;

► Implement a continuous education program for all professionals to keep them up to date.

Trial and error have shown the importance of always keeping "humans in the loop" (i.e., in the decision-making process) and exercising caution when deploying AIS that changes insureds' relationships with their own environment. To achieve this, we propose to:

► Encourage healthy transparency in automated underwriting, pricing and claims settlement procedures;

► Offer clients access to an advisor, if necessary, when dealing with individual insurance;

► Provide access to a human being when the automated service fails to satisfy the legitimate demands of insureds (transparency and explainability principle);

► Clearly inform insureds or insurance applicants whenever they are dealing with a chatbot;

► Offer insureds a simple remedy against algorithmic decisions they find questionable and develop ad hoc mediation services.

AIS and connected devices also allow insurers to set up nudging mechanisms (see chapter 5) and thus influence the behaviour of individuals in a non-coercive way, by automating goal prompts, notifications, activity tracking, etc. For nudging to work and be legitimate, insureds must understand, accept and share the objectives proposed by insurers.

Accordingly, we propose to:

► Encourage insureds to have smart assistants (including proven reliable connected devices) to facilitate the adoption of healthy behaviors that satisfy their own interests first and foremost;

► Ask insurers to inform their clients, in particular about the data they collect, when they encourage them to use smart assistants;

► Where insurers offer connected devices, not make this contribution contingent on the effective use of these devices by insureds or on compliance with the personalized recommendations provided by these devices, to avoid any intrusion into insureds' private lives and any constraints on their autonomy;

► Implement a smart assistant data access system that strictly guarantees anonymity and confidentiality of insureds, so that the data cannot be used to assess the behaviour of a particular insured, but can be used by insurers statistically to adjust their predictions;

► Where, in particular situations, personal data must be transmitted, limit them to what is strictly necessary and transmit them for control purposes only in the event of a claim or dispute;

► Where it is appropriate in certain cases to incentivize insureds to buy monitoring AIS to prevent behaviours that are contrary to the insurance contract or the law and that present a high risk of loss, in return for a buyer rebate and pricing that rewards good behaviour over time, ask insurers to make clear to insureds that the use of monitoring AIS allows insurers to access personal data as a condition for adjusting pricing or offering rewards;

► Implement a robust monitoring AIS data access system that strictly guarantees the confidentiality of insureds' data so that data from these AIS cannot be used by third parties for other purposes.

The regulatory environment that currently governs the collection of data on individuals is not the same in Europe and Canada. The European Union adopted a new framework in 2018 with the General Data Protection Regulation (GDPR), while Canada continues to be governed by legislation that is 20 years old, the Personal Information Protection and Electronic Documents Act (PIPEDA).

Canadian law also protects the rights of citizens, but contains significant differences from the obligations of the GDPR, giving organizations more leeway. PIPEDA does not address the issues related to the emergence of AI. The Canadian government is aware of this and is currently working on modernizing the Act.

We therefore propose that the Government of Canada complement its efforts to modernize and strengthen its regulatory framework by taking into account the principles and rules of data protection laws in other jurisdictions in order to remain a world leader in digital economy innovation.

Finally, new types of partnerships between technology giants and insurers, as well as the issues raised by the emergence of new data (e.g. genomic data, behavioural data) are complex and often poorly understood. The authors therefore propose that a permanent watch on the issue of the use of personal data and AI in the insurance industry be set up, and that a Franco-Canadian research fund be created to review the most complex and crucial aspects.

Insurers are aware that AI will transform their business permanently and that only by using it responsibly can they improve performance, maintain public confidence and minimize the negative impacts of new practices or business models. In both Europe and Canada, emerging risks associated with the use of artificial intelligence could be mitigated by building on the principles already embedded in existing regulatory and legislative environments, including those relating to governance practices and risk management frameworks within organizations.

We therefore propose that all insurance companies adjust their existing governance and risk management frameworks to systematically incorporate the requisites for introducing AI into their operations. Finally, with the aim of informing consumers, insurers should develop, perhaps jointly, materials and activities designed to build awareness among and educate the general public and insurance professionals.

Introduction

There is nothing to be gained from dwelling on the impact of artificial intelligence on every sector of the economy or the promises and fears that has generated.

Despite being already very heavily regulated and its stakeholders traditionally cautious, the insurance industry, and life and health insurance in particular, is likely to bring into sharp focus the tug-of-war between the major positive and negative forces unleashed by the accelerating development of AI. Firstly, because it has been driven by personal data and algorithms since its inception, the industry must inevitably leverage this new potential. Secondly, because it plays an essential social role in mutualizing risks between individuals and building solidarity between them, maintaining and accepting solidarity has been facilitated to date by the technical inability to assess in detail the risk specific to each individual. And lastly, because trust is key to the relationship between insurer and insured, due to both the information that each provides the other and the passage of time between payment of the insurance premium and payment of the claim settlement an insured may be entitled to for their loss.

That being said, in a world where precious digital data is now captured by a multitude of operators across all sectors, where technology makes it possible to estimate more precisely the probabilities of future events, where the expectations and face of solidarity are changing, where ethics and trust are increasingly demanded by the various stakeholders, insurance positioning and models will have to evolve. And by the same token, how insurance contributes to solidarity and protecting individuals.

The work undertaken in this report coordinated by the **Human Technology Foundation** and its **OPTIC** network, independent not-for-profit institutions, aims to address these issues from certain angles we felt were necessary:

► Broadening reflection at the international level: beyond the traditional USA-China-Europe trilogy which in particular segments the regulatory approaches to privacy and ethics, other crossovers of points of view are rich in lessons and offer potential geo-strategic synergies. A joint Canada-Europe initiative quickly and naturally fell into place;

► Bringing together – beyond the multidisciplinary approach involving academics, technology suppliers, ethicists, etc. – insurers of all sizes whose perceptions are necessarily very different from the outset;

► Not seeking agreement on a lowest common denominator or aggregating differing, siloed points of view, but rather bringing out potential divergences and dividing lines that often reveal complex and sensitive issues, and which therefore require further work;

► Giving priority initially to joint interactive work, i.e., with a limited number of stakeholders, at the risk of losing "market" representativeness;

► Striving to clarify for the general public and non-specialists the most significant issues at stake to facilitate awareness and foster invaluable future debates;

► Taking a reflective stance based solely on expertise and free of competition: we have asked representatives, named by insurers for their recognized expertise, to share their professional opinions and musings without defending their employers' interests. Accordingly, any positions expressed cannot at this stage be considered as official positions of the insurance groups that participated in this report.

These different viewpoints have facilitated the articulation of real dilemmas, for example around the legitimacy of insurers using new technological means to influence the behaviour of insureds, even for their own good. On the other hand, they require further in-depth work, the involvement of a greater number of stakeholders, and an exchange of views at the broadest international level possible. But who would be so rash as to claim that lasting solutions to such issues exist at the moment when the capabilities of technology and the numbers of new stakeholders grow by the day?

Put simply, we hope that this first report will be an invitation to freely address the most sensitive facets of artificial intelligence and the solidarity-building role of insurance for the future of our societies, and to encourage other countries to join in the exchanges it initiates between Europe, France in particular, and Canada.s

Eric Salobir – President, OPTIC

Jean-Louis Davet – President or Denos Health Management Former CEO, MGEN and VYV mutual insurance groups

Main uses

Data are the key to insurance, so AI opens a host of new opportunities.

Driven by developments in machine learning technologies, deep learning in particular, AI is extending to all areas of human activity, from transportation and mass distribution to education and health. A wide range of algorithm-based intellectual tasks can be automated and while this is obvious for simple repetitive tasks using a finite set of instructions, it is now the case for complex tasks as machines have surpassed human computing and data processing capabilities. The development of intelligent tools is causing massive changes in professional practices and setting the working world on its ear. Disruptive technology is certainly an apt description.

Given the context, it is hardly surprising that the development and deployment of artificial intelligence systems (AIS) in the insurance industry is raising hopes of improved products and services, along with fears centred on the use of personal data at the expense of insureds. It becomes necessary to anticipate the consequences of deploying AIS in the insurance industry and to prevent the risks of unethical use. While certain of the challenges are common to all uses of AI, some are specific to insurance and are not faced by other financial services.

What is insurance?

Insurance occurs when, in return for the payment of a premium or contribution, a person (the insured) is promised by another person (the insurer) a benefit in the event of a loss such as fire, accident or illness.

Accordingly, insurance rests on two pillars:

- The random nature of the risk covered by the contract: at the time it is signed, neither insured nor insurer should know whether the loss will occur. Insurance is not possible when a risk is non-existent or certain;

- Insurance is based on the principle of mutualization. Each insurer deals with a multitude of insureds who are exposed to risks that are of the same type, but also independent (e.g., the probability of a driver having an accident does not increase because another driver had one). And compensation for people who suffer a loss is drawn from the premiums or contributions that everyone has paid.

To insure a risk, insurers must first be able to define and estimate it. This allows them to determine the amount of the insurance premium, which is calculated mainly by factoring the probability and the average cost of compensation for the risk covered. It also allows insurers to define the scope of the contract, i.e., what will and will not be covered by a policy. Insureds accept to pay a premium with no certainty that they will receive anything in return (the anticipated risk might never occur), but with the knowledge that if they did suffer a loss one day, they would be compensated by their insurer.

> *Insurance rests on two pillars: the random nature of risk and its mutualization.*

HISTORY OF INSURANCE

When Benjamin Franklin founded the first property insurance company in 1752 (the Philadelphia Contributionship for the Insurance of Houses from Loss by Fire), risk mutualization through joint contributions was already a core principle, but the prediction of risk was not. Joseph Fox and Samuel Rhoads, two of the directors of the Philadelphia Contributionship, are credited with adjusting an insurance policy to the predicted risks. What Fox and Rhoads did using the human acumen and expert judgment of a master builder, AI is achieving to an unprecedented degree.[7]

INSURANCE BY THE NUMBERS
INSURANCE: A KEY SECTOR IN CANADA, FRANCE AND EUROPE [8]

Canada (2018)

- 357 private insurers
- Number of employees: 284,300
- Revenues: $169.6 billion
- Share of GDP: 9.8%

Europe (2018)

- 3,400 private insurers
- Number of employees: 950,000
- Revenues: €1,213 billion
- Share of GDP: 7.5%

France (2017)

- 741 insurance and mutual companies
- Number of employees: 146,800
- Revenues: €211.6 billion
- Share of GDP: 9.2%

The impact of IA on the industry

The advent of AI technologies has already begun to transform the insurance industry and its increasing potential is expected to cause a major shake-up in the rules of the game widely used across the industry.

AI WILL TRANSFORM 5 KEY AREAS OF INSURANCE

- CUSTOMER RELATIONSHIP MANAGEMENT
- CLAIMS MANAGEMENT
- FRAUD
- PRODUCT DESIGN
- PREVENTION

DIFFERENT AI APPLICATIONS FOR THE INSURANCE MARKET

CUSTOMER RELATIONSHIP MANAGEMENT

	ISSUE	TECHNOLOGY	IMPLEMENTATION EXAMPLE
ANSWERING CUSTOMERS WITH SUBSCRIPTIONS	Improve customer relations with systems that answer questions 24/7	► Chatbots /Voicebots	► AXA with Xtra: dedicated mobile app with an inbuilt chatbot that coaches and advises users in their daily lives
ASSISTING CUSTOMERS WITH SUBSCRIPTIONS	Offer customers digital and "guided" sales programs	► Linking Chatbots/ Voicebots with Data Analytics	► Trov: on-demand insurance for electronic devices ► Allianz: preparation of insurance quotes
OFFERING EACH CUSTOMERS AN OPTIMUM PRODUCT	Offer customes the product or service that meets their needs: a personalized product specifically configured for them	► Robo-Advisors NBO/NBA tools	► Gambit & Yomoni: automated portfolio management tools ► Fabric: on-demand life insurance ► Oscar: US insurer with referrals to healthcare practicioners
SUPPORTING SALES ADVISORS IN THE FIELD	Support sales advisors in the field by answering their questions or proposing suitable products	► Chatbots ► Robo-Advisors ► NBO/NBA tools	► Gambit via BPCE: portfolio advisory tools for advisors ► Natixis insurance with a chatbot document search tool ► Zelros and CNP Assurances: customer scoring to find the most suitable product

PRODUCT DESIGN

	ISSUE	TECHNOLOGY	IMPLEMENTATION EXAMPLE
ANALYZING DOCUMENTS	Automate document analysis (contracts, credit offers, general/ specific terms and conditions, etc.), their classification and categorization	► Automatic text analysis (NLP) linked to RPA ► Data Analytics	► JP Morgan with Coing: automated contract review and classification
OPTIMIZING SEGMENTATION	Refine customer segmentation, or adopt real-time segmentation, to further customize products	► Data Analytics	► Beampulse: real-time website personalization for each customer segment
IMPROVING RISK FORECASTING	More accurately predict each client's risk by limiting the impact on underwriting processes. Anticipate and identify "at risk" customers	► Data Analytics/Forecasting models using all available customer data (social networks, connected objects, etc.)	
ADAPTING PRODUCTS TO CUSTOMER BEHAVIOUR	Adapt coverage/price products based on customer behaviour	► Data Analytics ► IOT	► Michelin - Driving Data to Intelligence: white label Pay how you drive service platform for insurers

CLAIMS MANAGEMENT

	ISSUE	TECHNOLOGY	IMPLEMENTATION EXAMPLE
AUTOMATING CLAIMS MANAGEMENT	Automate situation analysis, claims analysis, compensation quotes and proceed to claim settlement	▶ Automatic document analysis (NLP, images) linked to RPA ▶ Data Analytics for compensation	▶ Fokuku Life (via IBM Watson): automatic compensation calculation and validation ▶ Lemonade: AI Jim bot for analyzing claims, verifying coverage, detecting fraud and validating the claim ▶ AXA: Fizzy's Smart Contract that triggers a refund as soon as the flight is delayed
AUTOMATING PROPERTY AND LOSS APPRAISAL	Automate and certify property appraisal Automate damage appraisal after a loss occurs	▶ Automatic IOT image analysis ▶ Blockchain	▶ Monuma: online certified artwork appraisal via the Blockchain ▶ Groupama and Exo Expert: drone analysis of the affected areas and automated compensation estimates (idem Allstate and Farmers Insurance)
AUTOMATING CLAIMS PROCESS END TO END	Automate the entire process: from identification of the loss to compensation via sensors on the insured item	▶ IOT Data Analytics RPA	

