MACHINE LEARNING: A BRIEF INTRODUCTION AND CRITICAL ASPECTS

Machine learning represents one of the most significant technological innovations of recent years, what are the risks for our privacy and data? What about advantages and disadvantages?

AUTHORS: Aurora Agostini and Jessica

SUMMARY

MACHINE LEARNING

What is a Machine Learning? How does it work?

The term Machine Learning refers to a subcategory of Artificial Intelligence consisting of mechanisms enabling a smart machine to improve its capabilities and performance over time. The functioning of a Machine Learning system is based on **algorithms** able to develop a **reasoning model** based on the provided set of data and to adjust it over time according to its experience. In other words, these algorithms can adapt their structure and functioning on the basis of the issues they solved - the more algorithms they solve, the more they learn. These peculiarities make the algorithms used to create machine learning models, increasingly precise and accurate, giving them a certain "**autonomy**" in behaviour.

The starting point of every machine learning system is a set of data, provided by the developer, composed of **situation** and **solution variables**, which respectively represent concrete examples of the issues the system will have to face and their solution.

The first person to show interest in this field was **Alan Turing**, who in 1950, put forward a proposal concerning the need for algorithms capable of analyzing the first prototypes of machines learning . Since then this technology has continued to improve and now it allows us to accomplish incredible things.

Different types of machine learning

Based on how a system collects information and learn from them, it is possible to define three different kinds of machine learning systems, which are:

- **Supervised machine learning**. In this case data regarding the input is provided to the computer, i.e. issues that are going to be presented to it, and information about the desired outcomes, i.e. the solution to the problems. The system has the goal to identify a general rule that connects the input data to the output data, so that it can then reuse this rule for similar tasks. In summary, input and output examples are provided so that the system learns the relationship between them and applies it to new cases.
- **Unsupervised machine learning**. Machine learning systems belonging to this category are provided with a dataset composed only of input data, without any indication of the desired outcome. The goal of this kind of systems is to "discover" hidden patterns and models, in other words, to identify a logical structure in the input data without them being previously labelled.
- **Reinforcement learning**. In this case, the system improves its learning model analysing not only past experiences but also the environment. The peculiarity of the reinforcement learning method lays on the reward/punishment mechanism that regulates the system's functioning. Indeed, while interacting with input data, coming both from the dataset and the environment, the system is rewarded for achieving some defined goals and punished for unwanted behaviours.

It is also worth mentioning **deep learning**, a sub-category of machine learning that is very similar to reinforcement learning. Deep learning also autonomously creates its reasoning model from a data set. However, unlike reinforcement learning, it does not proceed by trial and error. Deep learning, in particular, applies the reasoning rules extracted from "old" datasets to new ones in order to identify relevant features. For this reason, deep learning is mainly used for recognition tasks such as speech and image recognition.

The importance of machine learning

Regardless of the distinction between the types of learning systems, the data used in the **training phase** (data set) plays a fundamental role in the functioning of the system, since the algorithm needs a large quantity of information at its disposal in order to develop a **model of reasoning** capable of solving problems in a precise and effective manner. The results that can be achieved with machine learning cannot be achieved by the human mind, which cannot process such a large amount of information. It is therefore clear that this tool has enormous potential.

Just consider how machine learning has changed financial system with prediction and trading in the **cryptocurrency market**: right now there are more than 20 thousand different cryptocurrencies and AI is able to provide us with forecasts of data and graphics for each one at every moment of their existence in the metaverse. This would certainly be impossible for human mind.

A technology for everyone and everyday

It is often thought that this tool has applications only in very technical fields, such as science, medicine, space engineering or other branches not commonly understood by non-technics. This is a very common mistake, as machine learning actually has many applications in everyday life; although, of course, it does involve the use of technology. A classic application of machine learning is in the **home automation sector**: tools that use voice recognition in order to learn new words or ways of speaking by following voice commands that are given to them are widespread.

