KIC
Korean Institute of Criminology

Trends & Policies in Criminal Justice

No. 013 April 2021

The Criminal Justice Response and Development Strategy in the age of the Fourth Industrial Revolution (II) : The Internet of Things(IoT) and Blockchain

Jeeyoung Yun
Research Fellow at Korean Institute of Criminology
(gg7797@kic.re.kr)

Hyunwook Chun
Research Fellow at Korean Institute of Criminology

Jinmook Kim
Standing Commissioner at the National Election Commission

Bugon Ryu
Professor at the Korean National Police University

Wonsang Lee
Professor at Chosun University

Byeongwook Lee
Professor at Hankuk University of Foreign Studies

Min-gyu Kim
Research Fellow at Korean Institute of Criminology

Keywords

※ Fourth Industrial Revolution, cybercrime, Internet of Things (IoT), blockchain, bitcoin, cryptocurrency

Necessity and Purpose

- The theme of the 2016 World Economic Forum's annual meeting, Mastering the Fourth Industrial Revolution, initiated our interest in Artificial Intelligence (AI) and the Google DeepMind Challenge Match in March 2016 further ignited the phenomenon.
- The Moon administration has set 'the economy pursuing mutual prosperity' as one of government objectives and the 'Fourth Industrial Revolution led by the development of science, and technology' as one of major strategic goals in order to spread superintelligence and hyper-connected technologies igniting the Fourth Industrial Revolution, which will create jobs and growth by developing core technologies and fostering new industries.
- The development of cutting-edge science and technology will impact not only changes in production methods such as manufacturing but also trends and patterns in crime and the overall criminal justice system.
- Witnessed by the history of new crimes that emerged during the early days of the Internet boom, and criminal justice responses to them, we need to pay attention to the changing crime patterns and criminal justice response measures caused by new technology.

- Today, we are embracing another era of network innovation where non-human objects are also connected to the Internet to collect, transmit, and share information. Encryption technology has also been applied to the network and information process. The IoT and blockchain technology are leading the network innovation, which serves as the basis of the Fourth Industrial Revolution in terms of expansion and encryption of the network.
- Meanwhile, the WannaCry ransomware attack in May 2017 focused on important facilities including the railroad, medical and communications systems. The hackers demanded ransom payments in the Bitcoin cryptocurrency.
- As such, many have expressed growing concerns over cyberattacks exploiting security vulnerabilities of the IoT and the anonymity of cryptocurrencies. Therefore, we explored criminal justice issues and responses concerning the emergence of the IoT and blockchain.

Research Methods

Literature review and comparative legal analysis

- This study has conducted a literature review on domestic and international reports, books, and papers covering legal and institutional issues with the IoT and blockchain technology, the leading network innovations in the foundation of the Fourth Industrial Revolution.
- This study overviewed the history of criminal justice response in accordance with the development of information and communication technology, and conducted a comparative legal research on foreign countries' (the US, Germany, and Japan) responses to the crimes related to the IoT and blockchain technology.

Interview with domestic and international experts and seminar participation

- Reviewed the current status of technological development and the possibility of its utilization through interviewing experts, attending seminars, and reviewing the trend in improving relevant regulations through advisory meetings with legal experts.
- Carried out a joint research with technology experts in order to facilitate practical discussions based on the technical understanding of the IoT and blockchain and visiting relevant domestic and foreign agencies to hold expert meetings and seminars as a means for spotting criminal justice issues during the commercialization of such technology.
- In particular, given the situation where legal issues related to cryptocurrencies with blockchain technology are emerging, planned and provided lecture programs to improve the understanding of the relevant technology among experts and practitioners in criminal law and held a forum to discuss the possibility of applying the current laws and its limitation.

Main Contents

Development of information and communication technology and changes in criminal law

- History of criminal justice responses to the spread of computers and commercialization of the Internet.
- Criminal justice issues in response to the sophistication of information and communication technology.

Internet of Thing (IoT)

- Technical understanding and characteristics of the IoT.
- Possibility of change in crime patterns by the IoT
- Current status of legal adjustment of the IoT and its limitations.

Blockchain

- Technical understanding and characteristics of blockchain.
- Possibility of change in crime patterns by blockchain technology.
- Current Status of legal reformation on blockchain, and cryptocurrencies and their limitations.

Criminal response measures in the era of network innovation

- Criminal law.
- Criminal procedural law
- Criminal policy.

