OFFENCE DETERMINATION IN RELATION TO CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS NETWORKS

NGUYEN VAN KHOAT*

Abstract: The article addresses theoretical issues on criminalization for crimes in the field of information technology and telecommunications networks, and focuses on analyzing the criminalization for some specific crimes in this field as prescribed in Section 2, Chapter XXI of the 2015 Penal Code, amended and supplemented in 2017.

Keywords: The Penal Code; crimes; information technology, telecommunications networks; offence determination

ĐỊNH TỘI DANH ĐỐI VỚI CÁC TỘI PHẠM TRONG LĨNH VỰC CÔNG NGHỆ THÔNG TIN, MẠNG VIỄN THÔNG

Tóm tắt: Bài viết giải quyết các vấn đề lý luận về định tội danh đối với các tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông, đồng thời tập trung phân tích việc định tội danh đối với một số tội cụ thể trong lĩnh vực này được quy định tại Mục 2 Chương XXI Bộ luật Hình sự năm 2015, sửa đổi, bổ sung năm 2017.

Từ khóa: Bộ luật Hình sự; tội phạm; công nghệ thông tin, mạng viễn thông; định tội danh

1. General issues concerning offence determination for crimes in the field of information technology and telecommunications networks

Offence determination is an indispensable and inevitable activity throughout criminal proceedings - from the institution of criminal proceedings, investigation, and prosecution to trial - because it constitutes the first necessary legal basis for the attribution of criminal liability. In practice, offence determination is a particularly significant form of law application. Accurate offence determination provides the foundation for the correct and appropriate application of both substantive criminal law and criminal procedure to the resolution of each specific criminal case, thereby ensuring that the right person is held accountable for the right offence in accordance with the law.

To date, the scholarship has advanced various definitions of offence determination. Synthesising these approaches, the author notes that, notwithstanding differences in formulation, the literature converges on the following core points.

First, at its essence, offence determination is a cognitive process of assessing whether the indicia of a socially dangerous act that occurs in objective reality correspond to the statutory elements prescribed by criminal law for a particular offence.

Second, offence determination is a practical law-applying activity when carried out by competent authorities and authorised proceeding-conducting persons in accordance with the law. By its nature, it is primarily the application of substantive criminal law; however, in the course of offence determination, the relevant actors necessarily apply the rules of criminal procedure.

Third, the determination of the offence constitutes the most crucial basis for sentencing decisions and for resolving other issues related to the offender's criminal liability.

Crimes in the field of information technology and telecommunications networks are provided for in Section 2, Chapter XXI of the Penal Code No. 100/2015/QH13 (as amended, including the amendments and supplementations in 2017)

* *Email: Khoatnv@tks.edu.vn*
PhD, Rector of Vietnam Procuratorate University

(the 2015 Penal Code (as amended)). These offences are committed by persons with criminal responsibility capacity who, with direct intent, employ advanced knowledge, skills, tools, and technological means to unlawfully interfere with information and data that are stored, processed, or transmitted via computer networks, telecommunications networks, or digital devices - thereby infringing information security and causing harm to State interests as well as the lawful rights and interests of organisations and individuals.

Accordingly, offence determination for this group of crimes may be understood as the competent authorities' practical application of substantive criminal law and criminal procedure to identify, compare, and legally record the precise correspondence between the factual indicia of the relevant conduct and the constituent elements of the offences in this field.

Offence determination for crimes in the field of information technology and telecommunications networks is of critical significance, serving as the premise for sentencing and for the resolution of other issues related to criminal liability. In practice, however, this activity may give rise to divergent interpretations, leading to different offence labels and penalty brackets, which in turn affect the determination of criminal liability and punishment. For that reason, further analysis, commentary, and clarification of the theoretical issues surrounding offence determination for this group of crimes - grounded in the examination of representative cases - remain of substantial theoretical and practical value.

2. Practical issues concerning offence determination for crimes in the field of information technology and telecommunications networks

In practice, offence determination for crimes in the field of information technology and telecommunications networks continues to involve situations in which the conducting authorities misassess or misconstrue indicia relevant to the four constituent elements of the crime. As a consequence, offence determination may yield divergent outcomes. In particular:

First, there remain inaccurate assessments of the act of *"unlawfully accessing the account of an agency, organisation or individual for the purpose of appropriating property"* as prescribed in Point (c), Clause 1, Article 290 of the 2015 Penal Code (as amended). Such misassessment of the objective aspect of the conduct may lead to confusion between the crime of *Appropriation of property by computer network, telecommunications network, or electronic devices* (Article 290) and the crime of *Theft* (Article 173).

