FINAL THESIS IN

Data Protection Law

MAJOR IN

Law, Digital Innovation and Sustainability

A.I. TAXONOMY IN INSURANCE SECTOR

Author: Fabio Intonti
(630773)

Academic Year: 2022/2023

Supervisor: Prof. Filiberto Brozzetti
Co-Supervisor: Prof. Mariavittoria Catanzariti

LUISS

INDEX

0. Preface

This dissertation aims to investigate about the possible economic-legal and social consequences of the use of Artificial Intelligence algorithms in the European Insurance industry.

The idea for this project stems from the author's personal passion for economics and social psychology, combined with an internship opportunity at an IT consulting firm, where it was possible to observe the state of AI implementation in the Insurance industry.

A.I. TAXONOMY IN THE INSURANCE SECTOR

Law, Digital Innovation and Sustainability

Luiss Guido Carli University

LUISS

1. Sectorial Overview

The insurance industry falls within the broader context of the financial sector, where business is essentially based on maximizing profit and/or minimizing risk. Normally, only one of these two paths can be followed: maximizing profit by increasing riskiness or minimizing risk by decreasing profitability. Different companies operating in the same industry offer uniform profitability for the same risk. The introduction of artificial intelligence algorithms into the business model, however, can result in improved performance from many perspectives. It is possible to increase profitability by decreasing the risks taken by the enterprise. But let's take a step back and try to explain why the financial sector, specifically the insurance sector, was chosen as the object of investigation.

"The financial system is a complex set of credit and debt **relationships** of a dynamic and multi-relational type, built on a dense network of contractual ties that connect - through the direct channel of financial markets and the indirect channel of financial intermediaries - all the actors in the economic system. The **financial system feeds on information** (macroeconomic, including forecasting, socio-political, microeconomic, etc.), including non-public information, **and produces informatio**n (in terms of the prices of financial instruments traded in organized markets) necessary for economic agents to define their investment plans and strategies and, in a word, to make the economy in general function. It is precisely the uneven and asymmetrical distribution of information that occurs in reality that prompts traders to **seek out** (non-publicly available) **information** and pay for it in order to obtain extra profits from its exploitation."[1]

Here's the mystery revealed: in the financial sector, profitability is directly correlated with information’s exploitation. Thus, holding information and not exploiting it turns out to be inconvenient for business. Before the advent of Artificial Intelligence, relevant information was only that particular insight which a human agent could deem relevant to business. For years, the economic model in insurance sector was built based on balance sheets, returns on investment and other synthetic indicators that could forecast the company's future to financial (human) investors. With the advent of A.I., these synthetic indicators gradually lost relevance and were replaced by much more accurate and tailored models built on the specific business. Indeed, much information that previously appeared useless may encapsulate patterns invisible to the human eye. **Any information could potentially be relevant.**

The insurance industry consists of companies that offer insurance policies to their customers, who are usually individuals or legal entities. Insurance policies are **contracts between the insurer and the customer**, in which the customer pays a premium in exchange for a promise from the insurer to cover damages or financial losses caused by specific events. For example, a life insurance policy covers the risk of death of the insured, while a home insurance policy covers the risk of property damage caused by events such as fire or flood. Other forms of insurance include health, liability, automobile, and business insurance. Insurance companies use actuarial science and risk models to calculate the premium that customers must pay based on the risk of loss that the insurer must cover. The premium may be a fixed amount paid annually or fractionally, or it may be based on the frequency and severity of claims made by customers.

Insurance companies generate revenue through the premiums customers pay and by investing the money in financial assets such as stocks, bonds, and government securities. When a customer files a claim, the insurer evaluates the claim and decides whether or not to pay the required amount based on the terms of the insurance contract. In some cases, the insurer may ask the customer to pay a deductible or co-pay, which is a portion of the cost of repair or replacement that must be paid by the customer.

The insurance industry is regulated by supervisory authorities, such as the Istituto per la Vigilanza sulle Assicurazioni (IVASS) in Italy or the National Association of Insurance Commissioners (NAIC) in the United States, to ensure that insurance companies operate fairly and transparently and comply with local insurance regulations.

To give an idea of the economic size, the insurance sector represents an interesting portion of the financial system. Specifically, the insurance sector accounts for 7.9 percent of GDP in Italy (Source IVASS, 2021) The insurance penetration rate, as measured by the ratio of premiums to GDP, decreases from 8.1 percent in 2020 to 7.9 percent in 2021, also due to a more pronounced GDP recovery than premium income. There is also a reduction in Return on Equity (ROE) to 8.7 percent, nearly 3 percent lower than the previous year. In Italy, 90 domestic insurance companies, 4 representations of non-EEA companies operate and more than 237,000 insurance intermediaries (agents, brokers, etc..) are licensed. Companies paid out 76.3 billion euros to policyholders in life insurance and 19.8 billion against claims in non-life insurance, totaling 96.1 billion euros.

2. Challenge: the struggle for categorizing AI model and applications

2.1 Normative Gaps

From a regulatory perspective, insurance in Europe is subject to a series of rules and regulations designed to protect consumers and ensure the financial stability of the industry.

The European Union has expressed itself through the Solvency 2 Directive, establishing minimum capital requirements for insurance companies and imposing stringent limits on risk taking and management in order to maintain the stability of the financial sector. In addition, insurance companies must comply with transparency regulations, that is, they must provide clear and transparent information about the insurance products they offer and policy conditions. This measure is aimed at ensuring smoother control by the institutions in charge and, at the same time, ensuring adequate protections for consumers. Indeed, the European market is characterized by its focus on consumers, who are protected from several perspectives. First of all, consumers have the right to obtain assistance in case of need and to be able to formalize complaints in case of alleged injustice. Nevertheless, consumers' privacy and personal data are protected through Regulation 679/2019 (General Data Protection Regulation). This represents a key point in our discussion, as it is from the exploitation of personal data that an accurate profile can be extracted, and the customer portfolio broken down into increasingly precise clusters.

The information asymmetry is often favorable to the consumer: if an insurance penalty were to be received for every time the speed limit is exceeded, seat belt is not put on, apartment's door is forgotten to be locked and gas is left on when leaving, then the prize paid would be much more expensive. Consumers, therefore, find advantage in so-called **moral hazard**, that is, in engaging in conduct that potentially harms the other party without the latter being able to verify it. From a customer point of view, only favorable information is disclosed in order to obtain a positive rating evaluation and reduce the insurance prize. But **let us try to reverse the reasoning** and put ourselves in the shoes of the CEO of a large insurance company. In order to determine the level of riskiness of its client portfolio, it is important to have as much information as possible regarding the conduct of individual clients. Indeed, the ideal situation would be to perfectly know the potential losses that these customers will generate, determining the Customer Lifetime Value. Considering the information accuracy and depth required, the insurance company is interested in knowing whether the customer obeys traffic laws, is careful about his or her health, or is reckless. In the past, when the insurance company had a doubt that a customer was fraudulent, it would turn to private investigators. Private investigators help companies extract this information, but they certainly cannot violate the client's home or follow him all day long. What if, unknowingly, we had agreed to always carry a private investigator with us who observes our behavior constantly? Well, yes, this is what is happening today. All audiovisual information, messages, geographic location, and transactions are recorded through cell phones, through home security cameras, and by smart TV. Information that is often useless, but constantly captured by these devices that are designed to better understand the behavior of their human master in order to better serve them. In this section, we do not want to dwell on the possibilities of a cyber-attack that steals information without our knowledge. Rather, the goal is to understand how information that we ourselves agree to acquire is exploited.

Considering the GDPR, one of the regulatory pillars created to conduct the digital transition in a sustainable way, we can refer to one of the fundamental principles: purpose limitation.

Article 5 Regulation 679/2016 is below quoted:

> Personal data shall be:
>
> 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
> 2. collected for **specified**, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes […]

The purpose with which information is collected is to profile individuals in order to determine the aggregate risk level of the entire client portfolio to make short- and medium-term forecasts.

Since any information could be relevant to highlight patterns and correlations, it is very difficult to determine whether surveys and data collection are proportionate to the objective. When talking about proportionality of means, one must keep in mind the principle of data minimization expressed in Article 5(1)(c) GDPR in the context of Artificial Intelligence. The principle of data minimization is hardly applicable in pattern discovery or in forecasting. The principle of "data minimization" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. When we talk about Artificial Intelligence, we refer to a **bulimic** type of **technology**, which generates additional information from a smaller amount of input. But how are relevant and necessary data determined when it comes to personalizing risk? Is it really necessary to understand a person's behavior and/or emotional state, or is it just additional relevant data?

