DOI: 10.56794/VSSR. 2(214).3-14

Identifying Theoretical Issues in Vietnamese Criminal Laws under Impacts of Fourth Industrial Revolution

Trịnh Tiến Việt*

Received on 26 December 2022. Revised on 10 January 2023. Accepted on 2 February 2023.

Abstract: The Fourth Industrial Revolution has multidimensional impacts, not only bringing significant advantages and substantial benefits to society, but also posing threats and potential dangers. These include infringements upon security, national sovereignty, social order, safety, human rights, and citizens' freedoms. Therefore, to promptly address current and potential acts harmful to society that have caused or may cause damage, as well as anticipate changes in methods and acts of committing crimes facilitated by Industry 4.0, this paper identifies new theoretical issues in Vietnam's criminal laws under the influence of Industry 4.0. It aims to provide inputs for policymakers in the development and improvement of criminal laws. The following are the key recommendations: 1) Legislators should collaborate with technologists and scientists in other fields to develop a law on artificial intelligence (AI) soon; 2) There should be a comprehensive review of theoretical issues and awareness related to all AI-related matters; 3) The legal system and relevant laws pertaining to Industry 4.0 and associated laws of the Penal Code, often referred to as "satellite" laws, should be further reviewed and improved. This will help establish a comprehensive legal framework for crime prevention and other procedural laws.

Keywords: Criminal law; industry 4.0; crime; crime constituent; criminal liability.

Subject classification: Jurisprudence.

1. Introduction

Currently, we are experiencing the ongoing industrial revolution commonly referred to as the *Fourth Industrial Revolution* or *Industry 4.0*. The term *Industry 4.0* was initially introduced in 2011 at a technology expo held in Hannover, Germany, and has since gained global recognition. This revolution signifies a growing trend of integrating virtual and real systems, as well as the utilization of technologies such as the Internet of Things (IoT) and

* University of Law, Vietnam National University, Hanoi.

Email: ttviet@vnu.edu.vn

Internet of Systems (IoS) on a global scale (Klaus Schwab, 2018). Its impact extends to all countries, including Vietnam.

Hence, Industry 4.0 has brought about unprecedented and substantial changes, making it the most transformative revolution in history. It has given rise to global trends across various domains, encompassing a wide range of subjects and movements that were previously unimaginable. Referred to as *the revolution of convergence and savings* (Phan Xuân Dũng, 2018: 57), Industry 4.0 has continuously and comprehensively impacted the economy, society, culture, politics, national security, policies, and laws. These impacts extend to all entities and governing bodies, including the government, ministries, departments, businesses, organizations, and the general population. The multidimensional impacts of Industry 4.0 offer significant advantages and substantial benefits to society. They have resulted in notable advancements and cost savings in various aspects of human life. Examples of these advancements include implant technology, pocket supercomputers, storage services, the IoT, smart cities, automated cars, and artificial intelligence (AI) (Klaus Schwab, 2018: 201-279). However, alongside these benefits, Industry 4.0 also introduces threats and potential dangers that pose risks to society. These include encroachments on security, national sovereignty, social order, safety, human rights, and citizens' freedoms. To address these challenges, the Party and the Government have issued resolutions and legal documents to govern the profound and systemic changes brought about by Industry 4.0. These actions aim to establish *political and social bases* to effectively navigate this transformative era.

On April 14, 2016, Vietnam Prime Minister issued Decision No.623/QD-TTg approving *The National Strategy on Crime Prevention from 2016 to 2025 with a vision to 2030*, emphasizing the importance of "further developing and improving the legal system, focusing on timely researching, forecasting, codifying newly arising acts harmful to the society" (Vietnam Government, 2016: 65).

On May 4, 2017, the Prime Minister issued Directive No.16/CT-TTg titled "Strengthening capacity in accessing the Fourth Industrial Revolution". This directive outlines the necessary measures to ensure cyber safety and security within the context of Industry 4.0. It emphasizes the importance of developing a socialist rule of law state that serves the interests of the people and is governed by the people.

On July 25, 2018, the 12th Politburo issued two significant resolutions: Resolution No.29/NQ-TW titled *The National Defence Strategy in Cyberspace* and Resolution No.30/NQ-TW titled *The National Cyber Security Strategy*. Both resolutions hold immense importance for the Party and the Government as they provide guidance and manage tasks related to national defense within the new domain of cyberspace. They are in line with the resolutions of the XII National Party Congress, which focus on the construction and defense of the Fatherland, the development of a secure and healthy cyberspace, and the establishment and protection of sovereignty and national interests in cyberspace. These resolutions aim to

enhance the capacity to prevent, detect, and counteract conspiracies and activities by hostile and reactionary forces in cyberspace. They emphasize the need to be prepared to actively and effectively address any potential challenges and possibilities that may arise in this domain.