From a doctrinal perspective, unlawful access to an account refers to intentional conduct whereby an offender bypasses warnings, access codes, or firewalls, or uses another person's access credentials without that person's consent, to access an account that is not their own and thereafter appropriate funds belonging to the account holder (here, "account" refers to a bank account or an e-wallet account). In practice, however, cases involving similar conduct have been classified differently by different agencies conducting proceedings. Illustratively:

(i) The case of Nguyen Xuan D, adjudicated by the People's Court of Nam Tu Liem District, Hanoi, for the crime of *Appropriation of property by computer network, telecommunications network, or electronic devices* (Article 290).

In September 2022, V Company Limited entered into a four-month vocational training contract with Nguyen Xuan D as a probationary sales employee. D was assigned to use the store's MoMo e-wallet to top up and withdraw money for customers. Exploiting procedural loopholes at Store C, D repeatedly logged into Store C's MoMo e-wallet account to top up a total of VND 107,000,000 into D's MoMo e-wallet account (phone number 098632xxxx) and into fourteen MoMo e-wallet accounts that D had borrowed from friends, thereby appropriating a total amount of VND 107,000,000. The People's Court of Nam Tu Liem District, Hanoi, convicted D under Clause 2, Article 290 of the 2015 Penal Code (as amended).

(ii) The case of Nguyen Thi Nh, involving appropriation of property in Yen Son District, Tuyen Quang Province.

From 24 to 28 January 2024, Nguyen Thi Nh shared a room with Ms Phan Thi H in Yen Son District, Tuyen Quang Province. On 28 January 2024, Nh assisted H in installing and successfully logging into an Internet banking application on H's phone. During the installation process, Nh memorised the application login password and formed the intention to appropriate money from H's bank account. At approximately 22:00 on the same day, upon seeing H asleep with her phone placed at the bedside, Nh surreptitiously used H's phone to access the Internet banking application and transferred VND 64,300,000 from H's account to Nh's bank account. Nh subsequently transferred the entire amount through acquaintances' accounts to convert it into cash and spent it for personal purposes.

In the course of handling this case, certain views argued that Nh's conduct satisfied the constituent elements of the crime of *Theft*. This position reasoned that, although Nh used H's Internet-connected mobile phone - an electronic device operating through telecommunications networks - to appropriate property, the objective nature of the conduct lay in covertly logging into the Internet banking account, executing a transfer, and successfully appropriating H's funds. This view further relied on the wording of Article 290, which provides (in substance) that a person who uses a computer network, telecommunications network, or electronic means to commit specified acts, *"if not falling within one of the cases prescribed in Articles 173 and 174 of this Code, shall…"* - thereby indicating that the Code accords priority to handling ownership-infringing offences first, and only thereafter considers liability under Article 290.

Thus, the conduct in the two cases above is materially similar - namely, the use of a known password to access the victim's account followed by the transfer of funds from the victim's account to the offender's account for appropriation. Yet, the conducting agencies in different localities reached different conclusions regarding the applicable offence. In the author's view, the conduct of both D and Nh should be characterised as *"unlawfully accessing an individual's account (a bank account or an e-wallet account) for the purpose of appropriating property"*: The offenders intentionally used another person's access credentials without consent to access an account that was not their own, and thereafter appropriated the account holder's funds.

Second, there remain inaccurate assessments of the act of *"Commit frauds in electronic commerce, electronic payment, online currency trading, online capital raising, online multi-level marketing, or online securities trading for property appropriation"* as prescribed in Point (d), Clause 1, Article 290 of the 2015 Penal Code (as amended). Mischaracterisation of this objective conduct may result in confusion between the crime of *Appropriation of property by computer network, telecommunications network, or electronic devices* (Article 290) and the crime of *Obtaining property by fraud* (Article 174).

From a doctrinal perspective, the conduct described in Article 290 encompasses the following principal forms:

1. Fraud in e-commerce for the purpose of appropriating property
This refers to deceptive conduct involving the provision of false information regarding all or part of the process of commercial activities conducted by electronic means connected to the Internet, mobile telecommunications networks, or other open networks. Typical manifestations may include impersonating another trader, organisation, or individual to participate in e-commerce activities, or forging or copying the interface of another person's e-commerce website to obtain benefits or create confusion, thereby enabling the appropriation of property.