PREVENTION

	ISSUE	TECHNOLOGY	IMPLEMENTATION EXAMPLE
IDENTIFYING LOSS EVENT MARKERS	Identify the markers indicating that the risk is almost certain to materialize to anticipate it as far as possible	▶ Automatic document analysis (NLP, images) linked to RPA ▶ Data Analytics for statistical reconciliation	▶ Implicity: predict deterioration and meet the needs of patients suffering from heart failure
REACTING TIMELY TO RISK OCCURRENCE	Identify a loss event to react as quickly as possible and limit its impact	▶ IOT ▶ Image/video analysis ▶ RPA ▶ Data Analytics for statistical reconciliation	▶ Apple Watch: integrated cardiac arrhythmia detector and fall detector in the watch ▶ Generali: POC on installed home sensors (water leakage, smoke...)
IDENTIFYING RISK BEHAVIOURS	Identify risk behaviours/encourage good practices to limit claims events	▶ IOT ▶ Image/video analysis ▶ Data Analytics for statistical reconciliation	▶ Connected watches: measure exercise and daily targets achieved ▶ Road safety: encourage good driving habits by analyzing behaviour and making personalized recommendations (both Tesla and Autosteer)
TO PREDICT THE RESULT OF A BEHAVIOUR	Identify cases where treatment is effective/ ineffective	▶Image/video analysis ▶ Data Analytics for statistical reconciliation	▶ Thera Panacea: predictive model for patient response to immunotherapy treatment

FRAUD

	ISSUE	TECHNOLOGY	IMPLEMENTATION EXAMPLE
IDENTIFYING FRAUD	Identify fraud events to reduce the overall cost to society and avoid settlements	▶ Automatic document analysis (NLP, images) linked to RPA ▶ Data Analytics for statistical reconciliation	▶ Shift Technology: automatic learning algorithm to detect anomalies and fraud ▶ Thélem Assurances & Kernix: detection of fraud and false claims ▶ MasterCard: fraud detection algorithm developed in-house

PROPOSAL OF SHORT AND LONG TERM SCENARIOS

2020 SCENARIO

	Issue
TECHNOLOGY	Continuation of the successful development of connected objects Initiatives to launch platform to centralize health and data at the household level Launch of the first concrete use of AI: automatic expertise, automated payment, automated customer management
COMPETITIVE ENVIRONMENT	Rise of insurtechs such as Alan via innovative services Some traditional insurers launch pilots using AI
REGULATION	No major regulatory changes First GDPR alerts for tech players

2025 SCENARIO

	Issue
TECHNOLOGY	Connected objects fully integrated into society: each insured person has several, whether for health reasons or for the household "Internet of me" platforms have been deployed, users manage and monetize their data. "Firewall" tools on their mobiles or connected objects to prevent them from people taking their data without their consent AI fully integrated into the daily life of customers via multiple sensors and customer interactions mainly processed with AI
COMPETITIVE ENVIRONMENT	Insurtechs disrupt the market thanks to automatic on-demand insurance offers and the complete automation of the customer relationship management (underwriting, contract life, claims) Traditional insurers offer products linked to connected objects and some consumer insurance initiatives in use
REGULATION	2 divergent scenarios: Trend-based scenario at regulatory level Failure scenario with very strong data protection and prohibition of cross-exploitation of data

In other cases, the use of AI could lead to the elimination of certain risks. For example, the combined use of information processing and innovative home automation tools could make the probability of water damage in a commercial building or dwelling negligible. AI thus paves the way for an insurance activity based less on claims coverage than prevention.

> *With AI, some risks that were once difficult or impossible to measure may become almost certainties*

However, insurers typically do not have all the relevant information they would like to assess an application. This means that insurers are already exploring, as far as legislation allows, new ways of collecting information on their clients and prospective clients, as well as on the risks they are asked to cover.

For example, some companies now offer automobile insurance whose cost varies according to the driver's driving ability (pay how you drive). One such case is the Allianz Conduite Connectée service. A sensor is attached to the vehicle to record data such as insureds' driving speed when navigating curves or how fast they accelerate. This product better aligns the interests of insurers and their clients, in particular by limiting the risk that these clients will behave carelessly precisely because they have taken out insurance. In France, Luko, a specialist in home insurance sold exclusively online, offers to install sensors in clients' homes to detect anomalies in electricity consumption. In the United States, John Hancock, through its health insurance offering, encourages the use of connected devices that help clients adopt healthy eating habits.

The use of AI by insurers could also lead to increased customization of insurance policies. In other words, organizations could in some cases be able to offer policies better tailored to the risk profile of each client rather than the profile of the larger or smaller class of clients they appear to belong to.

Beyond risk assessment and product definition, AI is also already being used by insurers to improve productivity. For example, interactions with clients can be facilitated by chatbots that can immediately provide insureds the information or advice they need. Other tools can help process insurance policies, determine coverage eligibility or settlement amounts, and even manage claims.

Finally, AI tools will make it possible to more effectively fight insurance fraud, a real scourge for the industry and a source of prejudice for insureds not involved in fraud, and to significantly reduce contract management costs. This may lead to lower threshold above which a risk is insurable, which could make insurance accessible to previously excluded populations.

AI is therefore paving the way for creating new business models and adopting new insurance practices. However, its use in insurance could also have negative effects that should be taken into account. To mention just one example, the integration and processing by an AIS of a greater number of indicators could make it possible to pinpoint groups of individuals with the highest risk. This could lead to very significantly increasing the premiums charged to these clients, or even to excluding them.

How can we ensure, in sensitive sectors such as health, that these populations continue to have access to insurance on reasonable terms? In addition, digital economy stakeholders are entering the world of insurance: connected car manufacturer Tesla is now a broker. Platforms such as social networks, capable of putting highly targeted prospects in contact with insurers, also play a quasi-brokerage role without being subject to the rules of the profession. How can we support the emergence of new insurance models that are created by manufacturers or digital companies?

A review of current achievements and future potential shows that one of AI's main added values for insurers also poses a real existential problem in the sense that insurance industry sustainability depends on using AI for the right reason, namely its predictive function. By reducing uncertainty, AI seems to be undermining a pillar of the insurance business – risk mutualization. What is the future of risk mutualization? Are we seeing a paradigm shift in the insurance industry whereby insureds pay for quasi-certain risks only, which would amount to saving for the future? To better understand the issues at stake, we need to re-examine the ethical and technical principle underlying insurance: building solidarity through the calculated mutualization of risks.

> *AI paves the way for an insurance activity based less on the compensation of risks than on their prevention.*

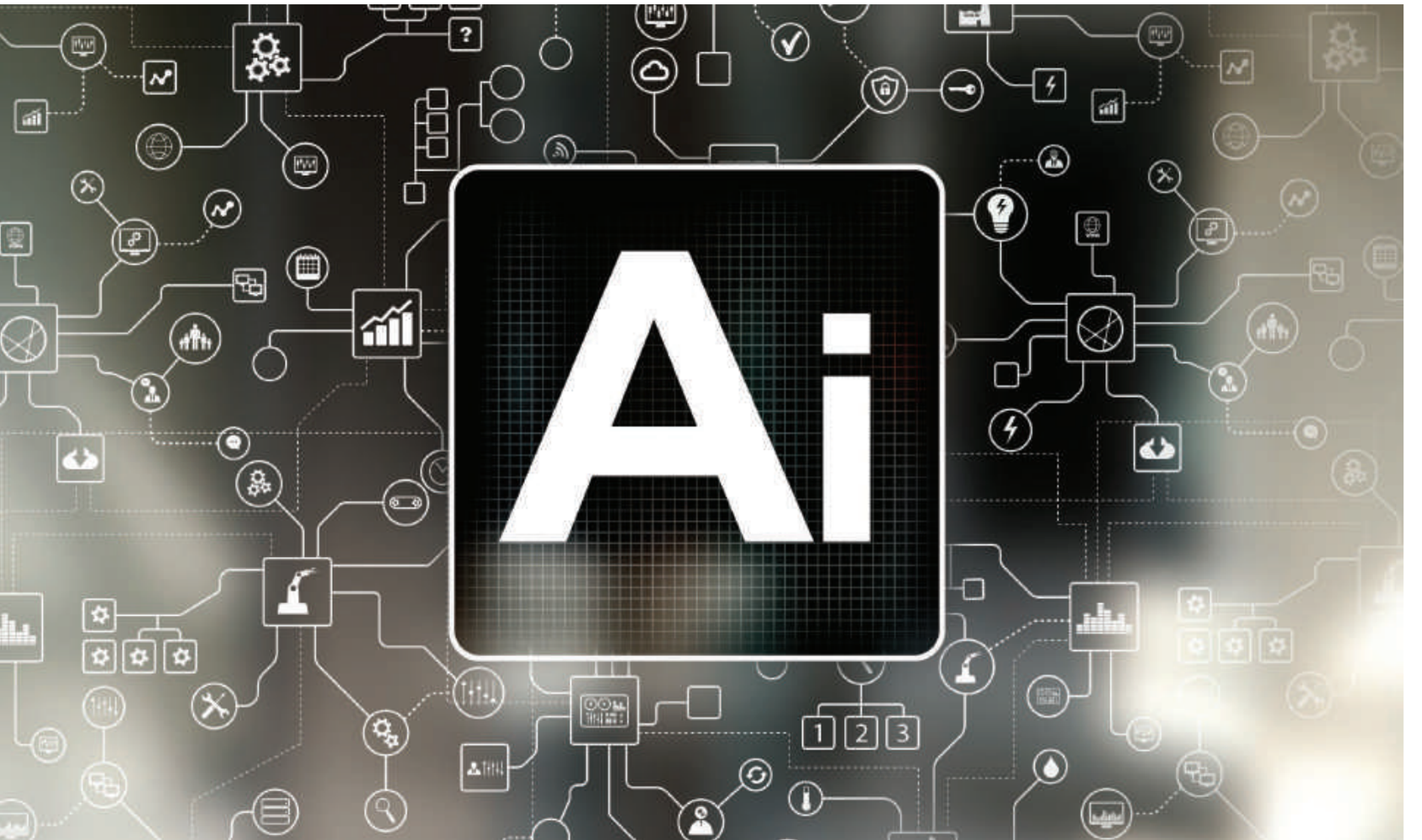
Mutualization: the challenge of solidarity

AI allows for better risk assessment and more precise client segmentation. Is solidarity at risk?

The mutualization of risks is a relatively recent innovation, dating back to the late 18th century, which has changed the way people think about their social bond. It is based on the paradigm shift related to individual responsibility and the introduction of solidarity; until that time, individuals had been held strictly responsible for their fate, with even good and bad fortune being their responsibility. This notion was weakened by the political vision of an egalitarian society where everyone saw their fellow citizens as participants in social cooperation, where by definition all enjoy the same freedoms. The social contract was thereafter seen as a solidarity pact. The members of the political community began to share resources to have the means to exercise their freedoms equitably. Social solidarity was understood early on as a way of insuring each individual against social risks. This view of solidarity puts risk at the core of community life and makes contracted social insurance the essential condition for cooperation. This facet of solidarity is also seen in the private insurance business that developed strongly throughout the 19th century. Of course, the differences between social and private insurance are significant: social insurance and the mutualist model are not based on profit, and the identification of insureds with a common purpose or a group based on an emotional bond which makes social solidarity unique is not found in private insurance. However, even in this case, there is a community of interest among insureds. Moreover, in France, the Pacte law considers services to insureds as part of insurers' raison d'être: "the company is managed in the interest of its shareholders, taking into consideration the social and environmental stakes of its activity" (Art 1833 cciv). The individual is therefore bound to all the other members of the group

who incur the same risks and accepts the duty to assist others. This is a moral element of insurance that cannot be reduced to pure calculation. Also, in France, public policies require individuals and businesses to purchase insurance products so as to create de facto solidarity between citizens, as is the case for car or home insurance. And sometimes when the State does not stipulate such solidarity, the economic world requires it, as is the case for loan insurance. In addition, the State stipulates certain obligations to ensure that certain insurance products benefit as many people as possible.

Finally, note the development of affinity insurance, which assembles individuals who wish to cover a specific risk.



From prediction to foresight: individual responsibility of insureds and insurer commitments

While a paradigm shift took place in the 19th century reducing the burden of individual responsibility, it has not disappeared. The dominant political ideologies, namely liberal and republican, have sought to formulate a balance between individual responsibility and social solidarity. If individuals suffer social misfortunes that are not of their making, social insurance covers the risks, and the social partners pool the resources. This is the principle of social redistribution. But this coverage does not go beyond what the partners are willing to pay, and a distinction is made between the misfortune suffered (brute luck) and the choices individuals make, which can increase the risks and amplify their consequences (option luck).

In the context of the relationship between insureds and insurers, the point of equilibrium follows the same logic of a division between brute luck (pure bad luck) and option luck (bad luck brought on oneself), although the breakdown is not as easy to determine in practice. Thus, the risk of contracting a disease is linked both to chance (circumstances, genetic characteristics) and to behaviours or actions such as smoking or frequenting asbestos-contaminated areas. Smoking will be said to be risky behaviour and developing lung cancer is not only pure bad luck but is partly caused by the individual's choices (option luck).

Two questions arise: firstly, should insurers refuse to cover the risks of lung cancer for smokers or increase premiums for the insured population who smoke? Secondly, can insureds who do not smoke refuse to pool their resources (premiums) with smokers in order to mutualize the risk of lung cancer? These classic dilemmas for actuarial equity illustrate the fact that the individual retains individual responsibility for risk taking and that having information on risky behaviours alters in-

surers' relationship with guaranteed risk. Access to massive data and algorithmic processing increases insurers' ability to predict risks related to insureds' behaviour.