On September 27, 2019, the Politburo issued Resolution No.52-NQ/TW titled *Guidelines and Policies on Proactive Participation in the Fourth Industrial Revolution*. This resolution laid out strategic and comprehensive directions, outlining objectives until 2025 with a vision for the year 2045. It included guidelines and policies for proactive participation in the Industry 4.0, which encompassed the enhancement of institutions, policies, and laws.

The term *Industry 4.0* is prominently mentioned approximately 20 times in the Documents of the XIII National Party Congress of the Communist Party of Vietnam in 2021. It is referred to as both an opportunity and a challenge for innovation and reform in terms of development (Communist Party of Vietnam, 2021: 31, 34, 37, 46, 106, 110, 115, 121, 136-137, 140, 166, 201, 208, 214, 231, 235, 244). The focus is on various aspects such as promoting research, transferring and applying advanced technologies and innovations, particularly achievements in Industry 4.0, implementing national digital transformation, developing the digital economy, increasing productivity and quality, and improving the legal system (Communist Party of Vietnam, 2021: 201).

In addition, in practice, Industry 4.0 has had an impact on and brought about changes to the entire legal system (as mentioned earlier). Therefore, with its inherent protective function, criminal law has the responsibility to promptly govern and address acts that pose a danger to society, whether they are occurring or have the potential to occur, resulting in damages or threats to society due to the influence of this revolution. Furthermore, it must anticipate changes in methods and strategies employed in committing crimes, taking advantage of the achievements of Industry 4.0. The state employs various methods and measures, including criminal laws, for self-defense and protection. This approach is implemented through criminal legislation, leading to the creation of a comprehensive set of regulatory documents that define crimes, criminal liability, and punishments.

Hence, the analysis of the political, social, and practical foundations mentioned above has confirmed the significance of scientific research in comprehensively identifying positive changes and new theoretical issues concerning Vietnamese criminal laws under the influence of Industry 4.0, as presented in Sections 2 and 3 below. Utilizing synthetic, analytical, and forecasting methods, this article proposes hypotheses regarding the theoretical issues that should be addressed in criminal law science under the influence of Industry 4.0. Subsequently, it discusses how Vietnamese criminal laws should respond and adapt to these influences through revisions, amendments, and the implementation of "satellite laws" to meet the requirements of crime prevention, protection of national sovereignty and security, maintenance of social safety and order, as well as the preservation of human rights and citizens' freedoms in the new context.

2. Positive transformations of Vietnam's criminal laws amid Industry 4.0

A thorough analysis of the scope of Industry 4.0 and the effective application of its advancements have demonstrated positive impacts on society, including Vietnamese criminal laws:

2.1. Innovations and reforms in legal education, including criminal laws

Industry 4.0 has influenced legal education, raising concerns about the need to reform our approach to legal subjects, legislative techniques, and specific limitations in digitalization and the application of artificial intelligence (AI), big data, and more. Therefore, it is crucial to reform legal education, including criminal law education. Specifically, the curricula of legal education and train-the-trainer programs must incorporate modules on digital technologies, electronic data, cybersecurity, AI, intellectual property, digitalization of teaching materials, and even intelligent robots equipped with knowledge of international laws, codes of conduct, ethics, and human rights. National borders and territories have transformed into "soft borders and virtual space" without limitations. Several documents issued by the Party, the State, the Government, ministries, and departments have provided a political, social, and legal framework for researchers, policymakers, agencies, and organizations to address emerging acts that pose dangers to society in this new context.

2.2. Achievements and applications of Industry 4.0 for researching, developing, and enforcing criminal laws

The advancement of science and technology, the effectiveness of technological tools, surveys, assessments, presentations, and the storage of research results (big data), have facilitated the study and teaching of criminal law, leading to the development and implementation of comprehensive strategies and plans for the effective enforcement of criminal laws in practice. For example:

(1) The future implementation of *Crime forecast technology* – PredPol (Prediction Police) in Vietnam, which predicts crimes based on the timing and locations of past crimes combined with sociological information on the behaviors and patterns of these crimes. This technology helps clarify trends and features of criminals and identifies offenders (Trúc Phạm, 2023).