2. Fraud in electronic payment for the purpose of appropriating property
This involves the use of electronic payment - i.e., payment by electronic means through the creation, sending, and processing of payment orders via electronic means (such as e-wallets, or payment through electronic gateways) - to conceal false information and induce the victim to carry

out payment operations, thereby enabling the appropriation of property.

3. Fraud in currency trading for the purpose of appropriating property This involves providing deceptive information to entice others to trade in currency-like assets, such as gold, foreign currency, or real estate, to appropriate property. The modus operandi may include: after the trading party places buy/sell orders for matching on the server, the platform operator retains such orders to capture spreads and commissions; or the platform operator fabricates circumstances - such as "hacker attacks" - or invokes purported objective impediments (e.g., power outages, system failures, connection errors with the server, failure of order matching, erroneous transactions) to appropriate property.

4. Fraud in capital mobilisation, multi-level marketing, or securities trading via the network for the purpose of appropriating property. This refers to using computer networks or telecommunications networks to establish purported "investment trading platforms" to induce others to deposit capital. After participants deposit funds, the offenders issue "investor codes", "multi-level marketing codes", or "securities trading codes" to the participants. Those codes function as "addresses" through which the offenders purport to pay interest returns, typically conditional on the participant completing "tasks," such as recruiting additional participants, to earn percentages and commissions from referrals. In reality, no genuine capital mobilisation, multi-level marketing, or securities trading takes place, and the deposited funds are not withdrawable or recoverable.

In several cases, the proceeding-conducting authorities have not clearly distinguished the foregoing forms from obtaining property by fraud, in which computer networks, telecommunications networks, or electronic means merely serve as tools or supporting instruments. For instance:

The case of Nguyen Dinh H, prosecuted for the crime of *appropriation of property using a computer network, telecommunications network, or electronic device* under Point (d), Clause 4, Article 290.

Nguyen Dinh H used computer networks and telecommunications networks to build and promote information, claiming that he had established "ECS Singapore Company" in Vietnam, purportedly specialising in blockchain technology and the business of a virtual currency called ECS, to attract investors. To operate the scheme, H hired individuals with IT expertise to write software code and develop a website interface; created the ECS token with no convertible value; and operated a website that was not licensed in Vietnam. H organised seminars and paid certain members a monthly salary to entice investors, offering investment packages of three, six, or twelve months and providing "product packages" as purported incentives. Once investors deposited funds into H's account to participate in the packages, H immediately appropriated the money, subsequently manipulated the displayed price of ECS upward, and then shut down the website. The total amount appropriated from investors was VND 2,350,763,000.

At the initial stage, the Hanoi City Police Investigation Agency instituted the case for *obtaining property by fraud* under Article 174. During the investigation, the institution later decided that the crime was *appropriation of property using a computer network, telecommunications network, or electronic device* under Article 290.

Classifying H's conduct as *obtaining property by fraud* in this case was not accurate. H hired coders to develop a website and created a trading platform that appeared genuine to attract investment and secure appropriate investors' deposits. Although H disseminated false information regarding the project, its business scope, and the company's establishment and licensing in Vietnam, the conduct in substance constituted fraud in capital mobilisation carried out via computer networks, telecommunications networks, or electronic means - one of the objective forms captured by Article 290.

In other cases, offenders employed materially similar methods (differing

primarily in the type of goods or services advertised online), yet different proceeding-conducting agencies reached different offence classifications. Illustratively:

The case of Phung Khac K, adjudicated by the People's Court of Ho Chi Minh City for the crime of *appropriation of property using a computer network, telecommunications network, or electronic device.*

Phung Khac K posted advertisements offering for sale non-existent electronic products on websites such as Rongbay.com, muaban.com.vn, 5giay.vn, and raovat.com. When customers contacted the phone number in the postings, K communicated with them and required that customers transfer deposits ranging from 10% to 50% of the purported purchase price into designated bank accounts, thereby appropriating property. After customers transferred money, they could no longer contact the phone number and did not receive the products as agreed. To facilitate the scheme, K borrowed friends' bank accounts for customers to transfer money into. Through this modus operandi, K appropriated a total of VND 196,301,153. The People's Court of Ho Chi Minh City convicted K under Clause 2, Article 290.

The case of Nguyen Hieu P, prosecuted for the crime of *Obtaining property by fraud* under Point (a), Clause 4, Article 174.