When insurers are able to make a reliable prediction based on legally available information, insureds should exercise caution. The premium is both the price of the risk predicted by an insurer and the cost of an insured's recklessness. But the example of health also shows a fundamental ambiguity of option luck. This can be reduced to a category of brute luck, i.e., risky behaviours can still be interpreted as the result of pure bad luck, a chance occurrence that is not, or only to a small extent, under the individual's control. That is precisely what theorists of social determinants of health (SDH) tend to show, a concept that has been fully adopted by the World Health Organization. Thus, smokers' addiction can be explained by many factors that relativize their ability to choose, such as predisposition and epigenetics, as well as culture, working conditions, living environment, lack of education or information on the risks involved. While SDHs are of paramount importance for public social insurance, which mutualizes the risks of the entire population and reinforces solidarity, taking them into consideration has a lesser impact on the private sector, which is not required to ensure all risks in the same way: in a segment of the population, the individual's behaviour is analyzed, all things being equal, as an unconstrained choice. The adoption of AIS in the insurance industry does not alter the two poles of the analysis, namely highly random risk not correlated with individual choices, and risks that are individual responsibility. However, AI changes their balance because with more data being processed, individual behaviour is better known, and risks are more predictable: individual responsibility may therefore be more often called into question.

> *When individual behaviour is better known, individual responsibility is called into question more often.*

Note the reversal in the informational asymmetry between insurers and their clients: whereas, in a declarative system, insureds were in a position of strength, the analysis of the data collected now puts insurers in a better position to know the risk than clients themselves.

And the use of AIS to change individual behaviours to reduce the risks that insurers (or all insureds) do not want to bear, further increases the burden of individual responsibility. Some insurance companies are tempted to do this by using connected devices (smart watches with sensors, for example) to influence or even constrain individual behaviours.

These practices, which are spreading, are at odds and sometimes in conflict with ethical principles and fundamental rights that guarantee people the option to lead their lives according to their idea of the good life. Thus, the issue becomes finding a balance that preserves individual responsibility without exaggerating it and which protects people's autonomy and privacy.

AI and the temptation to hypersegment

In this context of an overabundance of data resulting from the cross-referencing of existing databases and collection via sensors or social network threads, the temptation is great for insurers to fine-tune profiling their clientele to the extreme in order to segment it as precisely as possible and adjust the rate to the real risk. Even if this data cannot be used by insurers, and they must obtain information through reporting by insureds (the two parties must show the utmost good faith, uberrima fides), the learning algorithms can provide very reliable prediction factors.

But the use of AIS to segment is understandable in the highly competitive environment among different stakeholders, as each company prefers to attract the right risks and leave the wrong risks to other companies. The use of tools that promise near-perfect knowledge of risk classes is therefore central to the future of actuarial practice. This trend could lead to uninsurable risks and industry stakeholders need to remain vigilant to avoid this possibility.

On the other hand, the use of less information or less intrusive information about insurance applicants or their situations that AI systems make possible is likely to improve the client "journey", which is sometimes a source of frustration or irritation. Faster, paperless processes and real-time use of constantly updated data can make selection "more discreet" for clients. In view of these issues, the feasibility of hypersegmentation and its actual benefits for insurance companies need to be assessed. First of all, the use of AI itself carries risks of error, reliability and security that could trigger a higher number of challenges and complaints before the courts. These new risks constitute an important market for insurance companies.

Furthermore, hypersegmentation reduces the size of statistical samples and no longer allows the law of large numbers, the cornerstone of mutualization, to apply. The law of large numbers interprets probability as a frequency of occurrence and presents the average as the expected value. This refers to the fact that the empirical average, calculated using the values of a sample, converges toward the expected value when the sample size tends toward infinity.

Accordingly, the predictive value of a sample is all the more important when the sample is large. Insurers strive to estimate the amount of claims to be paid in order to set the premium (expected value) to cover risk. The sum of premiums is the amount of expected claims (including a profit margin). The greater the number of insureds in

a risk class, the lower the variability of outcome. By using segmentation, insurers could see their market share (their sample) decrease to attract only those risks for which the premium is advantageous. Although these are typically better risks, the variability of outcome is greater, and insurers are exposed to a greater probability of loss. In addition, the prudential regulations to which insurers are subject require them to raise more capital, the greater the variability of the result. That is why overly granular hypersegmentation could turn out to be riskier and less profitable than imperfect and limited segmentation.

Note that this conclusion is conditional, as we do not have a mathematical model to rule out the hypothesis that hypersegmentation is profitable where insurance companies operate in a competitive environment. Moreover, some consider that insurers have already exhausted their capacity to optimize the segmentation of the risks they cover. Others believe that, for certain "long" risks (e.g., borrower's insurance), the selection at the basis of segmentation no longer makes sense and that from now on, prevention should be encouraged. It should also be noted that an insurer can recreate a form of risk mutualization by combining various groups of the insured consisting of "hypersegmented" individuals.

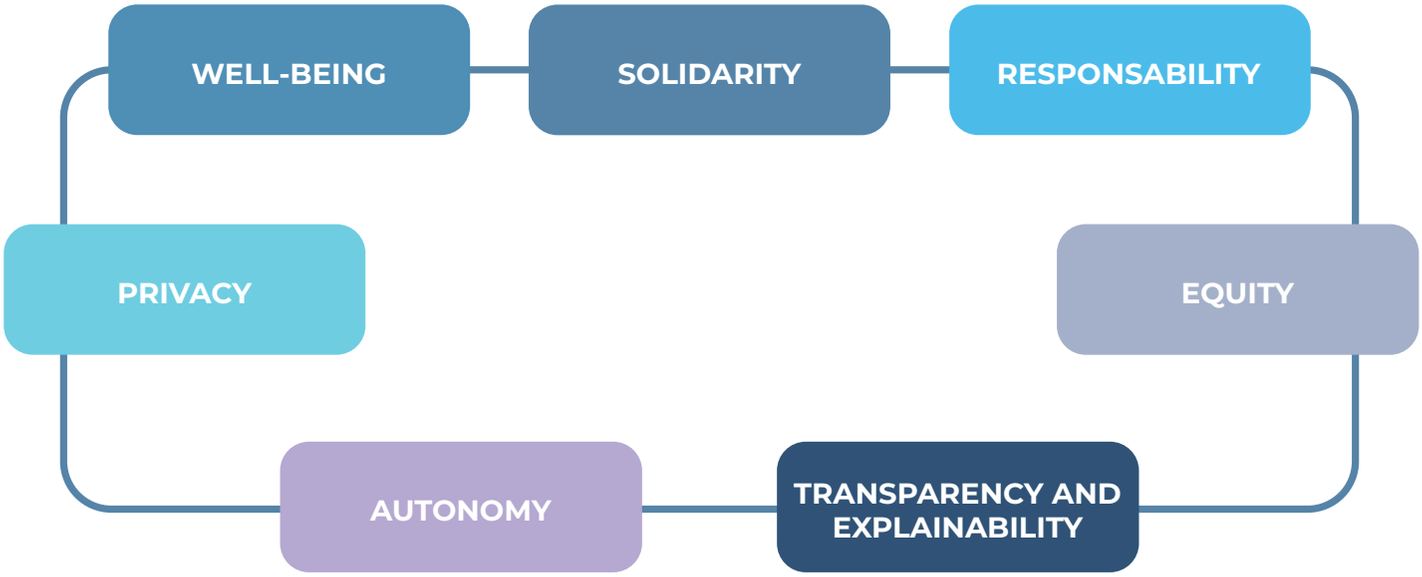
In a worst-case fictional scenario, by practising hypersegmentation, insurance would be doomed to disappear: by pushing the hypothesis to its limit, it would lead to such a fine-tuned customization of rates that it would transform insurance into a savings activity. Yet, in the face of innovation, competition does not necessarily tend to maintain diversity of practices. Technological innovation puts all players under pressure, and paradoxically, they tend to adopt identical practices even if the outcome is suboptimal for everyone. The worst-case scenario for the insurance industry, namely the disappearance of insurance is also a social dystopia, as the cost of exposure to risks would then be transferred to society as a whole, which would have to bear the full burden of social solidarity. Such a risk would likely not be accepted by public authorities against a backdrop of difficult fiscal conditions.

Ensuring responsible AI

Seven principles for ensuring AI use respects insureds.

The deployment of AI in the insurance industry offers many opportunities to develop, improve client service and enhance the performance of insurance companies. But this deployment is not without ethical and legal risk. Since the law has trouble keeping up with rapidly evolving technology, it is important to anticipate the risks of uncontrolled AI deployment to protect its full potential.

Referring to the OECD Principles for human-centric AI Development, the European Commission's High Level Expert Group Guidelines for Trustworthy AI and the ethical principles of the Montreal Declaration for a Responsible Development of Artificial Intelligence, we propose the following seven principles to support the adoption and deployment of ethical, trustworthy and human-centric AI in the insurance industry:



SOLIDARITY

The development and use of artificial intelligence systems must be compatible with maintaining solidarity between people and generations.

1. Insurance companies should deploy AIS to help improve risk management and foster conditions for the mutualization of individual and collective risks.
2. Insurance companies should not use AIS to exclude individuals from insurance on the grounds that the level of risk is too high.
3. Insurance companies should use AIS to foster collaborative work between humans and machines, and between humans, particularly on complex tasks.

EQUITY

The development and use of AIS must contribute to achieving a fair and equitable society.

1. Insurance companies must ensure that the deployment of AIS does not contribute to creating, reinforcing or reproducing discrimination among insureds. Any morally unjustified or unlawful difference in treatment constitutes discrimination.
2. The use of AIS must be consistent with actuarial equity under which cases presenting similar risks must be treated in a similar manner. Insurance companies must ensure that risk classes are appropriately defined.
3. Insurance companies should facilitate access to basic digital resources, knowledge and tools so that employees and insureds can better control their digital environment and understand AIS recommendations and decisions based on these recommendations.

RESPONSIBILITY

The development and use of AIS must not contribute to lessening the responsibility of insurance professionals or their clients.

1. Insurance professionals are responsible for decisions stemming from recommendations made by AIS they use, and the consequences that arise from them.
2. Insurance companies must ensure the robustness, reliability and security of the AIS they deploy. These characteristics should be guaranteed throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or even misuse, these systems should be able to function appropriately and not pose unreasonable safety risk, including privacy, and not cause any discrimination.[38]
3. Insureds should ensure that risks are reduced by adopting the relevant tools (particularly connected) and using them appropriately.

TRANSPARENCY AND EXPLAINABILITY

AIS must be intelligible and their recommendations justifiable and accessible to professionals and users.

1. The recommendations made by AIS should always be justifiable in a language that is understood by the people who use them or who are subject to the consequences of their use. Justification consists in making transparent the most important factors and parameters that shape the recommendation, and should take the same form as the justification we would demand from a human being making the same kind of decision.
2. Insurers should encourage healthy transparency in automated underwriting, pricing and claims settlement procedures to allow insureds to understand the key elements.
3. Insureds should be able to easily identify whether they are interacting with an AIS (chatbot) or a real person.
4. Those adversely affected by an AIS should be able to challenge its outcome based on plain and easy-to-understand information on the factors and the logic that served as the basis for the prediction, recommendation or decision.

AUTONOMY

The use of AIS must respect people's autonomy, with the goal of increasing their control over their lives and environment.

1. AIS should help people to achieve the moral and practical objectives to which they freely consent.
2. AIS must not be developed or used by insurance companies to impose a particular lifestyle on insureds.
3. On the other hand, insurance companies should facilitate the fulfilment of moral and practical objectives, including to reduce the risks posed to others by improper behaviour.

PRIVACY AND INTIMACY

Privacy and intimacy must be safeguarded from the intrusion of AIS and personal data acquisition and archiving systems (DAAS).

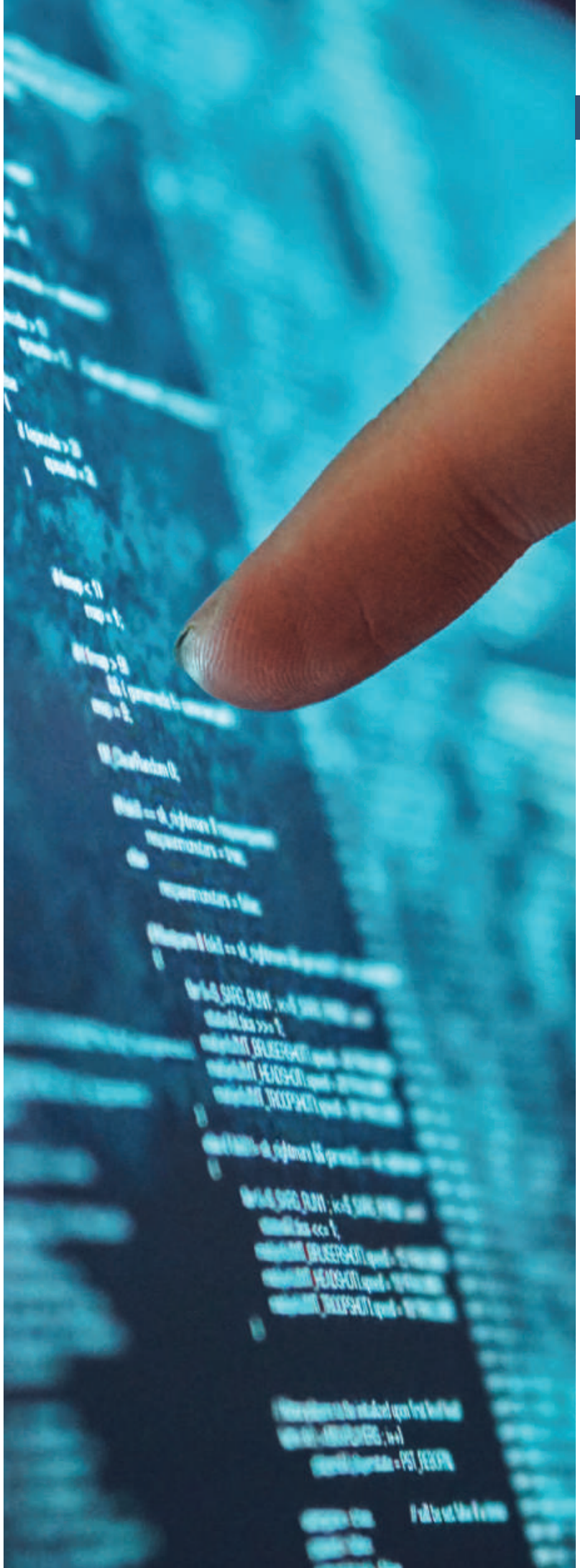
1. Insurance companies must strictly guarantee the confidentiality of data and implement appropriate mechanisms to prevent any potential breaches relating to insureds' personal data.
2. Insureds must be able to exercise extensive control over their personal data, especially when it comes to its collection, use, and dissemination.