(2) The possibility of *Inclusive coverage of the global internet* (IoT) assists legislators in timely accessing and effectively utilizing a large amount of big data related to trends and useful experiences in criminal legislation from around the world. It allows for prompt, multi-dimensional feedback from various sectors of society on criminal law provisions that have been or will be issued by the State.

(3) The application of the *Domain Awareness System* (DAS) developed by Microsoft, which includes technologies such as "fingerprints" of the brain (through crime memories imprinted in the brains of offenders) or 3D-image skull scanning identity technology, in Vietnam.

2.3. Timely issuance of plans, tactics, and programs for crime prevention and effective dissemination of criminal laws

The issuance of decisions, the enforcement of crime prevention and investigation, and the application of preventive measures to minimize societal consequences such as rescue operations, emergency services, and fire prevention are now more responsive and efficient. Furthermore, the inclusive coverage made possible by Industry 4.0 also plays a crucial role in promoting cooperation in crime prevention among different areas, localities, nations, and regions at both national and international levels. Additionally, Industry 4.0 enables the effective digitalization of knowledge, information, materials, and legal documents for widespread dissemination through the internet. This facilitates the spread of provisions of criminal laws and expands access to legal documents for all segments of society, thereby increasing awareness and compliance with the laws and guiding public opinion in crime prevention. In the future, AI will be utilized in implementing this task within criminal laws.

Notably, citizens can provide comments, feedback, and monitor law enforcement through an open mechanism that ensures the accountability of judicial agencies. As citizens are not only subjects affected by policies but also have the right to monitor the operations of state agencies, it becomes important to disseminate legal documents to all citizens and encourage their participation in the development of policies and laws. Consequently, ensuring the active participation of citizens in the development of policies and criminal laws will play a significant role in ensuring transparency and the efficiency of local authorities (Huỳnh Ngọc Chương, 2016: 21).

2.4. Cost savings in crime investigation and settlement, as well as offender education and rehabilitation

Thanks to the scientific and technological applications in crime prevention, crimes are promptly resolved, minimizing consequences and saving costs for the State and society, allowing resources to be allocated to other tasks. Furthermore, by harnessing the achievements of Industry 4.0, judicial agencies not only remotely prevent crimes, thus reducing damages and costs associated with such crimes, but also employ AI and other technologies to monitor the execution of punishments in the community, on the streets, and within prisons (Ying-Lung, Tenge-Yang, and Liang-Chih, 2023). As a result, Industry 4.0 has clearly demonstrated useful and practical impacts on Vietnamese criminal laws.

3. Theoretical considerations in Vietnamese criminal laws and effective response measures amid Industry 4.0

In addition to the positive achievements and impacts of Industry 4.0, Vietnam's criminal laws have also encountered a number of challenges and issues. The "core" elements of criminal laws, which pertain to crimes, criminal liability, punishments, and protective functions, have lagged in terms of awareness and education. This backwardness has led to the emergence of new legal issues in practice, which may seem contradictory or unsuitable for the present and the future. Therefore, it is essential to conduct research and training on criminal laws that can be promptly updated and responsive to modern digitalization, big data, AI, the IoT, and others. In the context of Vietnam's criminal laws, it is crucial to identify and implement effective measures to address the impacts of Industry 4.0:

3.1. Crimes

Currently, criminal laws define crimes as actions that are harmful to society, committed by either natural persons or legal persons (through their representatives), involving a culpable element that violates social relations defined and protected by criminal laws (Vietnam National Assembly, 2017). However, advancements in physical technology, information technology (IT), smart cities, sharing economies, and particularly AI within the context of Industry 4.0 have raised potential changes in awareness, such as:

(1) Acts that are harmful to society committed by "transcendent" intelligent robots (also referred to as electronic or AI entities) under the direction or control of human beings, or by AI entities operating at the highest level of autonomy and transcendency, surpassing the intelligence of even the most brilliant human beings (Walsh, 2019: 74-75). Criminal liability may not be applicable to any specific subject in these cases. Additionally, there are predictions that "digital humans" will emerge in 2062 (Walsh, 2019: 29).

