Three Areas of Law that May be Affected by AI

SONG haoyu

202300130183

Instructions for using artificial intelligence tools: The original text is written in Chinese and translated into English using ChatGPT 3.5. Tian Gong AI tools were used for auxiliary searches.

From the protection of information and data to the transformation of production methods and structures, the development of artificial intelligence technology has had an almost disruptive impact on many traditional industries, and this technological revolution has also had a profound impact on the law. The following are three legal areas that I think may be affected by artificial intelligence technology and my understanding of them.

First Area: Personal Information Protection Law

The AI models currently applied or about to be applied in the commercial field do not show this clearly when the models are small. However, with the increase in computing power, large models are gradually becoming mainstream in practical applications. Due to the limitations of current deep learning technology, training a usable model inevitably requires a large amount of data. This data can come from various sources, including public datasets, user-uploaded data, and data collected in other ways. Many application areas require the use of personal privacy and sensitive information, a typical example being the use of AI to diagnose diseases. Training a usable model requires a lot of CT scans and test data from previous patients, which may infringe on the privacy of many users. Similarly, many internet platforms collect and analyze user behavior, operations, and browsing records to train recommendation system models. Although this is often imperceptible to users, it still poses a risk to user privacy. Therefore, personal information protection laws need to improve provisions in this area to protect users' necessary right to know and information security. Supplement: Federated learning technology attempts to address this issue, but there is still no method that can train models while fully protecting user privacy.

Second Area: Intellectual Property Law

This field involves two aspects: the source of data used for model training and the ownership of the model's generated results. Many generative AI models require large amounts of data from the internet for training, such as natural language processing models needing large corpora, and image generation models needing other images from the web. This raises the issue of the use of copyrighted materials like texts and images. Currently, many large models avoid this issue by open-sourcing their code and model parameters and not using them commercially, such as the open-source NLP model LLaMA and the text-to-image model Stable Diffusion. However, many models used commercially still use unauthorized data for training. Relevant laws need to improve corresponding provisions to ensure that the original authors of copyrighted works have the necessary right to know and authorization and rights protection, but also need to ensure that the authorization process is efficient enough so that the cost of collecting training data does not increase significantly, to avoid hindering the development of relevant AI technologies. Another aspect is the ownership of the AI model's generated output. It is still an open question whether the results produced by the model should belong to the model's creators or the users. If users profit from the model's output, should the creators share in that profit? Laws need to determine fairly whether the output should belong to the creators or the users. Additionally, if the model's output is used in real applications and causes errors, the issue of accountability for losses caused by the model's results also needs legal clarification. For instance, if I use an AI service from a company to predict the stock market and incur losses, should I bear the loss myself or should the company be liable?

Third Area: Cybersecurity Law

Similar to the end of the previous section, this also involves the issue of responsibility. If someone uses an AI tool to launch a cyberattack on another computer, who should bear the loss—only the attacker or also the tool provider? If a model user uses certain methods to make the model output content that it was not originally designed to output, such as other users' private information or illegal information, who should be responsible for the resulting loss and the misuse of the information? Should the model's creators be held accountable? For example, if I use a code-generating model to create a computer virus and cause damage to others, should the creators of the code-generating model be held responsible? These are aspects current laws need to consider and improve. Lawmakers must also consider whether the laws they create will negatively impact the development of AI technology.

The above are my personal thoughts and understanding of the legal areas that may be affected by AI technology. If there are any mistakes, please forgive me.