2.2 ANIA's Insights

To explore the positioning of Insurance companies on the implementation of Artificial Intelligence as business practice, an interview was conducted with representatives from ANIA (Associazione Nazionale Imprese Assicuratrici) in which was declared:

> "Insurance companies are not interested in excluding potential customers from protection. Artificial Intelligence is a tool that enables better the companies to personalize risk more precisely."

It is essential to establish that various safeguards exist to protect citizens, particularly in relation to basic insurance services like vehicle insurance. The use of blacklists to exclude individuals from basic insurance coverage is strictly prohibited. Instead of identifying and excluding high-risk individuals from an insurance company's portfolio, the role of Artificial Intelligence is to personalize risk policies and establish contracts with premiums that accurately reflect the level of risk involved. This process is subject to supervisory verification known as "**Verifica di Vigilanza**," which is conducted by IVASS (Istituto per la Vigilanza sulle Assicurazioni). The purpose of this verification is to **determine whether any changes in pricing are legitimate** or if they belong to discriminatory practices. For instance, darker-colored cars may be charged higher premiums than lighter-colored cars due to their reduced visibility at night, which statistically leads to a higher number of accidents. This correlation can be demonstrated and serves as a valid basis for adjusting the price of the insurance policy for the end customer. However, it is important to note that discrimination based on gender is not permissible. In the past, policies for men and women had different prices, primarily because women historically drove less. Despite the demonstrable correlation, this approach was deemed unconstitutional as it was solely based on gender. Consequently, policies aimed at a female audience had their prices adjusted upwards to rectify this illegitimate discrimination. Similarly, discrimination based on sexual orientation, political beliefs, or ethnicity is strictly prohibited in the insurance industry. However, discrimination based on the geographical location of the insured asset is permissible. For instance, insuring a scooter against theft in an area known for its high crime rate, the insurer can justify adjusting the price to account for the increased risk involved in that specific location. To summarize, some features can be taken into consideration during price's evaluation phase others are restricted by law.

The Artificial Intelligence's support for insurance company is a matter of recognizing personalized riskiness patterns. In doing so, <u>it should be included a limitation on input data so that an AI evaluation do not conflict with the same principles of fair evaluation that a human agent</u> is also required to apply. Accordingly, sensitive data such as gender, religion, and ethnicity should be excluded upstream during the training phase of Artificial Intelligence, when the algorithm learns the correlations present between the pairs of data (input and output) entered. Although it is possible to exclude such data during the AI's training phase, the correlations between input and output do not recognize the limits imposed by law. If there is a group of subjects that represents a pattern, it will be discovered by the software that is able to classify also unlabeled information. The information extraction power of AI is combined with the actuarial necessities o and used to forecast the next events that could possibly affect business finances.

For example, if both a human agent and an AI agent were asked to analyze reports of 100,000 crash incidents starting with the insurance contract of each customer involved, they would probably have figured out different patterns explaining the causes and likelihood of a customer's type of crash. AI agent discovers an important correlation: there is a group of subjects with a higher propensity to make a traffic accident claim. If the algorithm were explainable, it could make explicit the relevant factor that resulted in classification into a certain category, in our example the factor is hair length (labeled information taken from the photo on the driver's license given when signing the contract). This is because there is a small but relevant probability that long hair in front of the eyes will cause an accident. On the other hand, if the algorithm could not be explained all people with long hair would see the price of their policy increased and, at least statistically, it would be very difficult for an insurer to prove that discrimination was not made based on gender. An **informational imbalance** is created between the company, which has hidden reasons for making a particular choice, and the consumer, who is succumbed to the choice but is not able to understand for which reason the decision has been made. If hair length was the identified factor in this case, it is not hard to imagine that calligraphy while signing, and other biometric data could potentially become grounds for categorization in particular risk areas. In the previous example, also if AI developer had limited the input data by removing gender information. An illegitimate discrimination could still occur if classifiable elements, like hair length, indirectly reflect limited discrimination factors like gender, ethnicity, religious opinions. The major risk in an AI driven insurance company is the lack of transparency for decision made. The human or virtual insurer visualizes the customer directly sorted in his/her category and does not question why he/ she was so classified, because risk personalization is an activity delegated to the algorithm. It is in this way that hidden discriminations can take place, invisible as they are fragmented in geographic space and time, but still existing. Such discriminations are not necessarily aimed at customer exclusion but implicate a much more precise allocation of risk to the individual. Given the greater precision in risk allocation, the individuals who need the most protection will also be the ones who will have to pay the highest premium. According to the AI Act draft, this situation would be on the borderline between exploiting the vulnerabilities of a social group[2] and the principle of risk mutualization by which an insurance company operates. From the point of view of the Chief Executive Officer of an insurance company, it is entirely justifiable to understand the risks taken and how they are distributed across its portfolio. The insurance company use of the information captured directly from the relationship with the customer, physical or virtual. In addition, information is also captured from online databases. These databases are unlocked for a fee and generally contain data from users who have given consent for tracking while browsing. No one can accurately estimate the traces left by a data subject's online activities, and potentially every activity that takes place on or near the device can be tracked. A human agent can only handle a modest amount of data so, the selection phase must be based only on what the evaluator considers business-related, and the output correlations are often the result of long and difficult calculations. With Artificial Intelligence, this paradigm changes: **every piece of information tracked can contain an indication of the customer's value to that specific company.**

For instance, a 45-year-old man decides to take out life insurance. Rationally, we can assume that the insurance company will be interested in data about his health, whether he is a smoker and whether he is physically active, etc. However, there is another information on this particular man, he owns a dog. A correlation could be identified considering all the previous experiences on dog-owner costumers in the AI database: if the dog is healthy, the owner will also be more likely to be healthy. Here is where new information becomes important: how many times does the average owner take his puppy to the park during a day, how many visits does he make to the veterinarian annually? Information far from insurance logic can help draw an accurate picture of a person's behavior and maybe health status. If this correlation were verified or verifiable, would acquiring it be a right of the insurance company, considering the principle of purpose limitation expressed in Article 5 GDPR? It is very difficult to answer this question, and the regulatory ambiguity is outweighed by the operational univocity in which companies feed monstrous amounts of data, even generic or non-business-related data, to algorithms. These are the most profitable correlations, the ones that have not yet been discovered by competitors. In one of the companies investigated, a surprising correlation was discovered: the client retention rate is x2.5 times higher in clients who have relatives already insured with the same company. In practice, acquiring a client's family makes the portfolio much more stable, secure, and valuable. The marketing campaigns of the said company are already moving in that

[2] Vulnerable groups: These terms apply to groups of people who, due to factors normally considered beyond their control, do not have the same opportunities as other more fortunate groups in society. Ethnic minorities, migrants, people with disabilities, homeless people, drug addicts, lonely elderly people, and children very often face difficulties that lead to greater social exclusion, such as low levels of education, unemployment, or underemployment.

direction, mapping families and networks of intimate relationships and ranking them by their realizable value.

2.3 The legal need to categorize unique algorithms.

Before the advent of information technology, calculations and forecasts were formulated through years of experience and from the statistical skills of workers. Nowadays it is done differently: each department can benefit from an algorithm that automates the most repetitive tasks and is able to extract a business report. Each of these departments has specific needs and acquires information from different sources. Companies are evolving to approach a new business model that is totally different from the one they were designed with. Each department is headed by a manager who reports directly to the BoD. There is no collaboration between departments, and goals are generally pursued with different budgets and suppliers. Each department has developed algorithms of varying complexity, some of them are built in-house but, in most of the cases, there is an externalization to an IT company.

The most widely used category is Robotic Process Automation (RPA), which decreases the number of staff used in standardized, repetitive tasks. Each algorithm leverages different underlying technologies to achieve the output of the automated process. To give a practical example, let us imagine that we had a medium-sized accident in the suburbs of Rome. As a result of the accident the customer report minor injuries, but his car is damaged. It is possible to call a 24/7 toll-free number that puts the customer in contact with a virtual assistant: a human voice that asks where he is, his health condition, and whether he needs immediate medical assistance. Following our answers, the robot interprets the sound and translates it into commands:

1. it searches for the owner and the vehicle in the internal database; 2. it contacts the local roadside assistance provider; 3. it forward him the directions necessary to fulfill his contract.

Through a set of photos or a video to the vehicle, the customer has an expedited reimbursement procedure, as an AI identifies the damage, compares it with the latest available photos of the vehicle to avoid reimbursing pre-existing damage (anti-fraud check), searches starting with the vehicle model, and compares the prices of spare parts on the official list to estimate the actual damage. Within 15 minutes we receive roadside assistance and partial pre-reimbursement. An excellent service that has been made possible through RPA software using artificial intelligence components from different domains: the interpretation of the customer's communications is entrusted to a natural language processing NLP software, which can translate the sounds emitted into instructions to be forwarded; the planning & interaction with different agents component facilitates roadside assistance by sending a notification with instructions to selected providers; finally, thanks to computer vision, damage can be identified and a decision making algorithm dispenses the eventual reimbursement.