Nguyen Hieu P engaged in conduct involving computer networks, telecommunications networks, and electronic means by creating fourteen Facebook accounts and purchasing five bank accounts under other persons' names, which were then used to appropriate property. P posted advertisements on Facebook offering services such as ordering football tickets for the 2018 AFF Cup final between Vietnam and Malaysia at My Dinh National Stadium, booking air tickets and hotel rooms, arranging travel services, and paying electricity bills, within Facebook groups. After customers contacted P to place orders, P required them to pay deposits or fees into the bank accounts they had used to purchase. P then blocked further contact and withdrew the funds for personal use. P defrauded ninety-six victims of a total amount of VND 757,557,399. The People's Procuracy of Hanoi prosecuted P for *"Obtaining property by fraud"* under Article 174.

It can be seen that, in the two cases above, K and P employed broadly similar methods. Both posted false information about goods or services on online platforms and then required victims to transfer deposits into designated bank accounts. Those bank accounts were purchased or borrowed from others to conceal identity and facilitate evasion by cutting off contact after receiving funds. Nevertheless, the conducting agencies in different localities adopted different offence classifications.

In the author's view, the conduct of both K and P should be characterised as the conventional offence of *obtaining property by fraud*. Advertising goods or services on the Internet or Facebook where no such goods or services in fact exist does not amount to "fraud in e-commerce", because the offenders merely exploit the speed and reach of online platforms to promote fictitious goods or services, rather than providing false information about part or all of the process of e-commerce activities. Likewise, requiring customers to transfer deposits or payments into bank accounts purchased or borrowed by the offenders does not constitute "fraud in electronic payment" because the transfer does not involve deception in the creation, sending, or processing of the payment order - the victim creates and sends the payment order of their own accord. Only where the payment process itself involves deception in the creation, sending, or processing of payment orders should it be regarded as fraud in electronic payment.

Third, there remain inaccurate assessments of the act of *"Illegal infiltration into the computer network, telecommunications network, or electronic device of another person"* as prescribed in Article 289 of the 2015 Penal Code (as amended). Mischaracterisation of this objective conduct may lead to confusion between this offence and the offence of *appropriation of property using a computer network, telecommunications network, or electronic device* (Article 290).

Under Article 289, the objective conduct

may be carried out through methods such as: (1) Bypassing warnings, i.e., overcoming notifications that unauthorised persons are not permitted to access a database; (2) Bypassing access codes, i.e., overcoming mandatory conditions that must be satisfied before using or accessing protected devices or protected data content; (3) Bypassing firewalls to intrude unlawfully, where a firewall is a system of hardware/software components placed between two or more networks to control connections in both directions and to prevent unauthorised intrusion or connection; (4) Using another person's administrator rights, i.e., exercising the rights to manage, operate, exploit, and maintain the stable operation of a person's or organisation's computer or telecommunications network; and (5) other unlawful intrusion methods, such as cracking, stealing another person's password or cryptographic keys, or physical intrusion (e.g., unlocking doors to enter rooms or areas beyond one's authorised access) in order to access computer networks, telecommunications networks, or electronic means.

After unlawfully intruding into another person's computer network, telecommunications network, or electronic means, the offender may engage in one of the following activities: (1) Seizing control of the computer network, telecommunications network, or electronic means; (2) Interfering with the operational functions of electronic means; (3) Stealing electronic data; (4) Altering or destroying electronic data; (5) Forging electronic data; or (6) Unlawfully using services. Accordingly, where following unlawful intrusion, the offender does not appropriate property, Article 289 may apply. Where the offender additionally commits appropriation of property, the conduct should be classified under Article 290.

In practice, however, certain cases reflect inaccurate classification. For example:

The case of Ma Kien D, adjudicated by the People's Court of Hanoi for the offence of *Illegal infiltration into the computer network, telecommunications network, or electronic device of another person.*

At the end of 2017, Ma Kien D formed the intention to access Mr D's Gmail and cryptocurrency accounts to appropriate Mr D's ETH cryptocurrency. D used computers at Internet cafés to access Mr D's Gmail address and successively bypassed both the first-step password and the second-step password. D then changed the phone number linked to Mr D's Gmail to a phone number 09XXXX9866 that D had purchased in advance. After gaining control of Mr D's Gmail, D used that Gmail account to access Mr D's cryptocurrency wallet account on Freewallet.org and transferred 58.01956 ETH from Mr D's wallet to a newly created ETH wallet controlled by D. After appropriating the ETH, D offered the remaining amount for sale on a cryptocurrency trading forum and borrowed a friend's bank account to receive the equivalent amount in Vietnamese dong (VND) upon purchase. D completed six sales and obtained VND 266,620,216. In this case, both the first-instance and appellate courts determined that Ma Kien D committed the offence of *Illegal infiltration into the computer network, telecommunications network, or electronic device of another person* under Point (c), Clause 2, Article 289 (i.e., obtaining illicit gain from VND 200,000,000 to under VND 500,000,000).