WELL-BEING

The deployment of AIS must not be prejudicial to individuals, professionals and users affected by them and must, as far as possible, contribute to their well-being.

1. AIS should help individuals improve their living conditions, their health, and their working conditions.
2. At the least, AIS must not become a source of ill-being or contribute to increasing stress, anxiety or a sense of being harassment by the digital environment.

The implementation of the most fundamental principles is detailed in the following chapters.



Expected technical characteristics

AI-based decisions must be understood by clients and free of bias

The insurance business is complex and is an integral part of our social protection models. Therefore, building AI into the sector is a very sensitive undertaking. Not surprisingly, companies, regulators, government authorities, data or technology professionals, the general public or clients feel concerned — and in some cases greatly concerned — about how AI is and will be used in our societies.

The issue of the key characteristics that AI tools developed for the insurance industry should possess is of particular importance to stakeholders. We will see below that any tool should have at least two characteristics. On the one hand, everybody should be able to understand AI system-based decisions. On the other hand, AIS should be designed and guided in such a way as not to duplicate or reinforce the biases already experienced by certain members of societies, or to introduce new biases.

Making AI understandable for all

Insurers have always sought access to information to which they assign a range of weightings to gauge the risks associated with an insurance contract and make decisions. For example, for a home insurance policy, insurers may place more emphasis on the fact that a house is on floodable land, and less on the individual characteristics of the owners.

In the past, the volume and nature of the data considered was more limited, and the technological capacity to process data was lower. But with the emergence of AI and techniques such as deep learning, things have changed. The challenge now is precisely to provide large amounts of information to the machine in order to identify risk factors and relationships among the data that once went unnoticed. Ultimately, a decision made by an AIS today can be based on the analysis of dozens, if not hundreds or thousands of different variables. However, this approach does not apply to modelling risks without pre-event data, such as the risk of corporate credit default due to Brexit. Which means that fuzzy logic algorithms continue to be more relevant.

The emergence of new types of algorithms and the drastic increase in the number of data points taken into account makes it more difficult than before to ascertain, let alone explain, the particular factors that led to a decision. However, it is imperative that this obstacle be circumvented. Indeed, AI will only integrate effectively and responsibly into the insurance industry if everyone is able to understand the decisions that are made. For example, the reasons why an insurance policy or compensation claim was accepted or denied must be clear to employees and clients so that employees can justify them to clients and clients can accept the decision they receive. Implementing AI in insurance will be difficult if the algorithms developed resemble “black boxes”.

Therefore, AIS must be designed to produce easily interpretable results that are likely to be accepted in good faith. In particular, this requires:

► That automated decisions affecting a client should be explainable with the same degree of detail and clarity that an experienced professional would provide in a similar case without using automatic processing. Similarly, in-house within insurers, the way AI tools present their decisions to employees should not be more complicated than how an experienced colleague would do it.[42];

► That the suitability of the factors selected is itself explainable;

- That the most important elements used in making the decision be highlighted;
- That the level of transparency be commensurate with the impact of the decision on insureds situations.

Finally, however intense the invaluable technical research into algorithm explainability currently being carried out by digital economy majors, research centres and the DARPA in the U.S. may be, it will not be enough to make a machine able to explain its decisions to insurers' current or potential clients. It will be essential for a real person to be able to act as an intermediary between AI and clients if necessary.

These considerations are in line with both the principle of democratic participation of tools such as the Montreal Declaration and the provision of the EU's General Data Protection Regulation (GDPR) which stipulates that a decision taken automatically by a system, without human intervention, can be rejected by the person concerned by this decision[44].

We therefore propose that AIS used in insurance that affect clients should be able to intelligibly explain to the persons involved how processing was carried out, and that clients should systematically have the option of requesting an explanation from a human representative.

Better managing new and existing biases

"[A]lgorithms and AI applications are prone to copy human shortcomings, and replicate biased decisions that reinforce ongoing inequalities." This warrants proactively taking rigorous measures to prevent this.

The challenge is significant for several reasons: first, the power of AI and the scope of its potential impact are causing the various stakeholders to rethink definitions of equity and bias, and then to advocate that the development of AI should ultimately incorporate higher standards than those currently expected of humans given the likely impact.

In addition, the difference between equity and bias is often misunderstood or not clearly grasped. Equity, from Latin aequitas (equality), means fair treatment as compared with equality, and differs from it by implying a judgment, which makes equity relative, whereas equality is a more fact-based concept and be seen as an absolute. For example, equality advocates giving the same financial assistance to all individuals, while equity can involve scaling assistance to raise the poorest to a level already attained by those who are better off. This makes equity an ethical concept, and how it is understood may vary according to geographical or cultural context. Bias, on the other hand, means both a difference between a true but unobservable value and an estimate of it, and a methodological error leading to flawed results. Algorithmic bias occurs when the data used to drive an AIS in fact reflects the implicit values of the human beings involved in collecting, selecting or using the data. Consequently, bias can drive a disconnect in equity.

> *"The increased ability to differentiate between individuals must not open the door to unfair differential treatment."*

Insurers' core business is based on segmentation, which can ultimately be equated with a form of

"discrimination" in the mathematical sense of the term, i.e., a determination. The challenge then becomes ensuring that differentiation between groups of individuals does not open the door to unfair differential treatment.

When it comes down to it, bias from multiple sources can creep into the use of AI, through both the data used (collection, labelling, sampling) and the models.

While the behaviour of AI must be unbiased, its increasing influence does not mean that insurance companies should take a one-size-fits-all approach to dealing with different types of clients or prospects. For example, Canadian auto insurers are permitted to use drivers' ages as a key variable that weighs heavily in assessing the level of risk — and therefore the premium — associated with a policy. They should keep this right in the AI era, as no new local social considerations have emerged to date to argue otherwise.

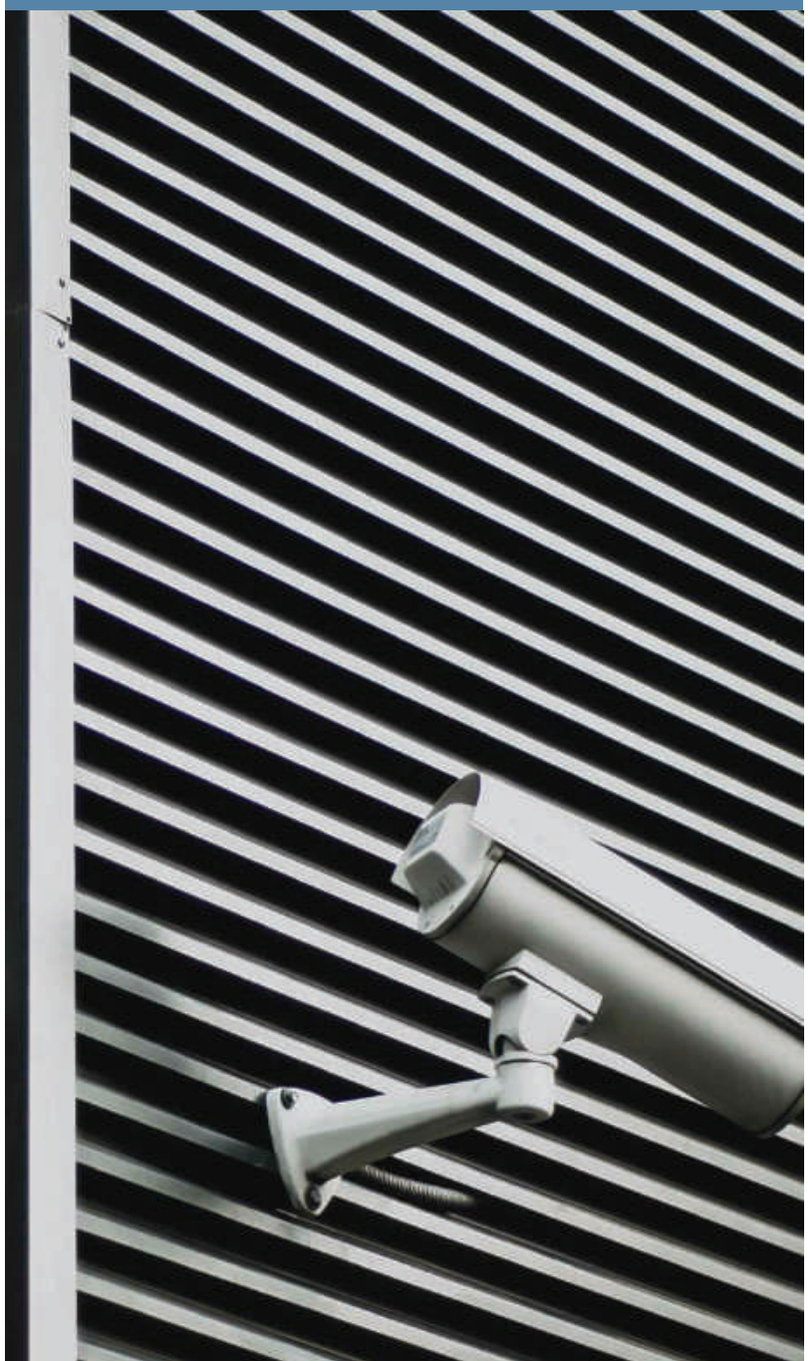
It will be necessary, however, to ensure at all times that the loss predictions made by their automated systems are ultimately as fair and accurate for inexperienced as for experienced drivers. Failing that, a new type of bias would emerge.

The explosion of digital data from non-insurance applications and uses (including social networks), segregated according to population categories, shows that the possibility of identifying one population better than another is real, and could generate different degrees of accuracy, which are potential sources of bias. Certain minority groups that have higher profiles or are better known could generate more accurate risk assessments, which might be to their favour or to their disadvantage. Any resulting difference in treatment would raise questions of ethics.

Measures to adopt to maintain equity and eliminate bias should include:

- Equity at all stages: Build equity considerations into every stage of AI development and operation (selection of training data, operating data, purpose of the algorithm, programming and validation of the algorithm, monitoring of the model over time, etc.).
- Transparency: In accordance with the above principle, explain AIS decisions with the same level of simplicity and level of detail as an experienced professional would.
- Diversity of perspectives: Build the perspectives of different stakeholders into model development.
- Regular review: Regularly challenge how fair and unbiased AI applications are with regard to behavioural, cultural and social changes on the one hand, and with regard to subsequent refinements (new data sources, enhanced algorithms) on the other.

We therefore propose that insurers take all necessary actions to sustainably prevent the AIS they deploy from unwittingly creating or reinforcing discrimination.



For enhanced performance

How do you enable people-centric decisions and use connected devices to better support insureds?

AIS are deployed with a view to optimizing performance, whether that be insurers' internal management (e.g., staff recruitment and assessment), actuarial tasks (risk and premium calculation) or improving customer services (chatbots solutions, optimizing sales paths, drafting contracts, tracking claims, etc.). So, deploying AIS in insurance should enable greater efficiency in contract management and a more effective response to the needs of insureds.

Data sharing

Based on clients' appetite for technology, 59% of the most "traditional" and 95% of the most "connected" are willing to share data with their insurer for faster and more personalized claims resolution.

Source: Accenture Technology Vision 2018

Examples of successful AI deployments

I. Simplified underwriting process

AI-based tools reduce wait times in the commercial policy underwriting process (fire, accident or other miscellaneous risks). AI solutions, including Element AI's Underwriting Partner, improve the speed and consistency of decision-making.

AI provides end-to-end support for the underwriting process, from quoting (scanning and structuring data, forms, documents and emails) to optimizing message verification. Other steps within the process include segmentation (applications are quickly classified through enabled automatic denial, processing time and complexity are estimated), assignment (assignment of applications to employees is optimized based on specialization and workload), risk assessment (assessment capability is enhanced through rapid comparison of applications, supporting decision-making and targeting anomalies), and coverage recommendation (coverage recommendations are generated automatically based on application characteristics).

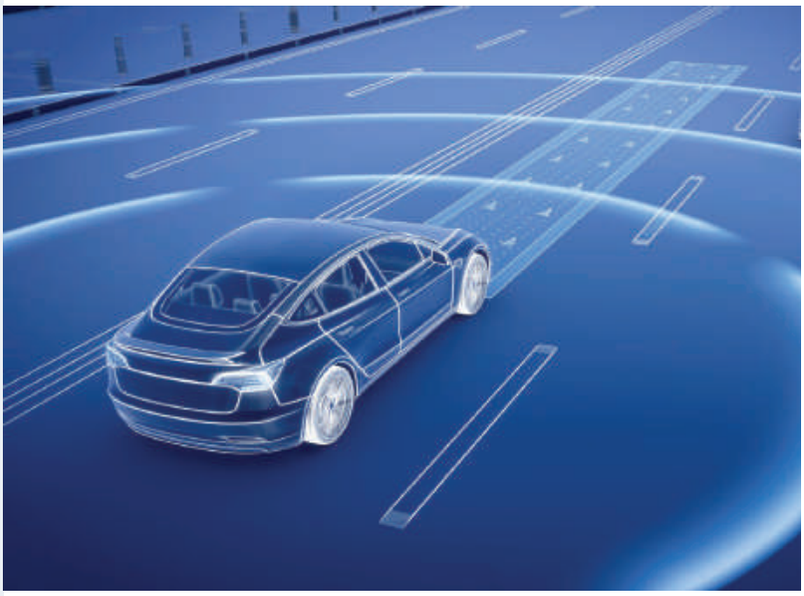
The benefits of adopting AI in this process include reduced application processing fees, higher total premiums written by underwriters, faster, more accurate and consistent quotes to clients, and an improved underwriting cycle.

II. Insurance company performance

Artificial intelligence helps improve productivity by automating repetitive sales and claims tasks.

Start-ups such as Zelros or DreamQuark leverage the notion of "augmented insurer" and deliver decision-support tools for employees' day-to-day work. AI's role, then, is to complement human expertise. The technology operates as a smart assistant that gives advisors recommendations ranging from products, sales strategies and opportunities to customer satisfaction. Recommendations are generated from client scores based on their profiles and expectations.