Now that we have explained how a software normally used by insurance companies works, it would be reductive to say that it is a technology that can be attributed to a certain category, such as NLP. Rather, it is a unique algorithm developed to specifically reach the need of the commissioning enterprise. As each insurance company decides to customize its service and differentiate itself, the combinations of technologies used can vary significantly between companies. This is why, during impact assessments on business, an auditor would need to break down the software into its primordial components, so as to identify what categories of risk each component intrinsically has that could fall on the entire ecosystem. In a large insurance company, the level of complexity is much greater than one might naively expect when looking at it from an outside eye. The commercial department works closely with the customer intelligence department to better understand the behavior of previous, current, and future customers. There is also the internal audit department, which makes sure that employees are loyal and compliant with company procedures. There is the anti-fraud department, the beating heart of new strategies for detecting hidden behavioral patterns. There is the Procurement department for service providers such as roadside assistance, or IT services. Each of these departments can benefit from better structuring of available information, generating predictions and decreasing uncertainty but they mainly operate compartmentalized. RPAs are developed for specifical processes of a department so each one has different and non-comparable features. The direction taken is to progressively integrate different tools into a digital agent able to support decision and help to run the company in the optimal way. Being able to categorize different application will be crucial if consumers have to choose among different AI-driven insurance companies.

2.4 Main problems preventing categorization.

As a relatively new concept, it is still difficult to clearly distinguish AI from other types of applications serving the enterprise. For the sake of convenience and consistency, we will consider the definition of AI proposed by the European Commission in 2019:

> “Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals.”

(European AI Strategy: EC Communication, Artificial Intelligence for Europe, 2018)

The definition proposed by the European Commission appears to be rather general, and strong doubts remain as to what degree of autonomy is discriminating in classifying software as AI. The lack of an objective measure extent the perimeter of the definition to all those applications that apply a minimum of data processing to achieve a specific result. This generates two types of problems.

The first problem is the compulsive inclusion of most data processing software, generating an overabundant information system compared to the objective of regulation.
The second problem is the costs incurred by companies for analysis and precautions taken to mitigate the risk of using AI. A big risk to the European market is represented by the fact that many firms may choose not to innovate because there are too many restrictions and administrative requirements.
The limitations generated by this definition can be overcome through the creation of a taxonomy based on objective characteristics. Such characteristics make it possible to immediately identify the AI's key points and provide an excellent synthetic starting point from which authorities, customers or investor can have a panoramic view. By identifying the structural characteristics of AI applications, IT developers and digital entrepreneurs will better understand the legal risks they face and possibly compare the best practice used to mitigate those risks.

In commercial AI applications, there is not technical standardization in the development stages. This means that different AI can be programmed in different languages and may be not comparable. More, not all AI applications include human in the loop principle and the cybersecurity measures are typically the result of a deal with a private Cybersecurity Firm. A second factor that makes the classification of AIs more complex is the specificity with which such software is developed. An advanced AI algorithm consists of software specialized in different domain that are combined and implemented. In fact, commercial applications are often the result of several pieces of automation dedicated to a specific task, which are integrated into a single application that manages an entire process or a phase of it. Finally, new technologies or models may be integrated after some time, and thus features must be updated periodically. It the following section the main factors preventing a common categorization will be analyzed:

- *Lack of technical standard during the A.I. developing phase*

There is no standard programming language with which AI is developed, although Python appears to be the most widely used. Each software therefore presents significant obstacles during the review phase. Not all developers are able to read those lines of code and identify possible errors or biases in the algorithm, as the programming language is different, and each software developer has his or her own specific training. It is therefore very difficult for a legal advisor-external to the development stage-to read, understand and explain a program developed by a third party. Even the national supervisory authorities have a shortage of adequate personnel for the technical-legal analysis of such tools, and we often defer to the common sense of the insurance company, which has information obligations to meet. Investigative power is difficult to apply, and one can only understand the extent of the impact after critical events have occurred. Moreover, there are no comparable and up-to-date safety standards; instead, there are principles of robustness and safety that must still be adhered to. In view of this, an AI taxonomy would not be sufficient to make such applications secure and usable but serves purely to contextualize them for the way they are designed. To ensure adequate security standards would require, at the very least, industry codes of conduct, developed bilaterally by insurance industry associations and techno-legal committees that can understand the needs of the industry and balance business and social interests.

- *A.I. combinations and Specificity of the purpose for which A.I. is created.*

The combination of software underlying commercial applications of artificial intelligence can be an obstacle to classification for several reasons. Artificial intelligence can be used in many different forms and with a wide range of objectives. For example, it could be used to understand how many fire accidents will occur in a neighborhood, to predict the number of thefts of a particular model of scooter, to select needed replacement parts, or to enable autonomous driving of vehicles. The purpose with which complex application is created justifies the inclusion of several underlying technologies that combine to achieve the goal. Artificial intelligence is often used in combination with other technologies, such as Big Data, IoT and Robotic. This can make classification even more complex because many applications may use a combination of these technologies, making it difficult to fit them into a generic class.

- *Rapid growth of extensions and integrations*

In addition, the field of Artificial Intelligence is constantly evolving, and new technologies and techniques are being developed and introduced on a regular basis. This raise the necessity to maintain an up-to-date and accurate classification, as artificial intelligence applications can evolve rapidly and become increasingly complex. Like a living organism, an AI application evolves, mutating and refining itself. Millions of years ago a reptile was classified as a fish, but it became reptilian over time, when its characteristics changed to the point where it became something new. Similarly, an AI that is created to handle a small task can expand over time to handle entire business processes or relationships between several related businesses. Thus, it is necessary to underline the fact that, to be representative, AI classification must be repeated and updated over time. It is possible to proceed with periodic updates taking into consideration the innovation propension of the company. Otherwise, whenever an extension is added to the application or one of its structural features changes, an update of the assessment and classification will be necessary.

To summarize, the classification of commercial Artificial Intelligence applications requires a comprehensive understanding of the technologies involved from different aspects like the type of data used, the level of security and transparency provided, and the stakeholders involved. Moreover, period updates are required to maintain the classification relevant.

3. Taxonomy Proposal

Classifying in a representative manner the huge varieties of Artificial Intelligence represents an important need for European policymakers. Artificial Intelligence will have an impact on all the main human activities and is considered a megatrend:

> "a major movement, pattern or trend emerging in the macroenvironment; an emerging force likely to have a significant impact on the kinds of products consumers will wish to buy in the foreseeable future[3]"

To facilitate the complex mission of classifying thousands of applications related to the financial sector, it is necessary to make use of tools that allow for an assessment as objective as possible, regarding the risks, impacts and, above all, the design by which the AI is implemented. **The aim of this study is the creation of a compliance tool, a Taxonomy of Artificial Intelligence, through which it is possible to identify the fundamental components that make up a complex AI application**. The Taxonomy should enable legal experts to contextualize AI applications and understand the technical and organizational requirements to enable a resilient operative model. Vice versa, through this taxonomy AI developers and entrepreneurs should be able to understand the legal and ethical consequences he/she faces, to take all reasonably necessary action during the developing phase. Specifically, six aspects have been considered as fundamental and are here mentioned:

- **A.** Type & Origin of Input Data
- **B.** Type of Learning
- **C.** Explainability
- **D.** Accountability
- **E.** Stakeholders involved
- **F.** Operational scope & features

These characteristics have been chosen because they reasonably and accurately represent the history and objective of a specific application of Artificial Intelligence. These six characteristics adequately address the needs of the European legislator and draw inspiration from the regulatory requirements outlined in the forthcoming AI Act. Clarity and user-friendliness of this taxonomy have been considered top priorities to enable a wide audience to have the necessary means to transform their

[3] Monsah business school https://www.monash.edu/business/marketing/marketing-dictionary/m/megatrend

operational business models innovatively and sustainably. The classification based on objective characteristics can be implemented with current evaluation methods that primarily focus on assessing impacts in case of incident or malfunctioning. Taking into consideration that the current assessment and rating methods rely predominantly on risk assessments, it is possible to ascertain that impact assessment is often subjective and variable, since the AI operational field is sometimes blurred. The purpose of this taxonomy can be summarized in the identification of structural features of sophisticated software, in order to provide an objective starting point for all those who will need to assess and mitigate risks. There is a huge quantity of commercial application and numerous possibilities to extend and implement new features to address complete an automated service delivery. AI has liquid characteristics that combine several previously separate streams of computer science, in order to create synergies between departments that deliver different output. It is for this reason that the proposed classification should be interpreted as a decomposition into prime factors in which AI is the resultant of various basic components that constitute it. The presence of a certain feature does not exclude the co-presence of another feature since it is a liquid technology that combine different components. With this in mind, the proposed definitions are only a starting point for classifying the AI support tools used in insurance sector. This Taxonomy can be enhanced by adding new techniques, practices and definitions that will be developed in upcoming years. By conferring comparable classifications, it will be possible to create an industry code of conduct on the responsible use of AI in Insurance sector, enhancing the ability to learn from mistakes and solutions already experienced by others in situations that can be considered “similar”, since the underlaying technologies have comparable points in common.