(2) Acts harmful to society are not limited to physical environments (traditional settings) but also extend to cyberspace, extraterrestrial space, outer space, and other planets. This has resulted in emerging issues concerning the subjects of new crimes (if any) and the validity of criminal laws in cyberspace (Vietnam National Assembly, 2014, 2018) and the objects that crimes infringe upon. Furthermore, with the development of "transcendent" AI, the term "AI crime" (Artificial Intelligence Crime, AIC) has also emerged (King, Aggarwal, Taddeo, Floridi, 2020: 89-120). The question arises whether AIC should be considered a new category of crime or a traditional crime committed by both human beings and AI entities, or solely by human beings through AI systems. All of these considerations should be taken into account when revising and amending the comprehensive definition of crime at a later stage, once sufficient theoretical and practical foundations have been established, similar to the process of including commercial entities

as subjects of crimes, which automatically necessitated the revision of definitions, punishments, and relevant institutions within criminal laws.

Based on this rationale, the theory of "legal science fiction" (Hallevy, 2010; Abbott, Sarch, 2019) predicts that if AI entities in the form of robots become subjects of new crimes in the future, it is important to supplement the definition of crime to include these subjects. Moreover, the classification of crimes committed by these new subjects should be specified. Additionally, if AIC is deemed a new category of crime, it is crucial to develop a new definition of AIC. AIC refers to acts harmful to society committed by human beings (which may include legal entities) through AI systems or AI entities, depending on their level of "intelligence", transformation and development, autonomy, and ability to independently engage in relevant acts, thereby violating social relations defined and protected by criminal laws and warranting penalties.

Currently, criminal law experts and technologists have begun studying AIC, identifying various types (King, Aggarwal, Taddeo, Floridi, 2020: 69). These types include: (1) Crimes related to commerce, financial markets, and bankruptcy (encompassing actions such as price fixing, collusion, underground transactions involving insider information, and market manipulation); (2) Crimes related to harmful or dangerous medications (encompassing smuggling and sales of prohibited drugs); (3) Crimes against human beings (encompassing murder, human trafficking, bullying, and harassment); (4) Sexual crimes (including rape, sexual assault without consent, sexual touching without consent, and sexual intercourse with minors or individuals under 18 years old); (5) Crimes related to theft, fraud, document falsification, and impersonation (highlighting the significant use of machine learning technologies and AI in conducting business beyond the business community) (King, Aggarwal, Taddeo, Floridi, 2020: 69-106), among others.

Therefore, it is crucial to establish a framework for the development and provision of new crimes, the classification of crimes, and the definition of AIC.

3.2. Crime constituents

Based on the definition of crime mentioned earlier, one may question how the constituents of crime, in terms of traditional elements, could change in the future due to advancements in AI. As machines, in the form of artificial intelligence, continue to evolve and enhance their performance through algorithms and other means, they may reach a transcendent level of intelligence by incorporating billions of data points based on big data. Clearly, this poses several challenges:

(1) Objects of crimes: There is a possibility of new social relations being violated or threatened by acts that harm society. In the context of globalization and Industry 4.0, issues related to cyberspace, particularly the protection of cybersecurity, cannot be effectively

addressed by any single nation alone. International cooperation is necessary in this regard. Simultaneously, national criminal laws should ensure the timely safeguarding of the safety and protection of these objects. The Cybersecurity Law of 2018, for instance, outlines the responsibilities of the state in implementing measures to protect national cyberspace and prevent acts that infringe upon national security, social order and safety, as well as the lawful rights and interests of online agencies, organizations, and individuals. Therefore, "cybersecurity" should be explicitly recognized and defined as an object of protection in national criminal laws (specifically stated and supplemented in Article 1 and Article 8 of the Penal Code 2015). Furthermore, provisions concerning any relevant constituents of crimes that violate this object should be amended in the section on specific crimes of the Penal Code to ensure prompt handling of such offenses. Consequently, the effectiveness of criminal laws is crucial in this realm.

(2) Actus Reus: There is a possibility of acts being committed by AI entities or other subjects utilizing AI. This raises the question of changes in the venues where crimes occur and the resulting consequences. Additionally, new methods and tactics for committing crimes may emerge. Therefore, in light of the aforementioned changes, it is crucial to raise awareness regarding acts committed by AI or other subjects through the use of scientific and technological advancements, such as money laundering, fraudulent appropriation of assets, terrorism, and other "non-traditional" crimes (Trịnh Tiến Việt, 2019: 91-96). These crimes must be acknowledged and addressed through specific provisions in national criminal laws. Moreover, the locations where crimes are committed might be far removed from where the harmful consequences to society occur. Even with advancements in physical technology and IT, these locations could extend to cyberspace, outer space, or other planets. Consequently, the harmful consequences to society may manifest in numerous countries and territories worldwide, resulting in various types of physical and psychological harm to individuals, organizations, as well as threats to life, health, residential areas, and territories.