The tool also reduces processing times for claims management files by ranking them according to complexity, automating processing for certain simpler cases and re-allocating time to more difficult ones.



Where the primary goal in deploying AIS is to maximize the interests of both insureds and insurers, it is clear that insurers should implement automated systems as quickly as possible. That being said, this apparently self-evident recommendation presumes that insurance companies have a sound grasp of the algorithmic solutions available through academic and industrial AI research, realistic expectations around the benefits of deploying these solutions, and provide AI training for employees with different levels of responsibility across their different business lines. AI training for insurance professionals needs to be built into the university programs that will produce future professionals, but the challenge of integrating AI into insurance business lines calls for action in the here and now, and making an optimal transition will be possible only if today's insurance employees and executives are given training they did not receive at the postsecondary level. As AI technologies evolve very quickly and the market offers ever better solutions, it is crucial that professionals constantly update their knowledge.

We therefore propose to:

- Encourage the implementation of AIS, consistent with the recommended ethical framework, in all sectors of the insurance business where the deployment of AI is beneficial to insurers and insureds;
- Carry out an inventory of current educational program and workplace AI training for insurance professionals;
- Implement a continuous education program for all professionals to keep them up to date.

AI and client relationships: Humans in the loop[47]

While the wisdom of deploying AIS seems obvious when it meets the converging expectations of all, things get complicated when the interests of some (insurers) diverge from others (insured), and when performance gains for some fail to go hand-in-hand with improved service for others. For insureds, service quality is assessed on the basis of practical, economic or financial criteria (for example, fluidity of the underwriting process, premium amounts, quality of advice or reimbursement time in the event of a loss) and ethical criteria (fairness of treatment, respect for autonomy, sense of human relationships). For insurers, performance gains are assessed against several indirect criteria, such as meeting the expectations of insureds which builds loyalty, but also against direct indicators such as increased profitability, due in particular to more accurate risk calculation or better fraud detection.

Anti-fraud initiatives, one area where the use of AI currently seems most advanced in the financial industry, are particularly informative for understanding the expectations and reservations of insureds. AI-assisted anti-fraud approaches are generally well accepted. This is particularly true where fraud causes clients direct harm, which is very largely the case in banking, but not in insurance. Banking anti-fraud measures protect clients from identity theft (theft of payment cards and data). In this case, banks benefit equally with their clients from deploying AIS. In insurance, the scammer is either a client or a client's supplier. So the interests converge to a much lesser extent. In addition, the protection systems put in place by banks are typically based on authentication techniques that may be a nuisance but are not invasive. Conversely, insurance companies focus more on controlling the behaviour and habits of their clients, along with their partners' practices, which is harder to swallow. For instance, location data may indicate an activity that shows an insured is committing fraud, but the prediction of fraud will be refined mainly by cross-referencing data.

However, the insured might feel unfairly surveilled and could challenge the use of these technological tools in view of their intrusiveness and the risk of error. In some cases, however, insureds understand their immediate purpose: the cost of fraud is reflected in the aggregate amount of reimbursements and so, ultimately, in premiums, and is passed on to all insureds.

Implementing AIS in insurance also poses technical problems. Qualifying fraud is often linked to an interpretation of the facts. If systems are not properly configured or robust enough, deploying them may trigger a significant increase in the number of challenges lodged.

Beyond fraud alone, caution is required in deploying AIS that change the relationship of insureds to their own environment. It is important to maintain a human relationship across the range of insurance services, whether it be for providing information on products and on algorithm-based decisions, drafting contracts or handling disputes and claims. AIS should be used to refine insurers' judgment.

Online distribution

Many insurers in Canada already offer AIS-based alternative distribution channels and 24/7 customer service. The new Québec legislative framework allows for online insurance sales (Regulation respecting Alternative Distribution Methods) and does not require transactions to be finalized by a human. However, clients must have access to an advisor, if necessary, when dealing with individual insurance.

We therefore propose to:

- Encourage healthy transparency in automated underwriting, pricing and claims settlement procedures;

- Offer clients access to an advisor, if necessary, when dealing with individual insurance;

- Provide access to a human being when the automated service fails to satisfy the legitimate demands of insureds (transparency and explainability principle);

- Clearly inform insureds or insurance applicants whenever they are dealing with a chatbot;

- Offer insureds a simple remedy against algorithmic decisions they find questionable and develop ad hoc mediation services.


INSURANCE

Nudging insureds in the right direction

To reduce claim number and size and limit variability, while adhering to the principle of mutualization, insurers may wish to influence the behaviour of insureds. A distinction must be made here between legal but risky behaviour and behaviour that is illegal or prohibited by insurance regulations.

As regards illegal or prohibited behaviour, it seems appropriate and acceptable to use AIS, including sensors and connected devices as "terminals", which can detect inappropriate behaviour, especially in the case of property insurance: driving is a good example. This type of use requires insureds' consent, barring certain illegal behaviour for which the laws of countries such as Canada provide exceptions, in order to prevent crime.

Behaviour that is merely risky should be met with assistance and support for insureds. This is the nudge paradigm developed in behavioural economics by Nobel laureate economist Richard Thaler and political scientist and philosopher Cass Sunstein. Nudging is a non-coercive way of influencing the behaviour of individuals. An appropriate nudging system improves achievement of a societal objective that is not imposed by law, but which is in the interest of both the individual and the community: better health, accident prevention, optimal use of energy, etc.

The idea of Thaler and Sunstein is to develop mechanisms that encourage individuals to keep their moral commitments over the long term. We see the full scope of this idea in application to insurance. Insureds have an interest in adopting a "healthy" or "virtuous" type of behaviour, such as breaking a habit or picking up new ones, to reduce the odds of illness, accident and other claims. In this respect, smart connected devices serve as powerful nudging tools by automating goal tracking, displaying activity metrics, sending incentive prompts, and making it easier for

> *"For nudging to work and be legitimate, insureds must understand, accept and share the objectives proposed by insurers."*

users to adopt the right behaviour as they play the game.

For nudging to work and be legitimate, insureds must understand, accept and share the objectives explicitly proposed by insurers. The aim is to provide insureds with the means to better control their life and environment, not to dictate coercive behaviour.

In this case, the interests of insurers and insureds appear sufficiently convergent for the use of a nudging AIS to be accepted without further incentives, including financial incentives. This is crucial if smart devices are to be used to achieve the set objectives. If the payback for using them is financial, the devices risk no longer being seen as assistants, but as burdens: the connected watch becomes an electronic tracking bracelet. Insureds might also try fooling the system to get the financial reward: giving their connected watch to someone who plays sports instead of engaging in regular physical activity.

In principle, the financial gain for insurers lies in the reducing of risks and, in turn, the probability of claims. However, success in evaluating returns on investments of this nature is currently uncertain, particularly as regards the type of risk covered and the time lag between the use of AIS and the measurement of their effect on claims triggering. The most significant effects of behaviour on health, for example, are measured over the long term and therefore hold greater interest for insurers covering long and "heavy" risks such as provident care and long-term care, especially insurers with a high loyalty rate that guarantees that they, and not their competitors, will benefit from their efforts. Beyond this, to date, few reliable and proven medical-economic models exist.

To protect the privacy of insureds, connected devices such as watches or sensors attached to automobiles should provide insurers only the information they need: for example, mileage or speeding, but not details of where the vehicle was driven. For security reasons, it is preferable to use AI directly embedded in assistants and connected devices (edge computing) that transmits only results and not raw data. Furthermore, there is no need for the information to be transmitted continuously. Making them available for audit in the event of a claim should be sufficient.

ACCEPTANCE OF ADVICE AND CONTROLS

Individuals are typically very suspicious of assistance measures that are in fact often perceived as control measures. This has been well illustrated in the case of bank notifications. In one study, "Participants were universally supportive of machine learning being used to monitor their transactions in order to identify patterns and spot any unusual activity that may be fraudulent. However, only a few were positive about the idea of machine learning providing an advisory service — warning people against spending money when their balance was low or stopping the transaction altogether. This was seen as potentially intrusive, and participants generally wanted this to be something individuals would choose to use, rather than it being imposed on them by banks." Source: Royal Society, Public Views of Machine Learning (April 2017).

The use of AIS would also make it possible to include high-risk individuals, such as patients with chronic diseases, in insurance plans from which they are currently excluded or for which they are overcharged. Connected devices that warn people with epilepsy of the onset of a seizure a few minutes in advance would, for example, allow drivers with epilepsy to get into their cars without their condition increasing the risk of an accident. Canadian insurer Humania has developed specific offers for people with chronic diseases, using information collected to assess their actual state of health and give them access, for example, to borrower's insurance for buying a principal residence.

> *"Connected devices should only provide insurers with information that is strictly necessary."*

We therefore propose to:

▸ Encourage insureds to have smart assistants (including proven reliable connected devices — the first tangible action of the Espace Numérique de Santé is to propose a repository of "validated" connected devices) to facilitate the adoption of healthy behaviors that satisfy their own interests first and foremost;

▸ Ask insurers to inform their clients, in particular about the data they collect, when they encourage them to use smart assistants;

▸ Where insurers offer connected devices, not make this contribution contingent on the effective use of these devices by insureds or on compliance with the personalized recommendations provided by these devices, to avoid any intrusion into insureds' private lives and any constraints on their autonomy;

▸ Implement a smart assistant data access system that strictly guarantees anonymity and confidentiality of insureds, so that the data cannot be used to assess the behaviour of a particular insured, but can be used by insurers statistically to adjust their predictions;

▸ Where, in particular situations, personal data must be transmitted, limit them to what is strictly necessary and transmit them for control purposes only in the event of a claim or dispute;

▸ Where it is appropriate in certain cases to incentivize insureds to buy monitoring AIS to prevent behaviours that are contrary to the insurance contract or the law and that present a high risk of loss, in return for a buyer rebate and pricing that rewards good behaviour over time, ask insurers to make clear to insureds that the use of monitoring AIS allows insurers to access personal data as a condition for adjusting pricing or offering rewards;

▸ Implement a robust monitoring AIS data access system that strictly guarantees the confidentiality of insureds' data so that data from these AIS cannot be used by third parties for other purposes.

Personal data

Reconciling the use of data for innovation with protection of privacy

Effectively training and operating AI tools requires access to large amounts of data. Naturally, in this context, information on potential and current insurance clients — from the data that Canadians and Europeans share knowingly with insurance companies and many other organizations to the digital footprints they often leave unwittingly while surfing online or via social media networks to the information and data generated by AIS based on other data — is considered a commodity of the highest value, to where some cite it as the "black gold" of the 21st century.

But both Europeans and Canadians rightly expect each organization to protect their personal data and make appropriate use of it. Which raises the question: how do you regulate the use insurance players — from start-ups to the most established insurer — make of their clients' and potential clients' data? In other words, how do you reconcile the interests of industry organizations, which seek to use data and AI to innovate and improve their performance, with the interests of consumers, who are increasingly concerned about what public bodies and businesses are doing to respect their rights to privacy?

Consumers and their data

74% of Canadians state that they believe they are the real owners of the data collected from them by companies, while 72% say that their data should be protected by governments as a "natural resource"[52]. Nearly 90% of Canadians are "concerned about companies or organizations using information available online to make decisions about them, such as for a job, an insurance claim or health coverage". [53]

Improving Canada's regulatory framework

The regulatory environment that currently governs the collection of data on individuals is not the same in Europe and Canada. The European Union adopted a new framework in 2018 with the General Data Protection Regulation (GDPR), while Canada continues to work with legislation that is 20 years old, the Personal Information Protection and Electronic Documents Act (PIPEDA).

The GDPR, which sets out guidelines for the use that organizations dealing with European nationals can make of the data they have on them, as well as its first applications, illustrate the delicate balance between insurers' need to innovate and consumers' expectations around protection of their privacy. The GDPR provides that users must be informed of the specific purpose for processing their personal data (e.g., the data that organizations collect can only be used for the purposes indicated when the data are collected; if organizations wish to use the data for other purposes, they must obtain their clients' consent). The Regulation gives consumers the right to explanations about the automated decisions organizations make. It requires organizations to take transparent measures to protect the public's personal data (e.g., they must know exactly who can access data and establish procedures to prevent piracy). It requires companies to quickly delete the personal data that a consumer asks to delete. And the penalties for non-compliance with the GDPR can be as high as 4% of their annual revenues.

The advantage for international organisations is that they can now comply with a single piece of legislation rather than a host of different national laws, barring a few areas where the GDPR leaves some flexibility to Member States. Companies that adopt virtuous privacy practices significantly reduce the risk of falling victim to incidents that could damage their reputation and impact profitability. Many international companies outside the European Union are choosing to adopt business practices based on compliance with the European regulation (or the most stringent requirements) in order to avoid the costs and risks associated with complying with multiple statutes. Applying business practices based on compliance with the European Regulation rules helps to drive business performance. Giving potential clients a better explanation of why they should share their data with an organization and how they can revoke the right to use it, as necessary, allows the organization to generate higher quality prospect lists).

Canadian law also protects the rights of Canadians, but differs significantly from GPDR requirements, giving organizations more leeway. The PIPEDA

also stipulates that data handling may only take place with the consent of the individual concerned (except in rare cases) and that a company wishing to use data collected from its clients for a purpose other than initially stated must obtain renewed consent. That being said, PIPEDA does not address the issues related to the emergence of AI (the issue of algorithmic transparency was clearly not a hot button topic when the Act was drafted). The Canadian government is aware of this and is currently working on modernizing its data management framework, including a review of the Personal Information Protection and Electronic Documents Act, the Competition Act and the Statistics Act.

We therefore propose that the Government of Canada complement its efforts to modernize and strengthen its regulatory framework by taking into account the principles and rules of data protection laws in other jurisdictions in order to remain a world leader in digital economy innovation.

