DENTONS HPRP

Grow | Protect | Operate | Finance

Criminal Liability for Felonies or Misdemeanours Committed by Artificial Intelligence

Prepared by:

Mika Isac Kriyasa (Partner), Leonardo Richo Sidabutar (Senior Associate) and Luthfi Arya Ramadhani (Associate)

Artificial Intelligence ("**AI**") has taken off recently. We can now find various uses of AI from making profile avatars to motor vehicle automatic driving systems. Developments in AI have made the European Union followed by the United Kingdom prepare legislation specifically governing AI. In its draft regulation, the EU has determined AI systems as software developed through one or more techniques and approaches which can, for a series of purposes determined by human beings, produce output such as content, predictions, recommendations, or decisions which will affect the environment with which they interact. This definition shows how wide-ranging, complex, and complicated AI is.

As time goes by, AI may be involved in a crime or illegal action. On 29 December 2019 in the US, a Tesla Model S in autopilot mode crashed into a Honda Civic resulting in the driver of the Honda Civic being killed instantly together with a passenger.[1] As another example, we often see reports where students have used AI to do their assignments for them. In 2020, researchers at University College London identified several crimes which could be facilitated by AI,[2] such as the use of driverless cars as weapons, making phishing messages adapted to the originals, selling fake goods or services labelled by AI, and stalking using AI.

As shown above, we can say in general that AI could be involved in crimes in the form of (i) crimes committed by the AI itself, and (ii) crimes committed using AI as a tool. If this happens, who is responsible for the crimes involving AI.

Artificial Intelligence Law in Indonesia

Unlike the EU, Indonesia has not yet seen the issuance of any legislation specifically governing AI and its use. However, we can find existing legislation relevant to AI in the Electronic Information and Transactions Act Law No. 11 of 2008 as amended by Law No. 19 of 2016 (the "**ITE Act**"). Article 1 item 5 of the ITE Act defines an Electronic System as a series of electronic tools and procedures which function to prepare, collect, process, analyse, store, display, publish, send, and/or disseminate Electronic Information ("**Electronic System**"). To date, this definition of an Electronic System is the most relevant for AI, bearing in mind the recent rapid development and use of AI.

The ITE Act regulates the operation of Electronic Systems in Articles 15 and 16. Article 15 states that every operator of an Electronic System **must operate the Electronic System reliably and safely and be liable for its proper operation.** Article 15 of the ITE Act also states that the Electronic System operator is liable for the Operation of the Electronic System. Article 15 paragraph (3) limits the Electronic System operator's liability by specifying that the Electronic System operator is not liable for the operation of the Electronic System if there is any error and/or negligence by the Electronic System's user. In the context of AI. This provision in the ITE Act means that the AI operator is liable for the safe, reliable, proper operation of the AI but the operator is not liable for any errors and/or negligence by the AI user.

This concept of the AI operator's liability looks simple enough, but its application in the context of the criminal law is another matter. If a crime is committed by or involves AI, the AI operator must prove that the AI is safe and reliable and is operating properly, and that any fault or negligence lies with the user. This is clearly something of a challenge because it involves technical and operational aspects as well as the AI operator's compliance and good corporate governance.

[1] https://www.latimes.com/california/story/2022-01-19/a-tesla-on-autopilot-killed-two-people-in-gardena-is-the-driver-guilty-of_manslaughter
[2] https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

On the other hand, the ITE Act provides prohibitions in connection with electronic information and documents, electronic transactions, and Electronic Systems in Articles 27 to 37, which prohibit:

1. the distribution, transmission and making accessible through an Electronic System of electronic information or electronic documents the contents of which involve immorality, gambling, insult, defamation, blackmail, and/or threats;
2. gaining access to another party's computer and/or Electronic System in any fashion;
3. intercepting or tapping electronic information and/or electronic documents in a computer and/or particular Electronic System belonging to another;
4. the unauthorised moving or transferring of electronic information and/or electronic documents to the Electronic System of another person in any fashion;
5. the performance of any action which results in disruption to an Electronic System and/or results in an Electronic System not working properly;
6. the manipulation, creation, alteration, erasure, or damage of electronic information and/or electronic documents with the purpose that the electronic information and/or electronic documents will be considered genuine.

The above prohibitions can serve as a reference for AI operators in ensuring that an AI is not contrary to the ITE Act. For example, an AI operator should not design AI which could make indecent, insulting, or defamatory photos, or design AI which can move or transfer another person's electronic information and/or electronic documents without the authority to do so.

The AI operator should also carry out a comprehensive review of the laws and regulations to ensure that the concept and operation of the AI produced is not contrary to legislation in order to mitigate the risk of liability for the AI operator.

Criminal Liability for Use of Artificial Intelligence from the Viewpoint of the Criminal Law

With regard to criminal liability, the Criminal Code Act Law No.1 of 2023 (the "**New Criminal Code**") provides that criminal liability for a crime can rest with a individual person or with a corporation. An individual may be held liable in the criminal courts not only for intentional acts but also in matters of negligence[3], while a corporation may be held liable in the criminal courts if the corporation does not take the necessary steps to prevent or to mitigate the impact of crimes and to ensure compliance with prevailing law in order to avoid the occurrence of crimes and/or if the corporation allows crimes to occur.

The element of criminal liability for a person's or corporation's negligence in not taking the necessary steps to prevent or mitigate the impact of crimes and to ensure compliance with the prevailing law in order to avoid the occurrence of crimes and/or if a corporation allows crimes to occur, **could potentially trigger AI operators being held criminally liable.** For example, the person who made or designed the AI in the Model S Tesla in the accident described above could be subject to criminal sanctions for the negligence which caused the injuries or death, if it could be proven that there was negligence on the part of the person who designed the AI. As another example, the AI operator who operated the AI in the Model S Tesla in the case described above could be subject to criminal sanctions if it could be proven that the operator had not taken the necessary steps to prevent the accident befalling the victims.

The New Criminal Code also provides for criminal sanctions which can be applied to corporations if the corporation is proven to have committed a crime, the sanctions being fines and additional penalties in the form of payment of compensation, remedying the results of the crime, performance of the obligations neglected, confiscation of goods or profits obtained from the crime, revocation of certain permits, a permanent prohibition on certain actions, closure of some or all of the corporation's places of business and/or activities, suspension of some or all of the corporation's business activities, and dissolution of the corporation.

For these reasons, it is important for AI operators to have, determine, implement, and ensure preventive measures against crimes in making and/or operating AI as Electronic Systems in order to reduce the risk of the operator of the AI as an Electronic System being held criminally liable.

[3]Article 36 of the New Criminal Code