For instance, concerning the "places" where crimes are committed, an additional paragraph 2 of point 1 in Article 5 is included in the Penal Code 2015. This provision is also applicable to acts of committing crimes or the consequences of such acts on Vietnamese planes, ships, exclusive economic zones, and continental shelves. However, in response to the impact of Industry 4.0 and in comparison to the criminal laws of other countries such as Germany and Finland, this provision clearly does not encompass certain circumstances. For example, it does not cover cases where crimes are committed by accomplices, or instances where offenders prepare to commit crimes but fail to do so. Consequently, it fails to address the complex dynamics related to acts of committing crimes that cause harmful consequences to society in one or more than two locations. These crimes often remain unresolved when detected in one location, as they have occurred in another. If harmful acts are committed in cyberspace without any punishment,

the effectiveness of criminal laws is diminished, as they do not adequately protect the interests of the community and human beings.

(3) Men's read: The identification of faults and the determination of penal liability for new acts that harm society can be challenging. In addition to acts committed by natural persons and legal entities, the question arises of how to attribute faults to acts committed by AI entities or other subjects using AI. It raises questions about when penal liability should be independently applied, when it should be applied to accomplices, and when it should not be applied at all.

Consider the following scenario: If a transcendent AI system (robot) is used to monitor and process medical data but autonomously alters the data, leading to incorrect treatment of patients, should this be considered an act harmful to society?

The alteration of data occurs during the AI's thought process. If penal liability is examined in such a case, it may be based on subjective conviction. However, if no penal liability is applied, a significant danger to society might be overlooked. It is impossible to determine the penal liability of any individual or organization for this act, as it involves unpredictable "self-transformation" and "self-changing" during the AI's learning, transforming, and adapting processes.

Moreover, at a more advanced level of "fiction science", where the "self-awareness" of a transcendent AI leads to grave consequences, it becomes important to consider the elements analyzed in point (4) below to identify and determine faults and criminal liability, particularly in a future where autonomous cars become prevalent.

(4) Subjects of Crimes: Do new subjects of crimes arise? In addition to natural persons and legal entities, AI entities might become new subjects of crimes. AI is also defined as a computer or machine capable of reasonable actions and thinking, exhibiting actions or thinking similar to those of human beings, and even surpassing human beings' capacity to act more precisely or accurately than human beings themselves (Russell, Norvig, 2010: 2). The world is demonstrating a strong commitment to addressing international terrorism, transnational crimes, and the production of biological and nuclear weapons, among other concerns. This is because if the key to controlling AI falls into the hands of individuals, organizations, or nations, it could be exploited to engage in the aforementioned activities, posing a threat to entire regions and the world.

Currently, research findings have identified 26 potential new types of AI (Kelly, 2018: 81), and this number continues to grow. However, AI development may undergo significant changes in this field in the near future (Claussén-Karlsson, 2017: 12-14). Notably, international AI researchers believe that at some point, AI might advance significantly (Trúc Phạm, 2023), surpassing human control and giving rise to warnings of a potential future disaster: AI endangering the safety of human beings or marking the end of the human era (Barrat, 2013: 35-68). Therefore, in practice, acts that are harmful to society, committed either by AI entities themselves or by other subjects (individuals, organizations) using AI entities as tools for criminal activities, might occur in the near

future (possibly in fiction), resulting in the emergence of AIC. As a result, legislators should collaborate with technologists to develop and amend provisions regarding the potential types of criminal liability for entities in the following circumstances: (i) AI entities as subjects of crimes (Mosechkin, 2019); (ii) AI entities as intermediaries and/or tools for committing crimes; (iii) AI entities sharing joint criminal liability (as accomplices); and (iv) subjects using AI not bearing criminal liability. Consequently, faults and criminal liability can be precisely defined (Trịnh Tiến Việt, 2020: 240-275), laying the groundwork for the development of AI Law as a specialized legal framework to address these crimes in addition to existing criminal laws.

3.3. Criminal liability and punishments

From a logical standpoint, changes in the definition of crimes, such as those committed by AI robots, naturally lead to changes in the definition of punishments and other forms of criminal liability. In this case, AI is an intangible entity existing within a tangible form. The question arises whether AI itself or the physical entity containing AI should be held accountable for criminal liability. Consequently, the current criminal punishments are outdated and insufficient when dealing with these new subjects, among other considerations. It is crucial, therefore, to amend and supplement relevant provisions on punishments and their objectives in the Penal Code of 2015 to promote and safeguard human rights.