Better managing the impacts of emerging new data

The digitization of society is making an increasing variety of data potentially available to insurers, including:

▸ Behavioural data: social network operators, merchant sites and search engines have significant amounts of information about consumer needs and preferences that enable them to anticipate or influence some of their decisions;

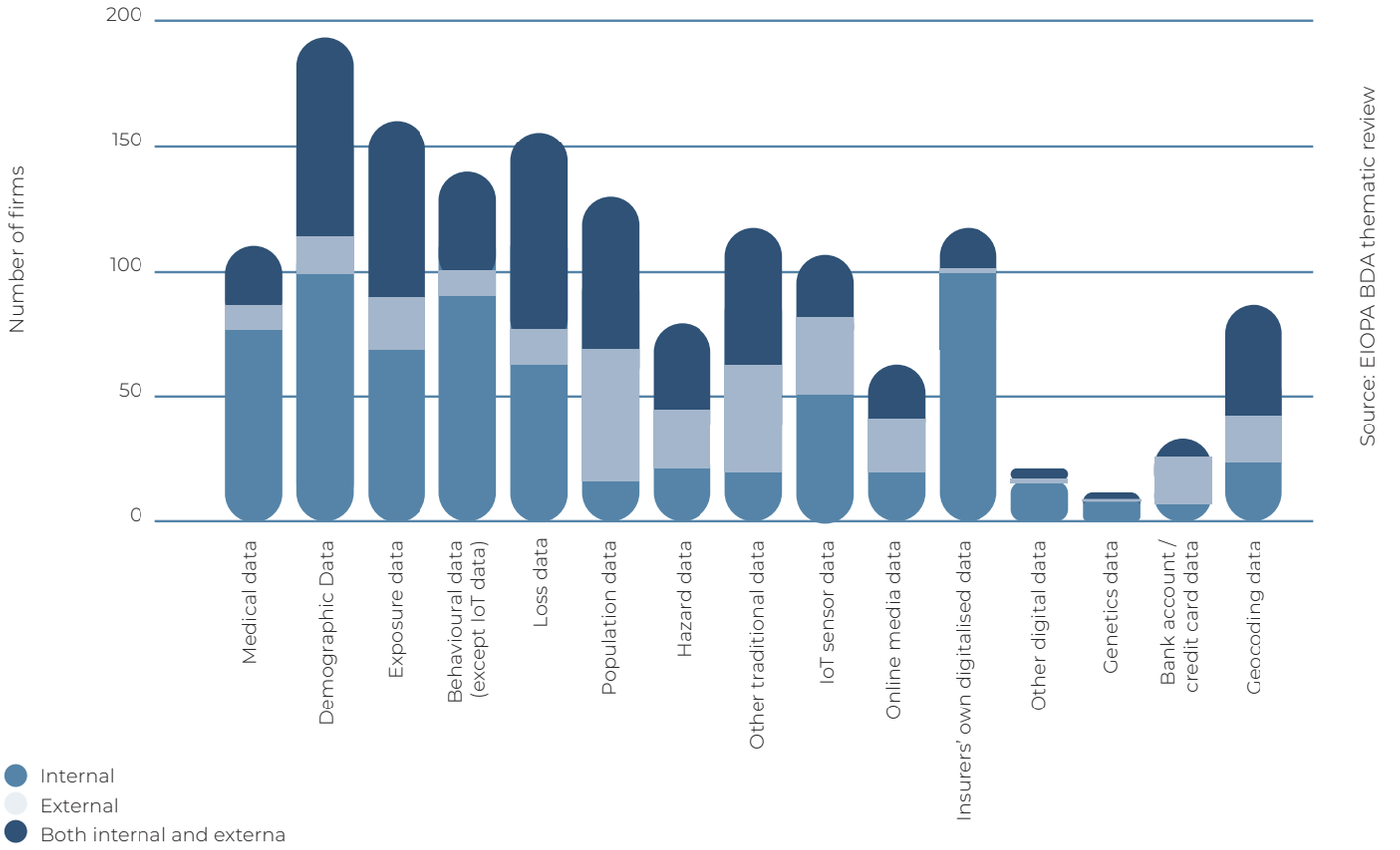
▸ Genomic data: using a saliva sample, tests are used to determine the presence of genetic mutations in a person predisposing certain types of cancer;

▸ Open data: governments and administrations are increasingly making public the data they possess, which can provide information, such as public transport timetables, property values of neighbourhood buildings), etc.[58]

▸ Data generated by the connected devices, and in particular geolocation allowing users' habits to be determined: regular visits to an oncology clinic or an allergist, for instance.

Given the appetite of businesses for this data, it is understandable that Canadians and Europeans are increasingly concerned about having a lopsided relationship with their insurer.

INTERNAL AND EXTERNAL DATA SOURCES



Source: EIOPA BDA thematic review

The legal environment surrounding many of these new types of data still varies from place to place and presents many grey areas. In addition, certain insurers state that, in their jurisdiction, the vehicle is the insured (and not the driver) and therefore data such as the number of kilometres travelled in a year are not considered personal data because "behaviour" relates to the car.

Section 1141 of the French Public Health Code prohibits insurance companies from using genetic testing to estimate the risk of disability or death of an insured, even with their consent, and French citizens whose cancer has been in remission for several years can also exercise, under certain conditions, a right to be forgotten (right of erasure)[59]. Conversely, the Canadian Genetic Non-Discrimination Act,[60] which prohibits companies from requiring consumers to undergo genetic testing to enter into or renew an insurance contract,[61] was ruled unconstitutional in 2018.[62] In addition, the Privacy Commissioner of Canada argues that it may not be necessary to create a right to be forgotten (right of erasure) in this country, as "the ability to request de-indexing and source takedown of information"[63] constitutes "an interpretation of current Canadian law [...] related to online reputation that can be found within the existing laws." In Quebec, section 20.1 of the Charter of Human Rights and Freedoms[64] stipulates that, in connection with an insurance contract, the use of an individual's state of health as a factor in determining the risk incurred by the company does not constitute a discriminatory practice. However, the new issue of how genetic information is used is not explicitly addressed. Moreover, the Québec Commission d'accès à l'information felt in 2016 that it was not "certain that this right [to be forgotten (right of erasure)], which is recognized in Europe, is applicable in Québec."[65]

> *"The digitization of society is making an increasing variety of data accessible to insurers, and the legal environment surrounding this is still unclear.."*

> *From contrasting comparisons of international experience reflecting different regulations and cultural perspectives will emerge lines of progress for all of our societies.*

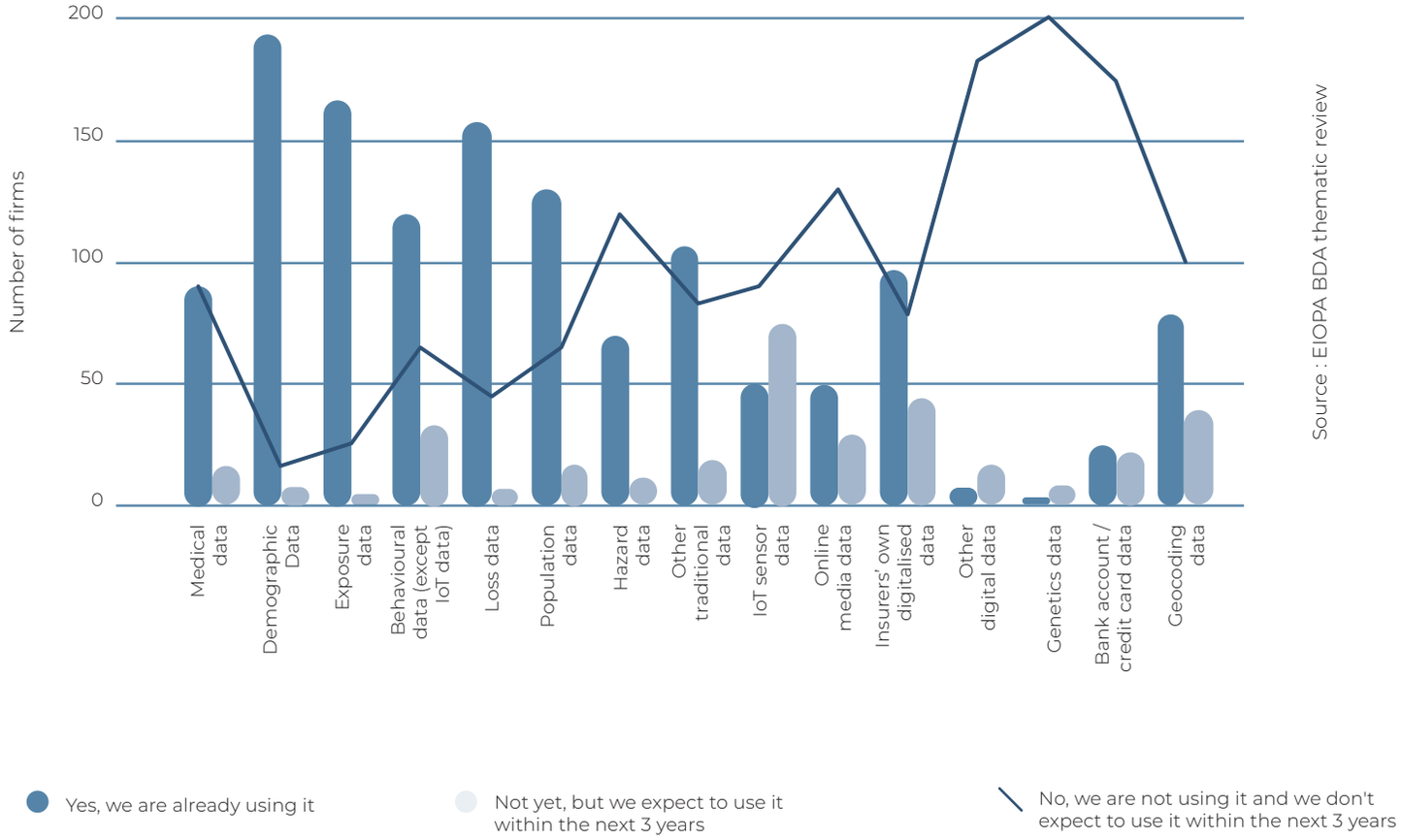
On the other hand, some technology giants such as Amazon, Google and Alibaba have certain advantages that could be used to rethink insurance services, and which are likely to be very attractive to their users. They are so ingrained in people's lives that they are well positioned to offer services in collaboration with insurance companies.

One example is Zhong An, a property and casualty insurance company resulting from a partnership between Jack Ma (Alibaba), Pony Ma (Tencent) and Mingzhe Ma (Ping An Insurance Company). China's leading property and casualty insurance company in 2013, Zhong An has more than 400 million consumers, and has sold more than 10 billion insurance policies since its inception.

The opportunities for new types of partnerships and the availability of new types of data raise major questions that professionals and regulators will have to resolve in the coming years. For example, the Montreal Declaration suggests that insureds who do not wish to share their health data should still have access to insurance coverage. The Solidarity[66] and Diversity Inclusion[67] principles clearly argue in favour of including such a rule in legislation and taking it into consideration in insurers' practices.

The issues raised here are complex and require careful consideration before any decisions can be made. With regard to genetic data, a document published in 2017 by the Québec Centre for Genomics and Policy noted in particular the lack of current information on the effectiveness of protection models and public policies implemented in this area. Accordingly, the authors recommended that the Québec government form an advisory committee of independent experts to monitor the incidence and consequences of genetic discrimination in Québec in real time and prepare

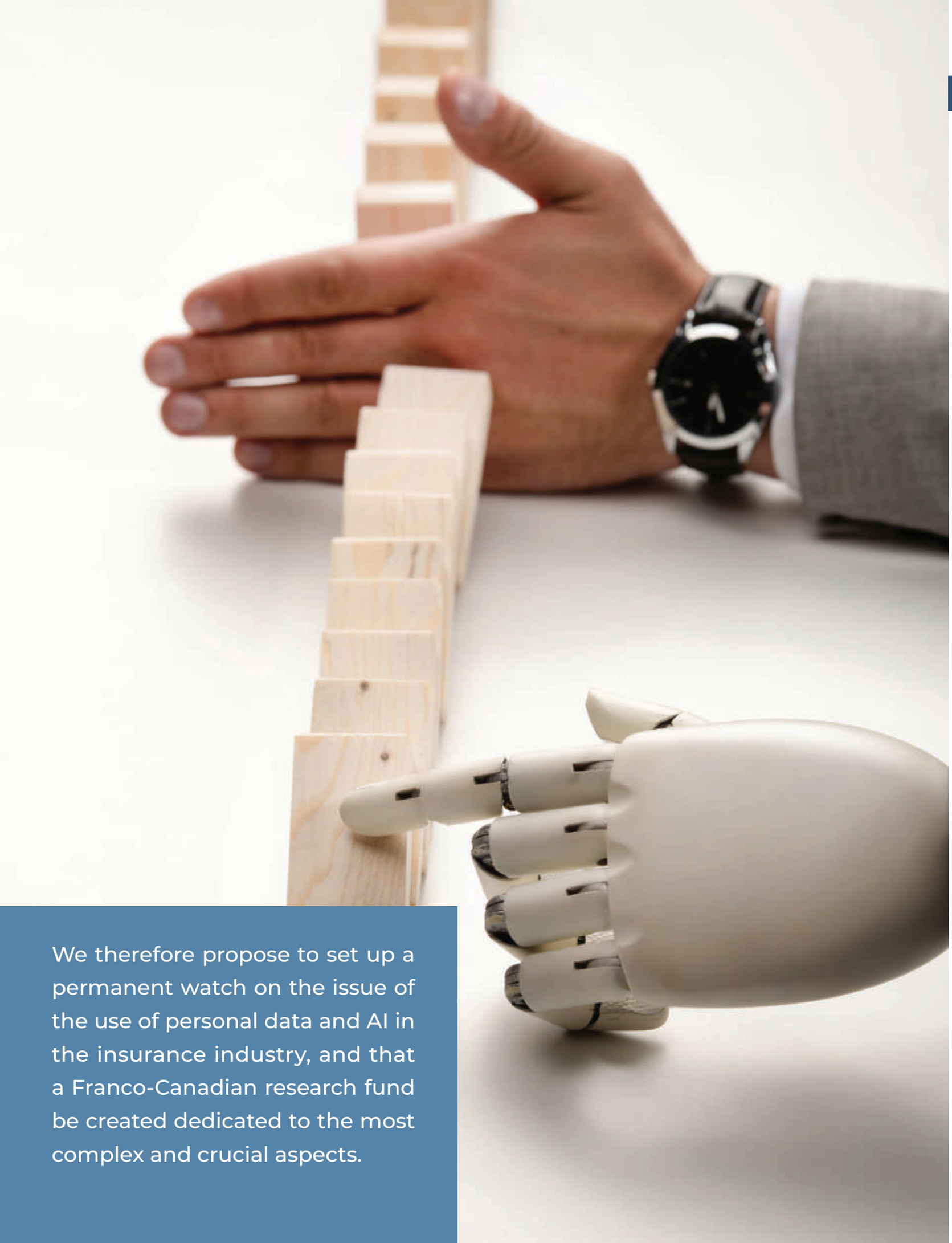
USAGE OF DIFFERENT TYPES OF DATA



a summary report. They also proposed that the Québec government request an advanced comparative study on the effectiveness of the various national genetic discrimination protection models and public policies that exist around the world [68].

