Abstract of Doctoral Dissertation

Title: The Criminal Problems of the use of Artificial Intelligence

- Focus on the Criminal Liability of Users and Producers -

Doctoral Program in Law
Graduate School of Law
Ritsumeikan University
ヒハラ　タクヤ
HIHARA Takuya

In this doctoral dissertation under the theme of "The Criminal Law Problems in the Use of Artificial Intelligence," I examine the criminal law evaluation of cases where AI products infringe on human life, body, or property, when they commit economic crimes, or when they are cyber-attacked, focusing mainly on manufacturers and users, who are involved in AI products.

In Chapter 1, I first attempted to establish the definition of AI by going back to the history of AI research before discussing its criminal law problems, especially since the definitions of AI assumed by the authors in the previous studies were ambiguous. However, since the definition of AI has been difficult, it was confirmed that so-called "weak AI," which specializes in performing specific tasks and cannot make autonomous judgments, should be the target of the discussion of these problems, by induction from the existing forms of AI phenomena.

In Chapter 2, I examined cases of infringement on human life and body caused by accidents involving AI products. Unlike in case of accidents by self-driving car, regarding accident cases involving AI products for which no legal obligation exists, the obligations of those involved in them should be determined based on certain legal obligations for others as in the case of self-driving cars. For example, for the manufacturer, product liability under criminal law should be examined, taking as clues the manufacturing duty, design duty, and instruction and warning duty (product monitoring duty) imposed under Japanese Product Liability Law. Here, the manufacturer must not immediately constitute criminal negligence for violating these obligations, but rather carefully examines whether there is a causal relationship with the consequences that have occurred, per the protective purpose of the content of those obligations. The same applies to the technical service providers, and to the state and local authorities responsible for licensing, and, on the other hand, users and owners may be obliged to comply with the manufacturer's instructions and refrain from misusing or abusing them.

However, in case of economic crimes for which there is no provision for punishment of negligence, the above scheme entails difficulties to consider. Therefore, in Chapter 3, I examined cases

where AI-algorithms, as a result of their learning, carry out market manipulation, securities crimes such as insider trading, and violations of competition laws such as price coordination, without the users' knowledge. In case of market manipulation, users are required to use AI while always considering the possibility of market manipulation, which may be an excessive burden both in terms of use and legality and may hinder the development and diffusion of such algorithms. Therefore, manufacturers are required to construct systems that are recognized as not market manipulation, and it is important for them to have a structure that clarifies the decision-making process. The same system must be constructed for insider trading, and it is important to have a structure that clarifies the decision-making processes. Meanwhile, if price coordination among users is realized by learning AI it may be interpreted as an unfair restriction of trade under the Antimonopoly Law, but the possibility of price coordination by learning AI is low at present. However, the possibility of price coordination by learning AI algorithms is currently low, and cease-and-desist orders, surcharges, and criminal penalties are stipulated for "unfair restraint of trade", so the finding should be made with caution. The evaluation under criminal law when an AI product is subjected to a cyber-attack and the user's information is obtained or the use of the product is prevented by modifying or destroying its internal data can be broadly divided into the issue of requirements for constitution of crime and the black box of AI's learning. In case of the requirement issue, first, the act of hacking into an AI product is not necessarily regarded as unauthorized access, the act of acquiring user information recorded in the AI product is not subjected to Japanese criminal code, and in case of modifying or destroying internal data, the use of the product is job-related, and these may be considered a criminal offense as long as it results in the obstruction of business. The problem of the black-box of AI learning is relevant to the crimes of obstructing business by damaging computers and fraudulent use of computers. In both cases, if the causality is unclear, even if the user's business is obstructed, the actor may only be guilty of an attempt, even if the result is that the actor has gained an unfair advantage. Again, the concept of explainable AI is important here, and it can be realized to prevent this consequence.

In Chapter 4, I confirmed that the guidelines and regulations for future AI development since the late 2010s are showing changes in their content as we enter the 2020s. In particular, imposing hard sanctions, as “AI Law” in EU, on future development without any concrete risk yet can discourage future AI development. As AI-equipped products continue to advance daily and numerous actors are involved with AI, the principles and the obligations should be made concrete. Thus, the principles to be observed by these entities and the obligations to be imposed on them should be specifically developed. It is essential for future AI R&D, as well as for sales, distribution, and utilization, to establish legal principles and obligations to be complied with by entities involved in AI products, starting from soft law such as licensing and auditing systems to ensure their effectiveness, while taking into consideration the balance between the interests of users and the burden on manufacturers. This is essential for future AI R&D, and for the sales, distribution, and utilization of AI products.