In the author's view, although D's conduct targeted ETH - an electronic currency used in Internet transactions and not formally recognised in Vietnam-after appropriating the ETH, D sold it and obtained VND 266,620,216. In substance, D sought to obtain Vietnamese dong resulting from the exchange and sale of ETH. It should therefore be affirmed that D acted with the intention to appropriate property, rather than merely "obtaining illicit gain" as determined by the courts.

3. Recommendations to enhance the quality and effectiveness of offence determination for crimes in the field of information technology and telecommunications networks

To further improve the quality and effectiveness of offence determination for crimes in the field of information technology and telecommunications networks, the author proposes the following:

First, competent authorities should promptly promulgate interpretive guidance on the application of the current Penal

Code (as amended, including the 2025 amendments) to this group of offences, with a view to harmonising understanding across proceeding-conducting agencies.

As analysed above, the understanding among the authorities conducting proceedings regarding the modus operandi and the manner of applying the law to resolve cases remains inconsistent. This, in turn, has created difficulties in assessing evidence to prove criminal conduct and determine the applicable offence for this group. In practice, guidance documents used for addressing certain offences in the fields of information technology and telecommunications have often relied on Joint Circular No. 10/2012 dated 10 September 2012 - a document that has ceased to be effective, as it guided the 1999 Penal Code and is not aligned with the provisions of the 2015 Penal Code (as amended). Accordingly, central inter-agency authorities should expeditiously issue guidance specifying offence-defining circumstances and penalty-bracketing circumstances for each offence within this group.

Such guidance should also address procedures and measures for the collection, preservation, storage, and transportation of electronic evidence. Electronic data constitute a critical evidentiary source in cases of this nature; they must be converted into forms that are readable, visible, or audible, and minutes must be prepared recording the contents of the electronic data recovered and analysed before such materials can carry probative value. It is therefore necessary to develop dedicated guidance and rules on the preservation, recovery, analysis, evaluation, and use of electronic data as evidence, to ensure consistent application by conducting agencies.

Second, the knowledge and skills of investigators, Prosecutors, judges, and lay assessors should be strengthened in determining offences in the field of information technology and telecommunications networks.

Given the distinctive features of these offences, offence determination in this domain exhibits several salient characteristics: (1) The objective acts can only be carried out through electronic means and devices, as well as software and software tools; (2) The evidence used for offence determination is predominantly collected and exploited from electronic data; and (3) to secure the most effective collection and use of evidence for offence determination, proceeding-conducting persons (investigators, Prosecutors, judges, and lay assessors) must possess specialised knowledge and a working understanding of information technology, computer networks, telecommunications networks, the Internet, and electronic data.

Accordingly, throughout the stages of institution, investigation, prosecution, and adjudication of these crimes - both generally and for the specific purpose of offence determination in particular - the relevant personnel should be equipped with an adequate level of IT-related literacy (computing, electronic devices, computer networks, telecommunications networks, etc.) and the practical skills required to collect, preserve, analyse, evaluate, and use electronic data in support of case resolution./.

LIST OF REFERENCES

1. Nguyen Hoa Binh (2009), High-tech crimes in Vietnam - Current situation and solutions for prevention and investigation by the People's Police force, Ministry-level scientific and technological project, Ministry of Public Security;

2. Le Cam, "Some General Issues Regarding the Determination of Criminal Charges," Vietnamese Criminal Law Textbook, Hanoi Law University, People's Police Publishing House, Hanoi;

3. Le Van Cong (2022), "Detecting, collecting and preserving electronic traces in scene examination and search", Prosecutorial Magazine, No. 23/2022;

4. Tran Dinh Hoa, Information Security and Crime Prevention Using High Technology (Monograph), People's Police Publishing House, Hanoi, 2011;

5. The 2001 Convention on Cybercrime of the Council of Europe (Budapest Convention);

6. Pham Van Loi, Crimes in the Field of Information Technology (Monograph), Justice Publishing House, Hanoi, 2007;

7. Nguyen Xuan Thu (2015), Preventing crimes using the Internet and digital telecommunications networks to appropriate property, Doctoral dissertation in Law, People's Police Academy;

8. Vietnam Procuratorate University, Vietnamese Criminal Law Textbook, People's Police Publishing House, Hanoi, 2018;

9. Vo Khanh Vinh, General Theory on Determining Criminal Charges, Social Sciences Publishing House, Hanoi, 2013.