Simultaneously, with the emergence of two potential new subjects of crimes, namely AI itself or other subjects using AI to commit crimes, and in light of scientific and technological advancements, it becomes vital to establish criminal coercive measures with a technological, monitoring, and positioning nature to prevent crimes and recidivism. These measures could include seizing and destroying AI software, confiscating accounts and blocking access, and implementing the use of positioning bracelets, among others. Furthermore, if AI entities are designated as subjects of crimes, it is important to define potential punishments applicable to AI entities, such as community service, temporary suspension for a specified period, or the removal of AI software controlling the AI entity (Trịnh Tiến Việt, 2021a, 2021b).

3.4. Areas at high risk of crime increase or the occurrence of new acts harmful to society in the context of Industry 4.0

In addition to the visible changes analyzed above, among the new areas of Industry 4.0 to be applied in Vietnam, some might be used by individuals to commit new crimes or acts harmful to society as follows:

(1) Internet of Things (IoT): This is an interconnected system of computer devices, machines, objects, animals, or human beings that are provided with a unique identity and the ability to transmit data through the internet without any human-to-human or human-to-

computer interaction. IoT includes the highest convergence of wireless technology, micro-electromechanical systems (MEMS), micro-services, and the internet (Macías, Navarro, and González, 2019: 31). However, it is forecasted that there will be an increase in crimes in aviation, banking, economics, and finance, as criminals have produced malicious codes and malware targeting these areas.

(2) Big data: Big data contains valuable and useful information that helps inform scientific research, business operations, transportation, epidemic forecasts, etc., thus assisting the governments in forecasting the unemployment rate, future career trends for investment or expenditure reduction, and stimulating economic growth (Gogołek, 2019: 212-217; Zhang, Liu, 2019: 10). However, this area is forecasted to see an increase in crimes relating to the infringement of personal confidential information, secrets of agencies and organizations, as well as crimes in IT, telecommunications, and competition.

(3) Sharing economies: Sharing economies might exist in various forms (Li, 2019: 1-20), including the use of IT to provide individuals, corporations, non-profit organizations, and authorities with relevant information to maximize resources through redistribution, sharing, and reuse of redundant capacities. However, this area is forecasted to see an increase in crimes relating to economic management, such as violations of regulations on distribution, competition, tax evasion, and money laundering, as governments have to manage and control information, electronic transactions, international payments, and the prevention of tax evasion.

(4) Bitcoin: This is a type of digital currency decentralized by an open-source code issued in 2009 (Halaburda and Sarvary, 2016: 34). Bitcoin operates without a banking system or borders, based on advanced coding algorithms and the Bitcoin Protocol (platform) with an open source. Bitcoin traders might choose an anonymous mode, i.e., no requirement on names and addresses (Lele, 2019: 197). However, in practice, although many citizens and civil servants have a vague awareness of this area, they have still rushed into bitcoin speculation, exposing themselves to extremely high risks, as bitcoin is not recognized as property by laws. Therefore, it is forecasted that crimes relating to obtaining property by fraud through using the cryptocurrency bitcoin for money laundering, trading in weapons, drugs, financing terrorism, etc., will occur.

(5) Artificial intelligence (AI): It is important to timely research and deal with new subjects of crimes in the future (which might be fiction) or new AIC that aim to obtain property by fraud, infringe upon cybersecurity, attack security systems, and appropriate materials, accounts of individuals and organizations in banking, aviation, and finance sectors. Subsequently, new acts harmful to society committed by natural persons and legal entities might occur, such as manufacturing and producing AI products with the ability to self-replicate, self-create languages and programs; using AI to impersonate behaviors, gestures, and voices of other people causing damage to individuals and organizations; and using AI for terrorist purposes and infringing upon national security. Consequently, all of

these changes require specific provisions and research in each area, as well as amendments to the Penal Code 2015 and related laws for effective crime prevention.

4. Recommendations for Vietnam

To meet these requirements, three recommendations for comprehensive measures to respond to changes in awareness of Vietnam's criminal laws under the impact of the Industry 4.0 are proposed as follows:

First, legislators should collaborate with technologists and scientists in various fields such as psychology, neuroscience, and linguistics to promptly develop a *Law on AI*, focusing on key issues as outlined below:

(1) General provisions on policies, principles, and scope of governance.

(2) Processes/procedures for research, manufacturing, production, registration, and ownership.

(3) Areas utilizing AI.

(4) Processes/procedures for checking, monitoring technologies, and technical solutions for response.