A. Type and Origin of Input Data (Trustworthy AI Principle)

A.1 Data Typology: the type of input data is a relevant factor in the classification of the AI algorithm as it allows us to understand the information ground through which the machine is trained and identify possible violations of the principle of human dignity. Where personal or sensitive data are being analyzed, more care will need to be taken in reviewing the inputs and minimizing possible cognitive biases as the evaluations may be apt to classify humans into categories. There are different types of data on which specific regulations apply, and different classes of data are often used simultaneously to achieve the technical goal of AI. The following are the most common types of existing data:

A.1.1 Personal Data: Personal data is information that identifies or makes identifiable, directly or indirectly, a natural person and can provide information about his or her characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc. They can be divided into:

- ☐ **Data that allow direct identification**-such as biographical data (for example: first and last name), pictures, etc. - and **data that allow indirect identification**-such as an identification number (e.g., social security number, IP address, license plate number). With the evolution of new technologies, other personal data have taken on a significant role, such as those related to electronic communications (via the Internet or telephone) and those that enable geolocation, providing information about places frequented and movements.
- ☐ **Data falling into special categories**: these are the so-called "**sensitive**" data, i.e., those revealing racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, relating to health or sexual life. Regulation (EU) 2016/679 (Article 9) also included genetic data, biometric data, and data relating to sexual orientation.
- ☐ **Data relating to criminal convictions and offenses**: these are the so-called "judicial" data, i.e., those that may reveal the existence of certain judicial measures subject to registration in the criminal record (e.g., final criminal convictions, conditional release, prohibition, or obligation to stay, alternative measures to detention) or the classification of suspect. Regulation (EU) 2016/679 (Article 10) includes in this notion data relating to criminal convictions and offenses or related security measures.
- ☐ **Non-sensitive Data**: Non-sensitive data is personal information that is not considered sensitive and does not require special protection under privacy laws. This data may include information such as name, e-mail address, residential address, telephone number, and age. This data may be used by organizations for marketing purposes, to send newsletters, to conduct market research, or to handle business transactions. Organizations that collect and use non-sensitive data are still required to comply with privacy regulations and provide appropriate security measures to protect such data from loss, theft or unauthorized access. In addition, some data may be considered sensitive only in certain contexts or in combination with other data. For example, age may not be sensitive data by itself, but when combined with other personal information, such as address or occupation, it could become personal data since is able to identify a specific subject.

A.1.2. Anonymized: this is data that has been anonymized, i.e., it is not possible to trace the identity of the data subject who owns the data

A.1.3. Pseudonymized: pseudonymized data represent a low level of security in that it is possible to reconstruct and trace the identity of the data subject. Such data can only be used for internal analysis purposes unless there is explicit consent from the data subject.

A.1.4. Aggregates: Aggregate data are obtained when the reference unit is an aggregate i.e., data are collected in a particular spatial area (e.g., individuals at the municipal, regional, etc. level).

A.1.5. Synthetic Data: Synthetic data are data artificially generated or created by algorithms or software, rather than collected from real sources such as human experience or sensors. These data are used in various contexts, such as training artificial intelligence and machine learning algorithms, verifying algorithms or software, and simulating scenarios.

A.2. Data Origin: Data origin is correlated with the quality of the input. It is not possible to build an efficient AI model from incorrect or inaccurate data. Therefore, the way such data is obtained becomes an indicator of model reliability and is a structural feature of the AI algorithm. There are various ways to obtain data for free or for a fee, and for some of them, such as sensitive data, it will be necessary to meet vendor selection requirements or to comply with specific regulations.

A.2.1. Internal Source: data from internal sources such as databases, client files or insurance contracts are generally authorized and fairly accurate. They were collected for business-related purposes and can be freely used for internal purposes. However, there are limits regarding the dangerousness of the activities carried out with this data and they cannot be disclosed to third parties without the explicit consent of the data subject.

A.2.2. External Source: data from external sources may be inaccurate, old or even unauthorized. Such data is the foundation on which the model is developed and is an inherent alert parameter to classify an AI. External sources can be divided into:

- ☐ **Institutional Sources:** institutional sources (e.g., Eurostat, ISTAT) provide aggregated, anonymized data that can be used for static and general research purposes. This data is open and usable by anyone who requests it.
- ☐ **Authorized Sources:** authorized sources are private companies often referred to as data warehouses that specifically collect and process data on behalf of third parties. Is possible to request specific data on a topic under analysis. Data warehouses handle data by virtue of the consent to process received from the data subject when browsing or in other situations. There are no guarantees about the quality of the data, and, for this reason, the choice of provider becomes a relevant and incidental factor in risk assessment.

- **Unauthorized sources:** unauthorized sources can be traced to all those entities that release data in the absence of consent for processing by a subject. Such sources provide no guarantee as to the accuracy of the data, the legitimacy to use it, and the safety of the result.

B. Learning type:

Learning type is a determining factor in the classification of an artificial intelligence because it determines the modus operandi by which the machine is trained. It gives an insight on the labelling procedure, on outliers' detection and on bias recognition during the training phase. Currently, artificial intelligence learning models are conventionally divided into three main categories (Supervised, Reinforced, and Unsupervised) but there are new models that are worthy of mention so have been included in the list:

B.1. Supervised: Supervised learning is a method in which the AI model is trained on a corresponding set of input and output data. The developer labels accurately each parameter and gives feedback on the output (prediction or classification) generated. This is the model that guarantee the major human involvement during the training phase and improves the accuracy of the model. This type of learning is particularly useful for data classification, as it allows for the accurate and consistent identification of different categories of input objects or data.

B.2. Reinforced: Reinforcement learning is a subfield of machine learning where an AI algorithm learns to make decisions by interacting with an environment, generally with a human agent. Every time that the foresight or the classification model is correct, the human agent provides a reward. In reinforcement learning, the algorithm learns to maximize a numerical reward signal provided by the environment. The software learns to take actions that lead to higher rewards and avoid actions that lead to lower rewards.

B.3. Unsupervised: Unsupervised learning is a machine learning technique that involves providing the computer system with a set of inputs and outputs (system experience) that it will reclassify and organize based on common features to try to make reasoning and predictions about subsequent inputs. In contrast to supervised learning, only unannotated examples are provided to the algorithm during learning, since the classes are not known a priori but must be learned automatically.

B.4 Semi-Supervised Learning: This approach combines elements of supervised and unsupervised learning. It uses a small amount of labeled data along with a larger set of unlabeled data for training. The labeled data helps guide the learning process, while the unlabeled data aids in discovering underlying structures.

B.5 Bayesian Learning: Bayesian learning incorporates prior knowledge and uses Bayesian inference to update assumptions based on new evidence. It combines prior probabilities with observed data to make probabilistic predictions and estimates.

B.6 Instance-Based Learning: Instance-based learning, also known as lazy learning, focuses on storing and comparing training instances to make predictions on new instances. It relies on similarity measures between instances and uses the closest instances to make predictions.

B.7 Online Learning: Online learning, or incremental learning, involves updating the model continuously as new data arrives. It adapts to changing environments and makes predictions in real-time. Online learning is well-suited for scenarios where data streams continuously and require immediate model updates.

B.8 Artificial Neural Network: Artificial neural networks are a class of machine learning models inspired by the structure and functioning of neurons in the human brain. ANN is composed of a set of interconnected nodes, called neurons, that process input data and produce an output. ANN can be trained using supervised or unsupervised learning algorithms to learn to recognize patterns in the input data and use them to make predictions or decisions.

- **Deep Learning:** Deep learning is a machine learning technique that uses multilayered artificial neural networks to process information. These networks can be very deep, that is, composed of dozens or even hundreds of layers of neurons, and are capable of learning complex representations of input data. Deep learning has achieved outstanding results in many artificial intelligence applications, such as speech recognition, computer vision, and text recognition.

B.9 Transfer Learning: Transfer learning involves utilizing knowledge gained from one task to improve performance on another related task. The pre-trained model's knowledge is transferred to a new task, reducing the need for large amounts of task-specific training data.

B.10 Ensemble Learning: Ensemble learning combines multiple individual models to create a more powerful model. It leverages the diversity of individual models to improve prediction accuracy and robustness. Popular ensemble techniques include bagging, boosting, and stacking. Ensemble learning can be divided into three fundamental techniques:

- **Bagging:** This technique aims to create a set of classifiers with equal importance. During the classification process, each model will vote on the prediction outcome, and the overall output will be the class that receives the highest number of votes.