Therefore it is possible to say that, for the first time in human history, there are tools capable of tracing what millions of people do every day: until not so long ago, only individuals at the peak of society could boast biographers who recorded their habits, interests and behaviors, but today we are all in the spotlight (although often involuntarily). Indeed, one of the most common uses of machine learning is **profiling** individuals in order to enable companies to create targeted advertisements. This means that it is possible to propose advertising strictly related to each user's interests, since its needs and preferences are recognized thanks to the analysis of its "**digital footprint**" i.e. the cluster of data generated by the user while using apps and navigating on internet.

An example of how this profiling activity impacts on the lives of individuals may be for example the use of wearable devices like **smartwatches**, which through the analysis of the **collected data**, such as the steps taken during the day and the track of the heartbeat, is able to identify and keep track of the various activities that the individual wearing it performs during the day. For instance, by monitoring the variability between beats, the smartwatch can indicate when an individual is stressed, as a decrease in the variability indicates higher stress levels, while an increase indicates lower stress levels.

Additionally, smartwatches can track physical activity, including when the heartbeat accelerates and slows during sleep, and monitor various other conditions. Cars and other shared modes of transport can also be used for profiling individuals by tracking their movements through geolocation to determine the places they frequent and their interests.

AI as a booster for public institution

It is worth emphasizing that artificial intelligence is not only of interest to private companies. In fact, the **public sector** has also recently shown some openness towards the use of **AI systems**. Some scholars refer to this "new era" as the "**Digital State era**" underlining the radical transformation of public activities through the introduction of new technologies.

For example, the European Commission's Coordinated Pl an on Artificial Intelligence sets as its goal the use of information technology and new technologies to **innovate Public Administration** as well. In the wake of the initiatives adopted by other European countries, Italy has started a process of **de-bureaucratization** and **streamlining** of procedures, which will lead to the creation of a single centralized Big Data structure, so as to avoid the duplication or significant loss of information and exploit the large amount of information available to the Public Administration.

Indeed, technology is going to have an impact on several different areas, from public services to the administration of justice. Concerning the administration of justice, a particularly interesting application of machine learning is the use of the so-called **automated decision-making systems** i.e. artificial intelligence systems that replace the judge in deciding a case. Estonia is a pioneer in this field, as it introduced in 2019 of the "X-road" platform for the settlement of small claims with a value lower than EUR 7,000.00.

AI: a delicate jigsaw puzzle

Although representing an interesting opportunity for companies and public institutions, it is crucial not to forget that machine learning entails also serious **risks**, in particular in relation to the processing of **personal data**, as demonstrated by the recent episode involving **Chat GPT** and the Italian Supervising Authority. The Italian Authority explained that Open AI did not provide any information to users and data subjects whose data were collected, and, more importantly, from the SA's inquiry resulted that "there was no legal basis underpinning the massive collection and processing of personal data in order to 'train' the algorithms on which the platform relies" . For these reasons, the Italian Authority imposed an immediate temporary limitation to Chat GPT's availability for Italian users and consequently to the processing of their data by OpenAI.

Even though it is not sure about how Supervising Authorities of other Member States will react to the adoption of this measure, on the other hand, this perfectly highlights that the functioning of machine learning systems can be very controversial and is also giving evidence of the reason why both national and European institutions are focusing their attention on the issue. For these reasons, it is the responsibility of both **industries** and **public institutions** to share information about how learning systems work. This will help to create knowledge about the topic, enabling people to trust artificial intelligence and use it to their advantage in the best possible way.

The next step will be the approval of the so-called **Artificial Intelligence Act**.

LEXIA
AVVOCATI

Avv. Aurora Agostini
aurora.agostini@lexia.it
(+39) 02 3663 8610

Dott.ssa Jessica Giussani
jessica.giussani@lexia.it
(+39) 02 3663 8610

www.lexia.it
Via del Lauro, 9 20121 Milano
Follow us on Linkedin: https://www.linkedin.com/company/lexia-avvocati/