Abstract

Artificial Intelligence (AI) is considered the great revolution of the modern era. After the industrial revolution that took place over a century ago, other technologies such as computers and the World Wide Web have drastically changed the world, but none of them has unnerved humanity like AI. In reality, artificial intelligence is nothing more than a technology like any other, with great potential and great risks. Like every new discovery and invention, it must be regulated, and we must learn to use it correctly to harness its full potential.

Contrary to its name, AI has nothing truly intelligent about it; it is simply an evolution of mathematical statistics. Thanks to the computing power of modern computers and state-of-the-art software, AI enables us to do things that, until recently, only humans could do. The significant change introduced by AI is hidden from the eyes of most people. AI has simply changed the paradigm of how we have always thought about solving problems. Until now, we thought that by having an equation (*f(x)*) and its solution, i.e., the output (*y*), we could obtain the input (*x*) by solving the equation mathematically. What AI does is change this paradigm, allowing us to find very complex equations, which we couldn't find with simple calculations, by examining not only the outputs but also the input variables. It's no longer a matter of finding the *x* of equations studied in school; with many *x* and *y*, we need to find the equation that connects them. This is the true revolution of AI.

However, like all major technologies, AI has its risks and dangers. What I will show in this thesis is an example of the most classic problems and risks associated with AI. Specifically, we will address privacy and security, providing examples in various fields to understand how sometimes a small manipulation can cause enormous damage, sometimes unintentionally, and other times with declared malicious intentions. In the following chapters, we will delve into the details of two cases, one related to security and the other to privacy, which I personally dealt with during my Ph.D. I will present some possible solutions that I found together with my research group. In conclusion, I would like to emphasize that it will not be AI dominating us but our intelligence deciding whether to remain masters of ourselves or choose self-destruction.