- **Boosting:** Unlike bagging, each classifier influences the final voting with a certain weight. This weight is calculated based on the accuracy error that each model commits during the learning phase.
- **Stacking:** While in bagging the output was the result of voting, stacking introduces an additional classifier (called a meta-classifier) that utilizes the predictions of other sub-models to undergo further learning.

C.1. Explainability (Trustworthy AI Principle) :

Explainability in AI refers to the ability to understand how an AI system makes decisions or recommendations. It means that the decision-making process of the AI system is clear and can be explained to the end-users or stakeholders:

C.1.1. Explainable Algorithms: The explainability of the algorithm should ensure that we know the exact reasons why we see one type of output and not another. An explainable algorithm allows one to find correlations between pairs of inputs and outputs by assigning weight to different factors that explain the relationship. It is then possible to understand which factor is considered determinant, which is uncorrelated.

- **Explainable AI (XAI):** This refers to the development of AI systems that can explain their reasoning and decision-making processes to human users in a way that is understandable and meaningful. This can involve visualizations, natural language explanations, or other methods to make the decision-making process more transparent.
- **Open and accessible algorithms**: This involves making the data and algorithms used by the AI system available to external reviewers or auditors. This enables external parties to verify the accuracy and fairness of the system.

C.1.2. Black Box Algorithms: A black box algorithm is an algorithm or system that operates using input and output, but the internal workings of which are not transparent or explainable. In other words, the user can observe what goes into the algorithm and what comes out, but the user does not have a clear understanding of how the algorithm arrived at its output or decision. Black box algorithms are often used in complex systems, such as deep neural networks, where the internal workings of the algorithm are highly complex and difficult to understand. In such cases, the algorithm may learn patterns or features in the data that are not immediately apparent to humans, making it difficult to explain how it arrived at its decisions. While black box algorithms can be highly effective in certain contexts, such as image or speech recognition, they can also present challenges in terms of accountability, fairness, and bias. Because the decision-making process of a black box algorithm is not transparent, it can be difficult to identify and address errors or biases in the system. A black box algorithm poses the necessity of additional safeguards measures on the data quality management and on the effectiveness and reversibility of the decision.

There are also several factors that influence the transparency of an algorithm and allow a human agent to read and understand the reasons why the AI generated a specific output. Some Insurance companies provides ethics and governance guidelines. This involves establishing clear **ethical guidelines and governance frameworks for the development and deployment of AI** systems. It can include considerations around bias, privacy, and accountability. Codes of conduct adherence and governance guidelines do not represent a structural feature of AI. These support tools rather represent a choice made by the private firm that pose standards and additional protection to ethical principles during the development of new algorithms. For this reason, the presence of ethical guidelines and governance frameworks is considered a tool to be taken into account during the risk assessment phase, rather than during the classification phase of an AI. Overall, transparency in AI is an essential aspect of responsible AI development and deployment, as it helps to ensure that AI systems are used in a fair, ethical, and accountable manner.

D. Accountability (Trustworthy AI principle):

Accountability represents a key parameter when an AI must be identified within an organizational context. Identifying the person responsible for the process represents an indicator of the control applied to the output generated by the machine and is a form of protection toward those on whom the effects generated by the algorithm fall back. In situations where an AI makes decisions for several actors simultaneously, identifying a person responsible for the transformation from recommendation to decision is a significant variable to consider. In any case, **name and address of the provider** should be collected to give a fast comparison among different AI providers that have a positive/negative history or weak security systems. In addiction there could be the possibility to have human oversight in the process or, on the other hand, delegate the decision to the algorithm:

D.1. Human in the loop: "Human-in-the-loop" (HITL) refers to a type of artificial intelligence (AI) system design where human input is integrated into the AI decision-making process. In this approach, human oversight is used to monitor and guide the AI system's actions, rather than relying solely on automated algorithms. The HITL approach is often used in situations where the consequences of AI errors are high or where it is difficult for AI to perform optimally due to complex or ambiguous situations. By incorporating human feedback and decision-making, HITL can help improve the accuracy and reliability of AI systems[4]. HITL represents a hybrid approach to AI development that leverages the strengths of both human and machine intelligence to achieve more accurate and reliable results. In particular, a human agent should be able to

- "Fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation, so that signs of anomalies, dysfunctions and unexpected performance can be detected and addressed as soon as possible" [art.14, 4(a) AI Act Draft]
- "Be able to decide, in any particular situation, not to use the high-risk AI system or otherwise disregard, override or reverse the output of the high-risk AI system;" [art.14, 4(d) AI Act Draft]

D.2. Human out of the loop refers to a type of AI system design where human input is completely removed from the decision-making process. In this approach, AI systems operate autonomously without any human oversight or intervention. This approach is often used in situations where speed and efficiency are critical, such as in high-frequency trading or automated customer service. However, there are also risks associated with removing humans from the loop, particularly when it comes to safety-critical systems or decisions with potentially significant social impacts.

[4] One example of HITL is in image recognition tasks, where AI systems may not always correctly identify objects or people in an image. In this case, a human operator could review the AI system's output and correct any errors or ambiguities. Another example is in autonomous vehicles, where human drivers may be required to take over in certain situations, such as navigating unfamiliar road conditions or dealing with unexpected obstacles.

E. Stakeholders Involved:

Recipients and stakeholders are an aspect to be taken into consideration when classifying AI algorithms. In fact, there are regulations that bund and protect employees, consumers, and third parties differently. By identifying the stakeholders involved, key characteristics can be assigned that affect the interface design, scope of application, and legal compliance measures. Stakeholders are individuals, groups, or organizations that have an interest or concern in a particular project, program, or company. There are several types of stakeholders relevant for a classification, including:

E.1. Internal stakeholders: These are stakeholders who are directly involved in the day-to-day operations of a company, such as employees, shareholders, and managers. They have a vested interest in the success of the company and are affected by its decisions and outcomes.

- **Shareholders:** A shareholder is a person, company, or organization that owns one or more shares of stock in a corporation. Shareholders are considered partial owners of the company and are entitled to a portion of the company's profits in the form of dividends. They also have the right to vote on important company decisions, such as electing the board of directors and approving major changes in the company's structure or strategy. Shareholders can be both individual and institutional investors, and the number of shares they hold determines their level of ownership and influence in the company. Shareholders' interests are generally aligned with the success of the company, as they stand to gain financially from its growth and profitability.
- **Managers:** A manager is a person responsible for planning, organizing, directing, and controlling the resources (including people, finances, materials, and equipment) of an organization to achieve its goals and objectives. Managers typically oversee a team or department and are accountable for the performance and results of that unit. They are responsible for making decisions, allocating resources, setting and achieving goals, and managing the daily operations of the organization.
- **Employees:** An employee is a person who is hired to work for a company, organization, or individual in exchange for compensation. The employee performs work under the direction and control of the employer and is typically subject to the employer's policies and procedures. Employees can be full-time, part-time, or temporary and can work in a variety of roles and industries. They are entitled to certain rights and benefits, such as minimum wage, overtime pay, workers' compensation, and protection from discrimination and harassment. The employer is responsible for providing a safe and

healthy work environment and cannot exercise an excessive control over the performance in accordance with applicable laws and regulations.

E.2. External stakeholders: These are stakeholders who are not directly involved in the day-to-day operations of a company but are affected by its decisions and outcomes. External stakeholders can include customers, suppliers, regulators, and the local community.

- **Customers**: A customer is a person or organization that purchases goods or services from a business with the intention of satisfying a need or desire. Clients are protected by protections related to privacy and consumer rights. Special attention must be paid to possible behavioral manipulations or classifications contrary to consumer protection and human dignity standards.
- **Suppliers:** A supplier is a person, company, or organization that provides goods or services to another company or organization. Suppliers are typically businesses that specialize in producing or sourcing products or materials, which are then sold to customers or other businesses. AI recruiting software CV screenings can for instance substitute HR in the selection of employees and suppliers, with effect on the resilience of the business.
- **Public Administration and Government**: The relationship between public administration and insurance companies involves regulation, oversight, and collaboration. Public administration agencies regulate and enforce laws to ensure fair practices and consumer protection in the insurance industry. They also oversee insurance companies' compliance with regulations and monitor their financial stability. Collaboration occurs in areas such as risk management, disaster preparedness, and social welfare, where insurance companies work with public administration agencies to address public needs and mitigate risks. Overall, the goal is to ensure the fair and efficient functioning of the insurance industry while protecting policyholders and serving the public interest.
- **Third parties:** There may be other stakeholders involved, such as industry associations, reinsurer, intermediaries or the media. These stakeholders have been identified as residual categories but may be included in the classification if necessary.