On the issue of processing new types of personal data as well as other difficult issues, systematic monitoring should be undertaken to understand the differences between European countries and Canada, as well as Canada's provinces.[69] From contrasting comparisons, informed by input from real life experiences reflecting different regulations and cultural perspectives, will emerge lines of progress for all of our societies.

Because of the stakes involved, Canada and France would also benefit from setting up a joint research fund to conduct scientific research on aspects related to the emergence of new types of data in the insurance industry.



We therefore propose to set up a permanent watch on the issue of the use of personal data and AI in the insurance industry, and that a Franco-Canadian research fund be created dedicated to the most complex and crucial aspects.

Governance

Towards better corporate AI governance and increased public awareness.

Insurers are aware that AI will bring about lasting changes to their business and that only by using AI responsibly will they be able to improve their performance, while maintaining public trust and minimizing the negative impacts of new practices or business models.

In both Europe and Canada, emerging risks associated with the use of artificial intelligence could be mitigated by building on the principles already embedded in the existing regulatory and legislative environments, including those relating to governance practices and risk management frameworks within organizations.

As the Villani report[70] in particular points out, implementing an effective governance structure is one of the first criteria for success in AI, as it is in developing information technologies in general). Targeted regulatory changes to governance and risk management frameworks will be required to enable insurers to capture the full potential of these new technologies, just as they have been needed over the years to incorporate other types of emerging risks.

More concretely, Canadian and European insurers could take all or at least a significant portion of the following actions [71]:

- Establish among themselves an advisory committee on issues related to the development and use of AI, including the related ethical and legal issues. This committee would be tasked with informing and alerting the board of directors about the risks associated with deploying AI across the organization's different lines of business;
- Assign responsibility for AI to a senior executive of the organization. This AI officer should have a dual role to ensure: firstly, that the insurer uses AIS effectively, and secondly, that it uses AIS responsibly; in particular, the AI officer would have responsibility over the sometimes inevitable trade-offs between the pursuit of operational or financial performance and the duty to preserve the fairness, autonomy and privacy of insureds;

- Conduct an inventory of the algorithms developed and used by the organization and conduct a review of their foreseeable impacts and the potential risks associated with their implementation;
- Develop internal policies and rules for the organization's development and use of AI, including ensuring that the ethical issues of potential AIS bias are adequately addressed;
- Identify the national and international norms and standards to be met so that the organization can quickly adapt to future market requirements;
- Periodically audit the AIS deployed by the organization to ensure that they behave as expected, with the desired effects, without negative impacts on the organization's clients or the communities where it operates. Organizations may conduct this review in different ways. For example, they may conduct this audit work with the support of independent researchers;
- Create mechanisms that allow the public to voice their concerns about the organization's use of AI;

Insurers could also consider developing tools to predict and measure the impact on the public of deploying AIS. These tools would not necessarily have to be designed from scratch. For example, insurers could consider adapting to their particular needs the Algorithmic Impact Assessment tool developed by the Canadian government to provide "designers with a measure to evaluate AI solutions from an ethical and human perspective, so that they are built in a responsible and transparent way." [72]

> *"Public awareness and training are priorities for an industry that needs to build a lasting relationship of trust."*

That being said, insurers implementing appropriate governance structures and adopting virtuous behaviour will not be enough.

We therefore propose that all insurance companies develop, perhaps jointly, materials and activities designed to build awareness among and educate the general public and insurance professionals.

The general public will also need to have a clear understanding of what companies in the industry may or may not do, why these organizations will or will not use AI, and what positive or possibly negative impacts adopting the new technology may have on the insurer-insured relationship in the long run. In fact, the level of knowledge around AI, which is still uneven across the insurance industry, is low among the population: for example, 48% of Canadians feel they know very little or are not at all familiar with it.

To correct this situation, companies should make use of their professional associations to adopt a plan to raise public awareness of the issues surrounding the increased influence of AI in the insurance industry. In particular, activities should enable consumers to better understand how their data is collected and used in a world where AI is increasingly dominant. Insurance companies should also educate and train insurance professionals to use AI tools or liaise between the systems and the public. Developing informational videos, online courses and case studies would increase the likelihood that employees and company executives will use AI in a manner consistent with the law and human-centred AI principles that draw from the OECD Principles on AI.

We propose that insurers develop, perhaps jointly, awareness-building and educational materials and activities designed for the general public and insurance professionals.

In conclusion

Let us mention the worrying results included in the 2019 Edelman Trust Barometer:

- Only 56% of the population trusted businesses (53% in 2018);
- 56% of Canadians and 44% of French citizens trusted businesses;
- 57% of overall respondents trusted companies in the financial sector, and 78% of these trusted tech companies.

From this, we can better appreciate that establishing strong AI governance structures and awareness building and education of both the public and insurance professionals are becoming priority issues for organizations in a sector whose business is closely linked to the protection of individuals and needs to be based on a relationship of sustainable trust. These actions will not only increase the likelihood that insurers' AI projects will deliver the expected financial results while fully respecting consumers' rights and expectations, but they may also lead to increased public trust in insurers and their use of AI and their data. In the end, everyone will reap the benefits.


WE
HELP

Glossary

ACCIDENT: A sudden, unintentional, unforeseen and external event that results in injury or damage to persons, property or intangibles.

ACTUARIAL SCIENCE: is a discipline specializing in the application of probability calculus and statistics to insurance, prevention, finance and social welfare issues. This analyzes the financial impact of a risk and estimates its associated future liabilities.

ARTIFICIAL INTELLIGENCE (AI): Artificial intelligence (AI) refers to the series of techniques which allow a machine to simulate human learning, namely to learn, predict, make decisions and perceive its surroundings.

ARTIFICIAL INTELLIGENCE SYSTEM (AIS): An AIS is any computing system using artificial intelligence algorithms, whether it's software, a connected device or a robot.

CHATBOT: A chatbot is an AI system that can converse with its user in a natural language.

DIGITAL DISCONNECTION: Digital disconnection refers to an individual's temporary or permanent ceasing of online activity.

DEEP LEARNING: Deep learning is the branch of machine learning that uses artificial neuron networks on many levels. It is the technology behind the latest AI breakthroughs; it is software that writes software.

DIGITAL LITERACY: An individual's digital literacy refers to their ability to access, manage, understand, integrate, communicate, evaluate and create information safely and appropriately through digital tools and networked technologies to participate in economic and social life.

DATA MINING: also known as data drilling and data prospecting, is the extraction of knowledge or information from large volumes of data, using automatic or semi-automatic methods. This practice differs from previous practice, where information was essentially transmitted in declarative form by insurers.

LOSS: Event (fire, death...) which may trigger the contract. For third-party liability insurers, a loss exists only if the victim claims compensation from the insured liable party.

MACHINE LEARNING: Machine learning is the branch of artificial intelligence that consists of programming an algorithm to learn by itself, which

gives the computer the ability to learn and recognize patterns like humans, without having to give specific instructions for each new piece of data. The various techniques can be classified into three major types of machine learning:

(1) supervised learning, which includes two main types of activity, namely classification and regression. Classification is the process whereby the computer organizes images, fraud indicators, relevant customer loyalty information, for example. Regression is the process whereby the computer improves predictions of life expectancy, population growth, weather, customer response to marketing campaigns, and so on;

(2) unsupervised learning, where the AIS learns to find similarities among data that have not been annotated, for example, in order to divide them into various homogeneous partitions. For instance, a system can thereby recognize communities of social media users or help to better segment the customer base. A second major function of unsupervised learning is to reduce dimensionality by allowing display of big data, significant compression, structure discovery;

(3) reinforcement learning, where the AIS learns to act on its environment so as to maximize the reward it receives during training. This is the technique through which AIS have been able to beat humans at the game of Go or videogame Dota2. This form of AI is particularly useful for navigational aids, training and skills development, and real-time decision-making.

MUTUALIZATION: In insurance, the principle of sharing or "mutualization" of risk means that the premiums of a group of insureds are used to compensate for claims that occur to only a few members of the same group. This is one of the core principles of insurance, along with the randomness of a risk or the unpredictability of the loss event.

OPEN DATA: Open data is digital data that users can access freely, for example, as for data held by municipalities on water use, noise, street furniture, tree felling, bus traffic, etc. These data are generally available to the public online. For example, this is the case for most published AI research results. Examples that are more meaningful to the general public include data on public transport timetables.

PERSONAL DATA: Personal data are those that are linked to an identified or identifiable individual.

PREMIUM: Amount paid by an insured in consideration of the guarantees granted by an insurer.

TRAINING: Training is the machine learning process through which AIS build an algorithm from data. The performance of the model generated by the AIS depends on the quality of the model, which itself depends on the quantity and quality of data used during training as well as the business expertise included in the model during training.

UNDERWRITING: Act of underwriting the insurance contract. The underwriter is also called the contracting party.

Participants

- **Simon Beaulieu**, EY Canada
- **Quentin Baumie**, EY Paris
- **Pierre Besson**, DreamQuark
- **Yves Bonneau**, Chambre de la sécurité financière (Québec)
- **Christophe Bourguignat**, Zelros
- **Sylvain Canu**, EY Paris
- **Ludovic Cohen**, Allianz
- **Jean-Louis Davet**, Denos Health Management
- **Didier Decaudin**, physician
- **Emmanuelle Demers**, Hudon Advocats
- **Jannick Desforges**, Chambre de l'assurance de dommages (Québec)
- **Laurence Devillers**, LIPSI
- **Marc-Antoine Dilhac**, Université de Montréal
- **Charles Dugas**, Element AI
- **Marie Elaine Farley**, Chambre de la sécurité financière (Québec)
- **Simon Girard**, EY Canada
- **Karim Hobeila**, Intact Insurance
- **Anne-Marie Hubert**, EY Canada
- **François Laviolette**, Université Laval
- **Lyse Langlois**, International Observatory on the Societal Impacts of Artificial Intelligence
- **Sarah Larose**, Element AI
- **Philippe Limantour**, EY Paris
- **Nathalie de Marcellis-Warin**, CIRANO
- **Mathieu Marcotte**, Element AI
- **Erwan Medy**, Vyv Corp
- **Nicolas Meric**, DreamQuark
- **Danielle Miller Olofsson**, BCF Business Law
- **Nicolas Neuville**, SwissLife
- **Anani Olympio**, CNP Assurances
- **Patrick Pascal**, Google
- **Marta Peguera Poch**, Université de Lorraine
- **Florence Picard**, President, commission scientifique, Institut des Actuaires
- **Anne-Marie Poitras**, Chambre de l'assurance dommages
- **Rémi Quirion**, Ministère de l'Économie, de la Santé et de l'Innovation du Québec
- **Donald Riendeau**, Institut de la confiance dans les organisations
- **Nicole Rigillo**, Element AI
- **Réjean Roy**, International Observatory on the Societal Impacts of Artificial Intelligence (Québec)
- **Eric Salobir**, Optic Technology
- **Marc Schoenauer**, INRIA
- **Alexandra Syrovatski**, Google
- **William Sanger**, Polytechnique Montréal
- **Xavier Vamparys**, CNP Assurance
- **Nicola Vizioli**, EY Canada

footnotes

1 European Commission. 2018. EU data protection rules. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

2 Personal Information Protection and Electronic Document Act (PIPEDA) / Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), 2000, https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

3 The definitions in this glossary are drawn from the Montreal Declaration. Report of the Montreal Declaration for a Responsible Development of Artificial Intelligence (2018) https://www.montrealdeclaration-responsibleai.com/

4 OECD, Artificial Intelligence in Society, OECD Publishing, 2019.

5 The excellent OECD report, Artificial Intelligence in Society (2019), for example, does not specifically discuss AI applications in insurance while focusing more on applications in financial services. But another OECD report was devoted to the topic: OECD, Technology and innovation in the insurance sector, 2017. https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf.

6 For example, see the definition by J. Kullmann, Lamy Assurances, Wolters Kluwer, 2017, p. 7: insurance is "l'opération par laquelle un assureur s'engage à exécuter une prestation au profit d'une autre personne en cas de réalisation d'un évènement aléatoire, le risque, en contrepartie de la perception d'une somme d'argent, la prime."

7 Contra: P. Thourot, J.-M. Nessi, K. Ametépé Folly. 2015. Big data et tarification de l'assurance, Risques, no. 103, p. 49.

8 V. E. Steiner, art. supra.

9 Nicholas B. Wainwright, "Philadelphia's Eighteenth-Century Fire Insurance Companies." Transactions of the American Philosophical Society, vol. 43, no. 1, 1953, pp. 247–252.

10 In France, it was only in early 19th century that insurance companies, insurance techniques and its experts, namely actuaries, came into being. The bottomry loan and the tontine were clearly the precursors to the creation of the first French insurance companies. R. Szramkiewicz et O. Descamps, Histoire du droit des affaires, LGDJ, 2nd ed., 2013, p. 316.

11 Sources: ACPR Banque de France. 2017. Les chiffres du marché français de la banque et de l'assurance; 2019 Facts of the Property and Casualty Insurance Industry in Canada; Journal de l'assurance, 2017; Fédération Française de l'assurance, 2017; Observatoire de l'évolution des métiers de l'assurance, 2018, Insurance Europe.