Response measures in terms of criminal law

- Under the current law, the regulation on breaching information and communication network has a strong characteristic of administrative criminal law to ensure the stability of the information and communication network. Also, it does not provide direct protection to the victims of privacy infringement. Therefore, we propose creating applicable provisions to punish privacy violation by technical methods.
- Questions have arisen about applicability of the crime of arson under the current law when a fire breaks out from overheating a device while manipulating the IoT. Therefore, we propose that the term 'set fire' change to 'start fire' or adopting separate elements of the offense to punish manipulating and controlling electric devices, or causing fire from doing so.
- A cryptocurrency is neither an object under the Civil Act, nor a property under the Criminal Act. Nevertheless, it could be an object of a claim in Civil Act and may be liquidated at cryptocurrency exchanges in accordance with the market price or appraised as a property interest with a certain value under the Criminal Act. Therefore, it could be regarded as an object of 'unjust enrichment' under the Criminal Act due to its liquidability.
- The act of stealing a cryptocurrency itself in an electronic manner can be regarded as a transfer of money without any authority using a computer, etc. and be charged not with larceny but with fraud by use of computer, etc. under the Criminal Act. However, it is difficult to consider the act of price manipulation, etc. of a cryptocurrency or a cryptocurrency exchange as a factual element of offense under the Criminal Act.
- Given the characteristics of cryptocurrency trade or exchanges, a even collusion by a relatively small number of people can cause a confusion in the cryptocurrency market. Therefore, regulations prohibiting and punishing such distruptions to the market, including price manipulation and the use of material non-public information, should be established.
- Currently, the act of using multiple accounts of others during the process of market price manipulation by collusion may be regulated under the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. However, it is necessary to add related regulations while preparing applicable acts concerning the issuance and transaction of cryptocurrencies to clarify its legality.

Response measures in terms of criminal procedural law

- Introduction of online search or network investigative techniques (NIT) so that investigations directly targeting networks and cyberspace can be carried out.
- In order to investigate a dark net, creating a certain identity may be necessary. Therefore, introducing an undercover investigator system under the Criminal Procedure Act could be discussed.
- Under the current Criminal Procedure Act, it is presumed that a warrant is issued in paper. However, we request amending the Act so that issuing and serving a warrant can be performed electronically in the future.
- A discussion on the procedures for and methods of seizing cryptocurrencies has often been requested. In order to seize cryptocurrencies by account creation and transfer, a court or an investigative agency must make its own account and establish procedures for its management. In addition, regulations on handling fees incurred in the process of transfer and procedural regulations are necessary so that the process of transfer can be officially recorded, documented, and stored for a certain period of time.
- In addition, it is difficult to obtain account information required for seizuring cryptocurrencies unless a criminal suspect or a criminal defendant voluntarily submits the information. Therefore, the scope of a search and seizure warrant should include personal records (PC, mobile phone, memo, etc.) of the criminal suspect or the criminal defendant so a court or an investigative agency can find information necessary for cryptocurrency transactions by using the information obtained from the warrant.

Response measures in terms of criminal policy

- Legislation to strengthen cybersecurity, such as reestablishing cyber security standards for the Internet of Things, to be established.
- It is also necessary to explore means to utilize the Internet of Things or blockchain in the criminal justice system. As for the Internet of Things, in order to facilitate the use of police cameras that are currently in use, a system where such devices are connected to the network and the data from the devices can be transferred via the network is needed. On the other hand, the applicable legislation regulating the operation need to be established.
- Reestablishing education programs to improve the efficiency and expertise of investigations and trials related to cybercrime and introducing courts dedicated to cybercrime.
- A "data protection impact assessment" needs to be carried out for the IoT. Guidelines should be prepared and provided to avoid confusion from legal inadequacy in the cryptocurrency investigation process.

Expected Effects of Policies

Contribution to the establishment of national criminal policy in the era of the Fourth Industrial Revolution

- Contribution to the preparation of comprehensive national strategies and policies in the era of the Fourth Industrial Revolution by checking the implications of the development of cutting-edge science and technology for crime patterns and the criminal justice system.
- Availability of criminal justice policy data that reflect the technical characteristics of the IoT and blockchain.

Establishment of the legal and institutional foundation for the commercialization of the IoT and blockchain

- Conducting a preemptive review of issues surrounding infringement of rights and criminal abuse that may arise as the IoT and blockchain become widely used.
- Creating a legal and institutional foundation for the era of the Fourth Industrial Revolution by suggesting means for improving criminal law and criminal policy in the era of network innovation.

◆ ◆ ◆

Change

Human Behaviors

Community Response

Social System

KIC Korean Institute of Criminology

Email secretariat@kic.re.kr **Telephone** 82 2 3460 9253

Address 114 Taebong-no, Seocho-gu, Seoul, 06764, Republic of Korea