A. Operational scope & Features:

The operational scope and features of AI aim to represent the domain of application and the peculiar characteristics of a specific AI. Artificial Intelligence is used to increase the knowledge of a phenomenon, but there are several related domains and implications. For this reason, we wanted to identify 4 categories (Reasoning & Decision Making, Perception, Learning & Classification and Robotics), composed of different underlying models, with different technical and legal considerations:

F.1 Reasoning and Decision Making: reasoning and decision-making applications are widespread in many fields and contribute to improving the efficiency and effectiveness of human activities. They are used in various fields such as business decision support, investment and strategy. An extension of this branch of artificial intelligence makes it possible to predict diagnoses following an accident, the possible outcome of legal litigation, and optimally manage the risk assumed by the insurance company. Typically, human oversight is required on such decisions since they can cause permanent effects on the legal or even the moral sphere of the person subjected to the decision.

F.1.1 Decisional Support System (DSS): Computer-based application that collects, organizes, and analyzes business data to facilitate quality business decision making for management, operations, and planning

- ☐ **Healthcare Decision Support Systems**: These systems assist healthcare professionals in diagnosing diseases, prescribing treatments, and making clinical decisions based on patient data and medical knowledge. This can be extremely important while forecasting the expected reimbursement for a crash or an injury.
- ☐ **Financial Decision Support Systems:** These systems aid financial analysts, investors, and business managers in making investment decisions, assessing risks, managing portfolios, and conducting financial analysis.
- ☐ **Supply Chain Management Decision Support Systems:** These systems assist in optimizing supply chain operations by providing insights and recommendations regarding inventory management, demand forecasting, logistics, and procurement.
- ☐ **Marketing Decision Support Systems:** These systems help marketing professionals in market research, customer segmentation, campaign planning, pricing strategies, and customer relationship management.

- **Human Resources Decision Support Systems:** These systems assist HR professionals in recruitment, employee performance evaluation, training and development, succession planning, and workforce management.
- **Legal Decision Support Systems**: These systems aid legal professionals in legal research, case management, document analysis, and providing recommendations based on legal precedents and regulations.
- **Transportation Decision Support Systems:** These systems help transportation planners and operators in route optimization, traffic management, fleet scheduling, and logistics planning.
- **Customer Relationship Management (CRM) Decision Support Systems**: These systems support sales and marketing teams in customer segmentation, lead management, sales forecasting, and customer satisfaction analysis.
- **Sales and Revenue Forecasting Systems:** These systems use historical sales data, market trends, and statistical modeling techniques to provide accurate sales forecasts and revenue projections.
- **Strategic Decision Support Systems:** These systems aid top-level executives in strategic planning, scenario analysis, business intelligence, and performance measurement for informed decision-making.
- **Compliance Decision Support Systems:** These systems help organizations ensure compliance with legal and regulatory requirements by providing real-time monitoring, analysis, and decision support for compliance-related activities.
- **Sensitivity Analysis (What if):** Method for determining the robustness of an assessment by examining which results may be affected by changes in methods, models, values of unmeasured variables, or assumptions.
- **Data Visualization**: Process of translating data into graphs and other visual elements, the presentation of quantitative information in visualization, the practice of translating information into a visual context
- **Expert system (ES):** A computer system that emulates the decision-making ability of a human expert. They are designed to solve complex problems by reasoning through bodies of knowledge, represented primarily as if-then rules rather than through conventional procedural code.
- **Optimization Models:** Translation of the fundamental characteristics of the business problem being attempted to solve. The model consists of three elements: the objective function, the decision variables, and the business constraints.

The list above provides a broad overview of the diverse applications of Decision Support Systems in different domains. These are just a few examples of decision support system applications, and the field continues to evolve with the integration of emerging technologies like Artificial Intelligence and machine learning. It's important to note that Decision Support System applications can be personalized on specific industry needs and organizational requirements.

F.1.2. Business Intelligence (BI): Automation of business processes and communications between two or more organizations

- ☐ **Customer Analytics**: BI enables businesses to analyze customer data, segment customers based on various attributes, and gain a deeper understanding of customer preferences, needs, and buying patterns. This information can be used to personalize marketing efforts, improve customer satisfaction, and drive customer loyalty.
    - **Churn Model:** Allows the identification of customer leaving intentions and extract the retention rate. It allows early intervention with appropriate actions, improving the company's ability to retain customers and stemming potential losses.
- ☐ **Financial Performance Management:** BI tools help organizations monitor financial performance by analyzing key financial indicators, such as revenue, profitability, cash flow, and expenses. It facilitates budgeting, forecasting, and financial planning to support strategic decision-making.
- ☐ **Operational Efficiency Analysis:** BI enables organizations to analyze operational data and identify areas for process improvement and cost reduction. It provides insights into production efficiency, resource utilization, and operational bottlenecks, helping businesses enhance operational effectiveness.
- ☐ **Marketing Campaign Analysis:** BI helps evaluate the effectiveness of marketing campaigns by analyzing campaign data, measuring ROI, and identifying the most successful channels and strategies. It aids in optimizing marketing efforts and allocating resources to maximize campaign outcomes.
- ☐ **Risk Management and Fraud Detection:** BI tools can analyze large volumes of data to identify patterns and anomalies that indicate potential risks or fraudulent activities. It supports proactive risk management, fraud detection, and compliance monitoring in various industries.

- **Human Resources Analytics**: BI assists in analyzing HR data, such as employee performance, retention, and recruitment metrics. It helps organizations optimize workforce planning, identify skill gaps, and improve talent management strategies.
- **Competitive Intelligence:** BI enables businesses to gather and analyze data on competitors, market trends, and industry benchmarks. It provides insights for strategic decision-making, market positioning, and staying ahead of the competition.
- **Executive Dashboards and Reporting:** BI tools provide real-time dashboards and reports for executives and decision-makers to monitor key performance indicators (KPIs) and track business metrics. It facilitates data-driven decision-making by presenting information in a visually appealing and easily digestible format.
- **Extract, transform, Load (ETL) tools** for extracting, transforming, and loading data: ETL tools enable data integration strategies, allowing companies to collect data from multiple sources and consolidate it into one centralized location. ETL tools also allow different types of data to work together.
- **Data warehouse and data mart** for archiving and warehousing: A data warehouse centralizes and consolidates large amounts of data from multiple sources. Its analytical capabilities enable organizations to derive important business insights from their data to improve decision making. Over time, it creates a historical record that can be valuable to data scientists and business analysts. With these capabilities, a data warehouse can be considered a single reliable source of business data.
- **Data mining**: Identification of information of various kinds (not known a priori) by targeted mining from large, single, or multiple databases. Complex extraction of implicit, previously unknown, and potentially useful information from data and the exploration and analysis, by means of automated and semiautomated systems, of large amounts of data in order to discover meaningful patterns.
- **Document warehouse & Document storage:** Software framework for analyzing, sharing, and reusing unstructured data, such as textual or multimedia documents.
- **OLAP (Online Analytical Processing):** OLAP methodology is part of business intelligence, the corporate ability to derive useful information from the data at hand with specific tools. Specifically, OLAP was created to speed up the process of reading, analyzing, and retrieving data through a different structure and organization of databases. In standard databases, data are stored in the form of two-dimensional spreadsheets and tables, which are not suitable for multi-dimensional

analysis: OLAP databases use cubes instead of tables, calculation structures in three or more dimensions instead of 2D.

F.2. Perception: In Artificial Intelligence, perception refers to the ability of a system to process and interpret sensory input data, such as images, sounds or other signals, to acquire information about the external world. Perception is a fundamental step in many artificial intelligence systems, such as those used in computer vision, speech recognition and robotics.

F.2.1 Semantics: In artificial intelligence, semantics refers to the ability of a system to process the meaning of natural language or other symbols, such as graphics and images. Semantics is a fundamental aspect of natural language understanding, as it enables systems to understand the meaning of texts and sentences, not just their syntactic structure.

- **Natural Language Processing** : is the general term used to explain the entire process of converting text into structured data. It processes spoken words or written texts, breaking them down into smaller elements that can be analyzed.
  - **Speech recognition:** also known as automatic speech recognition (ASR), computer speech recognition, or speech-to-text, is a capability which enables a program to process human speech into a written format.
  - **OCR software**: Optical character recognition (OCR) is the process that converts a text image into a machine-readable text format. For example, if you scan a form or receipt, the computer saves the scan as an image file, translates the symbols into characters, and extracts the content.
- **Natural Language Understanding**: is a component of NLP, which "teaches" machines the meaning of a portion of spoken speech or written text. It uses artificial intelligence to recognize linguistic features such as semantics, context, and intention. It allows machines to understand nuances and variations in a language. Through NLU, machines can recognize the many ways people say the same thing.
  - **Chatbot:** Software that simulates and processes human conversations (written or spoken), enabling users to interact with digital devices as if they were communicating with a real person. Chatbots can be as simple as rudimentary programs that respond to a simple query with a single line or as sophisticated as digital assistants that learn and evolve to provide increasing levels of personalization when collecting and processing information.