12 See Parletta, N. 2019. Artificial Intelligence Can Prevent Enormous Amounts Of Damage And Water Loss From Building Leaks. Forbes. https://www.forbes.com/sites/natalieparletta/2019/06/27/artificial-intelligence-can-prevent-enormous-amounts-of-damage-and-water-loss-from-building-leaks/#63181cd14861.

13 See for example the offering of Allianz Conduite Connectée, https://www.allianz.fr/assurance-auto/conduite-connectee/

14 CNIL. 2017. Véhicules connectés : un pack de conformité pour une utilisation responsable des données. https://www.cnil.fr/fr/vehicules-connectes-un-pack-de-conformite-pour-une-utilisation-responsable-des-donnees

15 Also, scoring applications have been designed to give insureds a rating that changes according to several criteria, including their behaviour. See Autorité de contrôle prudencielle et de résolution. 2018. Intelligence artificielle : enjeux pour le secteur financier, p. 14.

16 Ramnath Balasubramanian, Ari Libarikian, and Doug McElhaney predict the end of human interactions in the industry in 2030. See their article "Insurance 2030 — The impact of AI on the future of insurance", McKinsey, April 2018. https://www.mckinsey.com/industries/financial-services/our-insights/insurance-2030-the-impact-of-ai-on-the-future-of-insurance.

17 See the Tällt Ventures report, Insurtech Disruption Trends 2017. Artificial Intelligence, 2017.

18 In the area of loan insurance, for example, the AERAS agreement, introduced in 2007, facilitates access to insurance for people with, or who have had, a serious health problem. In 2017, of the 3.8 million applications for loan insurance for home and business loans, 14% were from people with an increased health risk, which did not allow them to obtain insurance under the normal terms of a contract. In the area of death insurance, for example, further studies showed that 72% of the applications eventually resulted in a contract with no additional premium and exclusion of coverage; in 28% of cases, coverage was offered with an additional premium and in less than 0.5% without additional premium but with exclusion or limitation of coverage. V. FFA, « Convention AERAS : 96% des demandes présentant un risque aggravé de santé ont reçu une proposition d'assurance de prêt en 2017 », December 17, 2018.

19 The history of insurance is much older, the principle of risk mutualization probably dates back to Roman antiquity. However, insurance contracts, which focused primarily on trade, were very similar to bank loans. Martin Boyer, « Une brève histoire des assurances au Moyen Âge », Assurances et gestion des risques, vol. 76(3), October 2008, 83-97.

20 This concept forms the core of the political liberalism that John Rawls systematized in A Theory of Justice (Cambridge MA, Harvard University Press, 1971); for a republican history of the concept, cf. also Jean-Fabien Spitz, Le moment républicain en France, Paris, Gallimard, 2005.

21 Léon Bourgeois, Solidarité, 3e édition, Paris, Colin, 1902; Colette Bec, La Sécurité sociale, une institution de la démocratie, Paris, Gallimard, Bibliothèque des sciences humaines, 2014.

22 Léon Bourgeois, op. cit.; François Ewald, L'État providence, 1986, Paris, Grasset.

23 Marie-Claude Blais, La solidarité. Histoire d'une idée, Paris, Gallimard, 2007.

24 Larry May, The Socially Responsive Self: Social Theory and Professional Ethics, University of Chicago Press, 1996.

25 This is reminiscent of Kant's duty of charity (English tr. Groundwork of the Metaphysics of Morals, Part 2, 1785).

26 One contemporary legal theorist who best expressed this idea of sharing and conceptualized social redistribution under the insurance model is American jurist Ronald Dworkin. Cf. Dworkin, Sovereign Virtue, Cambridge MA, Harvard University Press, 2000.

27 For an overview of the issue of actuarial fairness, see Landes, X. 2015. How Fair Is Actuarial Fairness? Journal of Business Ethics, Vol. 128, No. 3, pp. 519-533.

28 Philosopher Norman Daniels, Rawlsian in inspiration, was one of the most influential promoters of this idea. Among others, see, Daniels, N. 2007. Just health: Meeting health needs fairly, New York NY, Cambridge University Press.

29 Whitehead, M. and Dahlgren, G. 2006. Concepts and principles for tackling social inequities in health: Levelling up Part 1, Copenhagen, World Health Organization Regional Office for Europe.

30 This is the case for American insurer J. Hancock, which has decided to turn the page on "traditional insurance" and offer only "interactive" insurance policies. Insureds must wear "wearables", connected devices that provide the insurer with data on their physical activity, and recommendations to encourage them to adopt the behaviours set out by the insurer. See Enrique Dans, "Insurance, wearables and the future of healthcare", Forbes, 21 Sept. 2018; and Ana Senior, "John Hancock Leaves Traditional Life Insurance Model Behind to Incentivize Longer, Healthier Lives", Boston, 19 Sept. 2018, PRNewswire, John Hancock: https://www.johnhancock.com/news/insurance/2018/09/john-hancock-leaves-traditional-life-insurance-model-behind-to-incentivize-longer--healthier-lives.html

31 This was famously seen in an incident involving Target whose coupon allocation algorithms detected the pregnancy of a teenager based on her shopping habits before her parents found out about it. See Duhigg, C. 2012. Psst, You in Aisle 5, N.Y. Times.

32 Charpentier, A., Denuit, M. M. and Elie, R. 2015. Segmentation et Mutualisation, les deux faces d'une même pièce, Risques 103.

33 R. Karayan, « Quand la sélection médicale se fait plus discrète », l'Argus de l'assurance, 11 octobre 2019, p. 38 and following.

34 The literature on AI risks is extensive. From among over one hundred titles on this subject, Cathy O'Neil's book is worth mentioning: Weapons of Math Destruction. How Big Data Increases Inequality and Threaten Democracy, NY, Broadway Book, 2016.

35 See the story of a fiasco relating to the deployment of a welfare benefit algorithm in the U.S. state of Indiana in Virginia Eubanks' reference book, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor, NYC: St. Martin's Press, 2018. See also the criticism of the orientation algorithm for French lycée students in their final year, Parcoursup ("post-secondary path").

36 This is the conclusion reached by Arthur Charpentier, Michel M. Denuit and Romuald Elie (op. cit.).

37 R. Karayan, « Quand la sélection médicale se fait plus discrète », l'Argus de l'assurance, 11 octobre 2019, p. 38 and following.

38 Interview of B. Philippe in « Quand la sélection médicale se fait plus discrète », l'Argus de l'assurance, 11 octobre 2019, p. 38 and following.

39 See Daniel, J.-P. 2016. « Et si l'assurance disparaissait ? », Risques, n° 108.

40 The Montreal Declaration (2018), initiated by the Université de Montréal, is the product of a broad public and multi-stakeholder consultation. It is the most comprehensive ethical document to date. Cf. Berkman Klein Center. 2019. "Principled Artificial Intelligence." https://ai-hr.cyber.harvard.edu/primp-viz.html. The AI HLEG report is the most developed European proposal to date and was produced by a group of some 50 experts, mostly from the private sector; this report proposes an assessment list for a trustworthy deployment of AIS in the industrial sectors. The OECD Declaration offers five principles that are narrower in scope but have the advantage of enabling broad intergovernmental coordination. This is the only document signed by all OECD member states (thus by definition the G7) and adopted by the G20 member states; a total of 42 countries have adopted it (https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm)

41 In some countries, positive discrimination mechanisms are established by law. The term prohibited discrimination is therefore used here to refer to any distinction of a human group that leads to treating it worse than others or to putting it at a disadvantage, in contradiction with the laws in force.

42 The same phenomenon will be repeated in other industries if due care is not taken. For example, studies have shown that oncologists have a strong tendency not to rely on AI when AI comes to a diagnosis different from

their own, because they do not understand how this diagnosis was made. See for example: See, for example, Bloomberg, J. 2018. Don't Trust Artificial Intelligence? Time To Open The AI 'Black Box', Forbes, https://www.forbes.com/sites/jasonbloomberg/2018/09/16/dont-trust-artificial-intelligence-time-to-open-the-ai-black-box/#4771614d3b4a

43 Rudin, C. 2019. "Please Stop Explaining Black Box Models for High-Stakes Decisions and Use Interpretable Models Instead." Nature Machine Intelligence. Vol (1). pp. 206-215.

44 The higher the number of variables taken into account by a model, the more complex it is. The models used reflect this level of complexity, with the simplest (hence the most interpretable) design of linear models at one end and models using neural networks at the opposite end of the complexity spectrum. Hall, P. and Gill, N. 2018. An Introduction to Machine Learning Interpretability: An Applied Perspective on Fairness, Accountability, Transparency, and Explainable AI. O'Reilly.

45 However, the requirement for interpretability may vary depending on the various applications. For example, automated fraud detection systems may not have to work as transparently as others, as follow-ups will be performed to verify whether fraud has actually occurred. In other words, the need for explainability is not the same from one organizational process to another.

46 Defense Advanced Research Projects Agency

47 Recital 71, General Data Protection Regulation (GDPR). "The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. [...]"

48 See Safiya Umoja Noble, Algorithms of Oppression: How Search Engines Reinforce Racism, 2018.

49 Workplace training is a key pillar of the AI deployment strategy in France and Canada. See the third part of the French strategy in the Villani report, For a Meaningful Artificial Intelligence (2018): Anticipating and Controlling the Impacts on Jobs and Employment.

50 This is the essence of the groundbreaking CNIL report (2017), Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle.
https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de

51 The deployment of digital solutions has generally increased the number of disputes and triggered a sharp rise in mediation settlements. See Ethan Katsh, Orna Rabinovich-Einy, Digital Justice: Technology and the Internet of Disputes, Oxford: Oxford University Press, 2017.

52 Thaler, R.H. and Cass R. Sunstein, C.R. 2008. Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press.

53 See Greengard, S. 2015. The Internet of Things, MIT Press.

54 Warin, T., de Marcellis-Warin, N., Troadec, A., Sanger, W. and Nembot, B. 2014. Un état des lieux des données massives. Rapport Bourgogne, 2014RB-01, CIRANO.

55 See https://canadianinnovationspace.ca/wp-content/uploads/2018/05/IpsosCanadaNext_TrueNorth_May22.pdf

56 See Office of the Privacy Commissioner of Canada. 2019. 2018-19 Survey of Canadians on Privacy. https://priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

57 European Commission 2018. EU data protection rules. https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

58 Personal Information Protection and Electronic Documents Act (PIPEDA) / Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), 2000, https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

59 What data can we process and under which conditions? European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions

60 The Privacy Commissioner oversees application of the PIPEDA. When the Commissioner detects a breach, he or she can inform the public and make recommendations to Parliament, but his or her authority to draft legislation governing personal data extends no further.

61 Open data in France (https://www.data.gouv.fr/en/) and Canada (https://open.canada.ca/en/open-data)

62 Convention AERAS, 2019, http://www.aeras-infos.fr/cms/sites/aeras/accueil.html. According to the Convention AERAS, if a person has had cancer before the age of 18 and a five-year period without relapse has followed the remission of that cancer, that person is entitled not to disclose having had cancer to their insurer. People who have had cancer after the age of 18 must have a 10-year period without relapse.

63 Genetic Non-Discrimination Act / Loi sur la non-discrimination génétique. 2017. https://laws-lois.justice.gc.ca/PDF/G-2.5.pdf

64 The case will be heard by the Supreme Court in the coming months (2019 when this report was written).

65 This case will be heard shortly by the Supreme Court of Canada.

66 See Guilmain, A. 2018. Droit à l'oubli : deux solitudes entre le Québec et le Canada ? Droit-Inc, http://www.droit-inc.com/article21894--Droit-a-l-oubli-deux-solitudes-entre-le-Quebec-et-le-Canada

67 Charter of Human Rights and Freedoms, section 20.1 http://legisquebec.gouv.qc.ca/en/showdoc/cs/C-12

68 See Guilmain, A. 2018. Droit à l'oubli : deux solitudes entre le Québec et le Canada ? Droit-Inc, http://www.droit-inc.com/article21894--Droit-a-l-oubli-deux-solitudes-entre-le-Quebec-et-le-Canada

69 "AIS should help improve risk management and foster conditions for a society with a more equitable and mutual distribution of individual and collective risks." Montreal Declaration, p. 11

70 "AIS must avoid using acquired data to lock individuals into a user profile, fix their personal identity, or confine them to a filtering bubble, which would restrict and confine their possibilities for personal development — especially in fields such as education, justice, or business." Montreal Declaration, p. 14

71 Joly, Y., Dupras, C., Ngueng Feze, I. and Song, L. 2017. Genetic Discrimination in Québec – Policy Brief, Centre of Genomics and policy, http://www.genomequebec.com/DATA/PUBLICATION/32_en~v~Genetic_Discrimination_in_Quebec_-_Policy_Brief.pdf

72 In fact, significant disparities exist from one Canadian province to another. Each province has its own laws regarding the use of personal data. Alberta, Québec and British Columbia have laws substantially similar to PIPEDA on the use of personal data, while Ontario, New Brunswick, Newfoundland and Labrador and Nova Scotia have laws very similar to PIPEDA on health-related information.

73 Villani report. 2018. For a Meaningful Artificial Intelligence: Towards a French and European Strategy, 2018, p. 143

74 Some of the actions presented below are based on the content of the AI public sector governance report from the AI Now Institute at New York University. See Reisman, D., Schultz, J., Crawford, K et Whittaker, M. 2018. Algorithmic Impact Assessments: A Pratical Framework For Public Agency Accountability. https://ainowinstitute.org/aiareport2018.pdf

75 See https://canadianinnovationspace.ca/wp-content/uploads/2018/05/IpsosCanadaNext_TrueNorth_May22.pdf

76 See the Government of Canada's Algorithmic Impact Assessment, https://www.canada.ca/en/treasury-board-secretariat/corporate/news/algorithmi-impact-assessment.html

HUMAN TECHNOLOGY FOUNDATION

The Human Technology Foundation works to put people at the heart of disruptive technologies. Acting mainly through the OPTIC international research network, the Foundation helps public and private stakeholders manage the ethical challenges around innovation and related regulation. The Human Technology Institute–Montréal represents the Foundation in Québec and across Canada.

Report produced in partnership with:

OPTIC

INSTITUT DE LA TECHNOLOGIE POUR L'HUMAIN MONTREAL

t OpticTechno

i Optic Technology

f OpticTechnology

c optictechnology

http://optictechnology.org