(5) Punishments to address violations related to AI, including administrative, civil, and criminal penalties.

Second, concerning the impacts of the Industry 4.0 on criminal laws, it is crucial to comprehensively review theoretical issues and awareness, including:

(1) Revise and amend the definition of crimes with new awareness to account for AI entities as potential subjects of crimes or subjects bearing joint criminal liability. Additionally, include provisions for crimes committed in cyberspace as objects of crimes. Utilize the advancements of Industry 4.0 as tools/means in the provisions of the General Part of the Penal Code, such as the validity of the Penal Code and extenuating circumstances for criminal liability.

(2) Revise and amend provisions on the classification of crimes to encompass crimes committed by AI entities, individuals, and legal persons through AI. Define and specify the governance of AI crimes, if applicable.

(3) Review the provisions on specific crimes in the Penal Code of 2015 to consider revising the provisions on crime constituents, conditions for examining criminal liability, and the presence of "transnational" signs. This is done to address the new context of globalization and the organized nature of crimes, especially non-traditional crimes like terrorism against the people's administration, gambling, money laundering, and crimes in IT and telecommunication networks. Conduct research on the possibility of joining the Convention on Cybercrime and developing specific provisions on cybercrime in Vietnam,

which establish limitations on the impacts of international social networks on national security. Currently, some countries have taken advantage of ownership of social networks like Facebook, Twitter, Google, Yahoo, and YouTube to covertly exploit intelligent information. They spend significant amounts of money on promoting democracy and shaping public opinion on these networks, which profoundly and comprehensively affects and changes various aspects of religious, cultural, economic, political, and social domains, particularly concerning global national security (Nguyễn Văn Hưởng, 2014: 261-265).

(4) Review and amend criminal punishments for individuals and legal persons, and tentatively consider punishments for AI entities and AI crimes (King, Aggarwal, Taddeo, Floridi, 2020: 69-72). Alternatively, develop new criminal punishments that employ technological, monitoring, and positioning methods, if applicable.

(5) Criminalize and decriminalize acts that are harmful or no longer harmful to society. This step aims to increase or decrease preventive measures against acts detrimental to society in the context of Industry 4.0 (as referenced under point "d") of Paragraph 2, which includes the possibility of emerging harmful acts).

Third, undertake a thorough review and enhancement of the legal system and relevant laws pertaining to Industry 4.0, as well as the "satellite" laws of the Penal Code, to establish a comprehensive legal framework for crime prevention and other procedural laws in response to the impacts of Industry 4.0. This includes:

(1) The Law on High Technologies of 2008, with revisions in 2013 and 2014.

(2) The Law on Information Technology of 2006.

(3) The Law on Cyber Information Security of 2015.

(4) The Law on Cyber Security of 2018, along with legal documents addressing specific issues such as cryptocurrency and 3D printing technology.

(5) The Criminal Procedure Law and the Law on Enforcement of Criminal Judgements, considering the influences of Industry 4.0.

While these laws may not directly align with the content and scope of this research, they are considered "satellite" laws and procedural laws that contribute to the establishment of a comprehensive legal system for crime prevention. These aspects will be further examined in separate research endeavors.

5. Conclusion

The advent of Industry 4.0 has not only brought about positive impacts but has also presented significant challenges to the political, economic, cultural, and social aspects, policies, and legal systems of all countries, including Vietnam. These challenges necessitate comprehensive changes across the entire system and all areas of social life and legal

frameworks to adapt to the new context. The emergence of Industry 4.0, coupled with issues like non-traditional security, globalization, and the Covid-19 pandemic, has posed significant challenges that require various approaches, including the utilization of criminal laws.

Hence, it becomes imperative to promptly address new theoretical issues and adapt the criminal justice system in general. Vietnam's criminal laws need to effectively respond to the challenges brought by this revolution and the evolving context. By doing so, they can contribute to the successful implementation of the guidelines outlined in the Resolution of the 13th National Party Congress. This includes timely and effective measures against crimes, particularly transnational and organized crimes, high-tech crimes, and more. It also involves continuous improvement of policies and laws related to national defense, national security, and international integration, in line with the requirements of safeguarding the homeland in this new context (Communist Party of Vietnam, 2021: 279-281).

References

Abbott, R., Sarch, A. F. (2019). Punishing artificial intelligence: Legal fiction or science fiction (February 1, 2019). *53 UC Davis Law Review*, *323*(1). DOI: http://dx.doi.org/10.2139/ssrn.3327485

Barrat, J. (2013). *Our final invention, artificial intelligence and the end of the human era*. Thomas Dunne Books.