- **Robo advisors:** Algorithms that provide insurance advice in an automated manner, without any human intervention, consistent with the client's characteristics and goals.

F.2.2. Computer Vision: Computer vision is a field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos, and other visual input-and take actions or formulate alerts based on that information.

- **Image Segmentation:** The process of classifying each image pixel to a class.
- **Object recognition:** Ability to find a particular object in a sequence of images or videos. Insurance companies are more interested in damages recognition to estimate the value of the loss, preventing frauds and boosting reimbursement.
- **Facial Recognition:** Facial analysis software identifies or confirms the identity of a person based on the face. It works by identifying and measuring facial features in an image. Facial recognition can identify human faces in images or videos, determine whether the face in two images belongs to the same person, or search for a face in a large collection of existing images. Biometric security systems use facial recognition to uniquely identify people during onboarding or user logins, as well as to reinforce user authentication activities. Mobile and personal devices also commonly use face analysis technology for device security. Having such a feature means dealing with sensitive data and comply to more strict regulation.

F.3. Learning & Classification: The operational scope of learning and classification has not been included in the overarching category of reasoning and decision making, as the discovered patterns generally serve as decision support. However, it is also possible for the learning algorithm to be used solely for exploratory and research purposes, without directly influencing or making operational decisions. The fundamental characteristic of this operational domain is the underlying approach to research, which also serves as an indicator of AI explainability. Machine learning-based models are generally more explainable compared to deep learning-based models.

F.3.1. Machine Learning: Machine Learning can be understood as a subfield of AI that encompasses the utilization of algorithms and techniques to facilitate autonomous learning and data-driven decision-making processes. It involves the collection, processing, and analysis of large datasets, as well as the development of models and algorithms that enable systems to adapt and improve their performance over time. In the legal context, the use of Machine Learning algorithms raises important considerations regarding data privacy, transparency, fairness, and accountability. Issues such as data protection, bias mitigation, explainability, and the potential impact on individual rights and freedoms must be carefully addressed when deploying machine learning systems in various sectors, including but not limited to finance, healthcare, and law enforcement.

- **Inferential Approach:** A procedure whereby the characteristics of a population are induced from the observation of a part of it (called a "sample"), usually selected through an experiment.
- **Statistical Approach**: Approach based on a small amount of sample data on which assumptions generated from past demand periods are made. Such models, in order to find a solution, prefer a smaller amount of data, repeatable and linear, in contexts where the relationships between them prove to be relatively stable.
- **General Linear Model (GLM and Simple Regression**): A compact method for writing several multiple linear regression models simultaneously. In this sense, it is not a separate linear statistical model.
- **Monte Carlo:** A mathematical technique used to estimate the possible outcomes of an uncertain event. It also provides several advantages over predictive models with fixed inputs, such as the ability to conduct sensitivity analysis or calculate input correlation. Sensitivity analysis allows decision makers to see the impact of individual inputs on a specific outcome, and correlation allows them to understand the relationships between any input variable.
- **Random Forest:** A random forest model in artificial intelligence is an ensemble learning method that combines multiple decision trees to make predictions or classifications. It is a supervised learning algorithm used for both regression and classification tasks. In a random forest, a collection of decision trees is created, where each tree is trained on a randomly sampled subset of the training data and a subset of the input features. During training, each decision tree independently makes predictions. The final prediction of the random forest is determined by aggregating the predictions of all the individual trees, either through majority voting (for classification) or averaging (for regression). This feature indicates an high level of complexity, determining a more accurate output but posing problems on the explainability.
- **Clustering:** In machine learning, the unsupervised task of grouping a set of objects so that objects within the same group (called a cluster) are more "similar" to each other than objects in other groups.

F.4 Robotics: Robotics in AI is the combination of artificial intelligence and robotics to create intelligent machines that can perform tasks autonomously or with minimal human intervention. AI algorithms are used to enable robots to sense their environment, make decisions, and take actions based on that information. This involves using sensors, cameras, and other hardware to collect data, and then processing that data using machine learning and other AI techniques to create models that the robot can use to understand and navigate its surroundings A practical example is the Roadside Assistance RPA System, which allows, following a signal from the black box installed in the vehicle, to geolocate the driver and select the roadside assistance provider, from those available at that time, and contact him or her automatically, giving instructions on the type of intervention required.

F.4.1 Integration and interaction: Integration refers to the process of combining different AI components or systems to create a larger, more complex system that can perform more advanced tasks or achieve better performance than any of the individual components alone. For example, a self-driving car might integrate components for computer vision, natural language processing, and decision-making algorithms to create a complete autonomous driving system. Interaction refers to how AI systems can communicate and interact with humans or other systems. For example, a chatbot might interact with users through a conversational interface that uses natural language processing to understand and respond to user input. Similarly, an autonomous robot might interact with its environment using sensors and actuators, and with humans through natural language commands or physical gestures.

F.4.2 Robotic Process Automation (RPA): Robotic Process Automation (RPA) is a form of artificial intelligence that involves the use of software "robots" to automate repetitive, rules-based tasks. These robots can be programmed to perform a variety of tasks, such as data entry, form filling, and report generation, that were previously done by humans.

RPA systems are designed to mimic human actions, using algorithms and machine learning techniques to learn how to perform tasks based on user input and feedback. These robots can be integrated with existing IT systems, such as enterprise resource planning (ERP) and customer relationship management (CRM) systems, to automate business processes and increase efficiency. RPA is often used in back-office operations, such as finance and accounting, human resources, and supply chain management, to reduce errors and improve process efficiency. By automating routine tasks, RPA can free up human workers to focus on higher-level tasks that require creativity, problem-solving, and decision-making skills. One of the key advantages of RPA is that it can be implemented quickly and with minimal disruption to existing systems. RPA systems can also be easily scaled up or down to meet changing business needs and can be reprogrammed as needed to adapt to new processes or requirements. However, RPA has some limitations. It is best suited for tasks that are highly structured and rule-based and may not be well-suited for tasks that require judgment or decision-making. Additionally, RPA may not be suitable for tasks that require interaction with unstructured data or natural language processing, as these tasks may require more advanced forms of AI.

- ☐ **Multi agent systems:** A multi-agent system consists of multiple decision-making agents which interact in a shared environment to achieve common or conflicting goals.
- ☐ **Connected and automated vehicles:** Connected and autonomous vehicles (or CAVs) combine connectivity and automated technologies to assist or replace humans in the task of driving. This can be through a combination of advanced sensor technology; on-board and remote processing capabilities; GPS and telecommunications systems.
- ☐ **AI services:** Artificial Intelligence as a Service (AIaaS) is the third-party offering of artificial intelligence (AI) outsourcing. It enables individuals and companies to experiment with AI for various purposes without a large initial investment and with lower risk.

Operational activities must always comply with the principle of nondiscrimination and fairness, in accordance to EIOPA Guidelines on Trustworthy AI. For the sake of completeness, below are reported the activities considered as "high-risk activities" and therefore restricted in Annex III of the AI Act in preparation. These activities require more in-depth assessments because they may have military or mass control applications and require official approvals to be carried out. Any evaluator who detects high-risk components should immediately investigate and report such activities to the authorities, if necessary. Specifically, they are categorized as:

F.5. Limited field of application:

F.5.1.Biometric identification and categorization of natural persons

F.5.2.Management and operation of critical infrastructure

F.5.3.Education and vocational training

F.5.4.Employment, workers management and access to self-employment

F.5.5.Access to and enjoyment of essential private services and public services and benefits

F.5.6.Law enforcement

F.5.7.Migration, asylum, and border control management

F.5.8.Administration of justice and democratic processes

It is worth re-emphasizing that this taxonomy's aim is mapping the main characteristics and features that represent better a commercial AI application, in order to understand the possible shortcomings, the level of complexity achieved and easily compare points in common among different operators. The taxonomy has the ambitious goal of becoming a Compliance Decisional Support System to facilitate the development, adoption, and implementation of new AI models in insurance companies, enabling an optimized communication between legal and IT specialists.

4. Conclusions

4.1 Proposal fit on the basis of the AI act

During the realization of the AI Taxonomy, the AI Act being drafted by the European Commission was taken into account. For this reason, some characteristics mentioned in the draft were chosen with insights and specifications that are suitable to have an overview of the extensive topic of 'Artificial Intelligence', without necessarily having a background as a software developer. The reasoning behind this decision is that there may be different interpretations with which to create a taxonomy, but explicit reference should be made to the hierarchically most relevant normative sources. Considering this, the compliance tool does not revolutionize a European act, but rather implements and ensures easy operational application of the latter. By means of standardized benchmarks, the aim is to ensure that AI systems placed on the EU market are safe and comply with existing fundamental human rights legislation. Furthermore, the user-friendliness of the taxonomy, when combined with best practices in the management of a specific component, would improve governance and compliance with existing regulations. The AI Taxonomy in the Insurance Sector facilitates the monitoring of regulatory requirements for commercial applications of Artificial Intelligence to ensure the stability of the financial system and respect for human dignity. There is a need for absolute consistency with existing EU legislation applicable to the insurance sector where high-risk AI systems are already in use. Furthermore, it is crucial to ensure adherence to the EU Charter of Fundamental Rights and existing EU laws on data protection, consumer protection, non-discrimination and gender equality. The Taxonomy application during the AI assessment, does not interfere with the General Data Protection Regulation (Regulation (EU) 2016/679) or the Directive on Data Protection in Police and Judicial Activities (Directive (EU) 2016/680). Ultimately, the AI Taxonomy in the Insurance Sector aspires to be a tool to improve regulatory efficiency and simplify the entry of new businesses while maintaining high security standards.

4.2 Competitiveness of the European AI model - business advantage [missing]

The European legislator has decided to place clear limits and safeguards on the development of Artificial Intelligence, especially because it is very difficult to predict the large-scale effects of any error. Other states or confederations have decided not to place strict limits on the development of AI and seek to extract the maximum benefit from the exploitation of such technologies. On the one hand, the possibility of obtaining precise metrics, classifications and forecasts is an important boost for the economic development of a nation or an individual company. The implementation of AI safeguards and regulations in Europe has the potential to negatively impact the development of AI technology in the region. While the intention behind these measures is to ensure ethical and responsible AI deployment, the stringent rules and bureaucratic processes may stifle innovation and impede progress. The complex and expensive compliance procedures for AI systems can slow down the pace of development, making it difficult for startups and small companies to navigate the regulatory landscape. These barriers may discourage investment in AI research and development within Europe, leading to a brain drain as talented researchers and entrepreneurs seek more favorable environments elsewhere. Consequently, Europe may risk falling behind other regions in the advancement and competitiveness of AI technology, limiting its potential benefits and hampering economic growth. On the other hand, the implementation of AI safeguards and regulations in Europe has the potential to positively impact the development of AI technology in the region. These measures are designed to ensure the responsible and ethical use of AI, instilling public **trust** and confidence in the technology. By providing clear guidelines and standards, regulations can promote transparency and accountability, encouraging organizations to adopt responsible practices. This fosters an encouraging environment for innovation and investment, as companies can demonstrate their commitment to ethical AI development. Additionally, robust data protection and privacy regulations enhance individuals' rights and safeguard their personal information, which in turn builds trust and encourages the sharing of data for research purposes. The emphasis on fairness, bias mitigation, and explainability in AI systems helps address societal concerns and ensures that AI technology benefits all segments of the population. By prioritizing ethics and accountability, Europe can position itself as a global leader in AI technology, attracting talent and encouraging a vibrant ecosystem that promotes responsible AI innovation for the betterment of society. In any case, promoting very high safety standards will allow Europe to have **applications that are marketable in every country** of the world and, at the same time, it will be possible to limit the effects of some foreign accidents that could affect the European economic resilience and the whole social system.

4.3 Conclusions

At the conclusion of this research project, it emerges that the applications used by insurance companies have certain basic characteristics in common but it's almost impossible to have two identical AI. These characteristics can be better used while assessing and classifying AI and represent a reliable reference model for the objective description of the software in use in the company. Starting from extensive definitions, it was possible to deepen the six macro-categories into specific subsets that more precisely represent which features are objectively relevant for describing the state of the art of a process or software. The characteristics identified describe:

- Purely technical features such as the type of learning used in AI training and development;
- Purely legal features such as the presence of a human in the decision loop or the legal configuration of certain special categories of data;
- Hybrid features describing a technical choice that could have legal impacts such as the explainability of the output and the operational scope of use.

Ideally, an AI taxonomy should be used as a tool for communication and collaboration between two professionals with completely different academic backgrounds, i.e. legal experts and IT developers. This work aims to promote the sustainable development of applications that will significantly impact the operating models of insurance companies and, consequently, the entire financial sector. The management and control of regulatory compliance becomes a focal point of sustainable technology development and aims to minimize systemic risks and possible negative externalities. In conclusion, the AI Taxonomy represents a compliance tool that can easily be taken up by the Data Protection Officers already present in insurance companies or by other specific figures that will be diesigned in the upcoming years. The choice of this tool saves money, staff training costs and time, in favor of a standardization of assessment metrics and a qualitatively effective output.

5. Methodology’s description

Considering the empirical and experimental nature of the subject under discussion and considering that the main legal source aiming to regulate Artificial Intelligence in Europe has not yet been officially approved, it was decided to place special emphasis on the presentation of results rather than on the review of the scientific literature produced. The lack of academic material on a methodology for classifying Artificial Intelligence systems has been offset by other empirical sources that ensure the quality of the paper. The proposed research methodology is based on three main pillars: the review of existing and forthcoming regulatory provisions; the on-site experience as a compliance consultant for a management consulting firm; and the interview with the most important sectoral association in the Italian insurance landscape.

Firstly, regulatory sources were analyzed, including the AI Act currently in preparation at the European Commission; Regulation (EU) 2016/679 (General Data Protection Regulation); the Solvency 2 Directive, including the Technical Standards Implementation Framework (ITS) and the EIOPA guidelines. Subsequently, through an internship activity performed at an Italian Management Consulting company, it has been possible to take part in a formal assessment of the Artificial Intelligence systems employed by an insurance company. Based on this significant experience, it was possible to understand the operational needs of a large insurance company and the typology of output required from the Board of Directors, taking into account the information demanded by the national insurance authority (IVASS) in order to deem the assessments compliant and adequate. Finally, ANIA (Associazione Nazionale Imprese Assicurative), established in 1944 and based in Rome, which represents all insurance companies operating in Italy, was also included in the discussion. By means of an interview, it was possible to understand how private and institutional interests are balanced. The result of the research aims to be a product that can be used in the phase prior to risk assessment, to facilitate the comparability of assessments and make them more objective. This research project stands as a precursor to a new field of study, related to the efficient implementation of European legislation, and it is hoped that it will be a starting point for future discussions and debates.

Bibliography & Reference

1. *Martin Ebers*. Standardizing AI – The Case of the European Commission's Proposal for an Artificial Intelligence Act, 2022.
2. *Jonas Schuett.* A Legal definition of AI, 2019 (https://www.researchgate.net/profile/Jonas-Schuett/publication/336198524_A_Legal_Definition_of_AI/links/5e20599a458515ba208b9e4c/A-Legal-Definition-of-AI.pdf)
3. High-Level Expert Group on AI. Ethics Guidelines for Trustworthy AI, 2019.
4. European Commission, Communication on Building Trust in Human-Centric Artificial Intelligence, 2019.
5. European Commission, Communication on Fostering a European approach to Artificial Intelligence, 2021.
6. European Commission, White Paper on Artificial Intelligence, 2020
7. Consob, the current financial system: a stylisation (https://www.consob.it/web/investor-education/il-sistema-finanziario-attuale-una-stilizzazione)
8. European Commission, Financial sector and access to finance (https://reform-support.ec.europa.eu/what-we-do/financial-sector-and-access-finance_it)
9. IVASS, Publication and statistics, 2021 (https://www.ivass.it/pubblicazioni-e-statistiche/statistiche/numeri-assicurazioni/2021/Focus_I_principali_numeri_2021.pdf)
10. IVASS, Publication and statistics, 2022 https://www.ivass.it/pubblicazioni-e-statistiche/pubblicazioni/relazione-annuale/2022/Relazione_IVASS_sul_2021.pdf (pag. 10-13; 222)
11. JRC Technical Reports, AI Watch defining Artificial Intelligence towards an operational definition and taxonomy of artificial intelligence (https://eprints.ugd.edu.mk/28047/1/3.%20jrc118163_ai_watch._defining_artificial_intelligence_1.pdf)
12. https://aiknowyou.ai/cosa-significa-natural-language-understanding/
13. *Fabrizio Montanari and Lorenzo Mizzau*, The Places Of Open Innovation: Models of territorial development and social inclusion, 2016 https://iris.luiss.it/bitstream/11385/183951/1/q55_I%20luoghi%20dell%27innovazione%20aperta_def.pdf
14. Monsah business school, Marketing Dictionary, 2020 (https://www.monash.edu/business/marketing/marketing-dictionary/m/megatrend)