Claussén-Karlsson, M. (2017). Artificial intelligence and the external element of the crime, an analysis of the liability problem. [JU101A, Final Thesis for the Law Program, Second Cycle, 30 Credits].

Communist Party of Vietnam. (2021). *Documents of the 8th National Party Congress*, Vol. 1. National Political Publishing House.

Gogołek, W. (2019). Refining big data. *Bulletin of Science, Technology & Society*, *37*(4). DOI: https://doi.org/10.1177/02704676198640

Hallevy, G. (2010). The criminal liability of artificial intelligence entities – from science fiction to legal social control. *Akron Intellectual Property Journal*, *4*(2).

Halaburda, H., Sarvary, M. (2016). *Beyond bitcoin the economics of digital currencies*. Palgrave Macmillan. New York.

Huỳnh Ngọc Chương. (2016). Participation of citizens in public policies under impacts of social networks in Vietnam: A case study. *Science & Technology Development*, Vol. 4.

Kelly, K. (2018). *Twelve technological trends under the industry 4.0.* National Economics University Publishing House. Hanoi.

King, T.C., Aggarwal, N., Taddeo, M. *et al.* (2020). Artificial intelligence crime: an interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, Vol. 26. DOI: https://doi.org/10.1007/s11948-018-00081-0

Lele, A. (2019). *Blockchain in disruptive technologies for the militaries and security.* Springer.

Li, Y. (2019). Governing the sharing economy smartly, a tale of two initiatives in China. *Public Policy and Administration*, *36*(1). DOI: 10.1177/0952076719852421

Macías, A., Navarro, E., & González, P. (2019). A Microservice-based framework for developing internet of things and people applications. *The 13th International Conference on Ubiquitous Computing and Ambient Intelligence UCAmI 2019.* Toledo.

Mosechkin, I. H. (2019). Artificial intelligence and criminal liability: problems of the formation of a new type of subject of crime. *Bulletin of St. Petersburg State University, Law, 10*(3) (in Russian language).

Nguyễn Văn Hưởng. (2014). *Non-traditional security: Threats, challenges, policies and countermeasures in Vietnam*. Vietnam National University Press, Hanoi.

Phan Xuân Dũng. (2018). *The fourth industrial revolution – the revolution of convergence and savings.* Science and Technology Publishing House. Hanoi.

Russell, S. J., Norvig, P. (2010). *Artificial intelligence, a modern approach*. Prentice Hall.

Schwab, K. (2018). *The fourth industrial revolution*. National Political Publishing House. Hanoi.

Trịnh Tiến Việt (ed.). (2020). *Vietnam criminal policies and challenges of the industrial revolution 4.0.* Justice Publishing House. Hanoi.

Trịnh Tiến Việt. (2021a). Punishments against artificial intelligence (AI) entities: From science fiction to the future perspective of Vietnam penal code in a "certain year". *People's Court Journal*, Vol. 4.

Trịnh Tiến Việt. (2021b). Awareness on non-traditional security under the 13th National Party Congress and arising issues in Vietnam criminal laws. *Communist Review, 970*(7).

Trúc Phạm. (2023). Predpol – crime prevention software. *World Security Online*.

Vietnam Government. (2016). *Official Gazette*, Vol. 299 + 300.

Vietnam National Assembly. (2017). *Penal code 2015, revised and amended in 2017.*

Vietnam National Assembly. (2018). *Law on cybersecurity*.

Vietnam National Assembly. (2014). *Law on high technology 2008, revised in 2013, 2014*.

Vietnam Prime Minister. (2016). *Decision No.623/QD-TTg on approval of "National strategy on crime prevention in the period of 2016-2025 with a vision to 2030"*. Hanoi.

Vietnam Prime Minister. (2017). *Decision No.1255/QD-TTg on Approval of "Project on Improvement of Legal Framework on Management and Settlement of Virtual Property, Electronic Currency, and Cryptocurrency"*. Hanoi.

Walsh, T. (2019). *2062 - Times of artificial intelligence*. (Translation). Ho Chi Minh City General Publishing House.

Ying-Lung, L., Tenge-Yang, C., & Liang-Chih Y. (2017). Using machine learning to assist crime prevention. *IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*. DOI: 10.1109/IIAI-AAI.2017.46

Zhang, C., Liu, Z. (2019). Application of big data technology in agricultural internet of things. *International Journal of Distributed Sensor Networks, 15*(10). DOI: 10.1177/1550147719881610