BETWEEN SECURITY AND PRIVACY: LEGAL CHALLENGES IN ADMINISTRATIVE INSPECTIONS OF PERSONAL ELECTRONIC DEVICES UNDER VIETNAMESE LAW

Hao Van LE*

I. INTRODUCTION

The rapid development of digital technology has significantly impacted the collection, storage and sharing of personal information on electronic devices. In this context, many countries have regulations on procedures for item search, or search of electronic devices when the owner of a personal electronic device violates the law.

In Vietnam, the search of electronic devices according to administrative procedures raises several questions related to legality, mainly related to the protection of privacy and personal data. This study focuses on addressing significant gaps in the current regulations on these issues within Vietnam's legal

* Ph.D Procuratorate University, Vietnam. Email:haolv_t3@vks.gov.vn.

framework. The primary research goal is to analyze how Vietnamese legislation regulates the search of electronic devices through administrative procedures, with a focus on issues related to privacy and data protection. The urgency of this study is underscored by the limited legal research on this issue in Vietnam. Despite the increasing use of electronic devices and concerns about data privacy, Vietnam's legal regulations in this area are still vague and underdeveloped[1]. The lack of clarity in legal provisions has practical implications for the legitimate rights and interests of individuals subject to electronic device searches, posing potential risks to their privacy and data security.

Currently, Vietnamese law is not clear and specific about the parameters and limitations of electronic device searches, leading to inconsistencies and the possibility of abuse in implementation. These shortcomings not only undermine the legal principles

[1] Do Hai Ha & Le Thu Hien, *Privacy in Vietnam*, available at <https://www.mondaq.com/constitutional-administrative-law/106926/privacy-in-vietnam> (last visited August 01, 2024).

for protecting privacy and personal data but also reduce public confidence in the legal system's ability to protect individual rights. In the face of these challenges, it is essential to scrutinize existing legal norms, identify shortcomings, and propose comprehensive legislative reforms.

This Article aims to fill the existing research gap by providing a detailed analysis of Vietnamese legal regulations related to the searches of electronic devices according to administrative procedures, evaluating the effectiveness of these regulations in comparison with international standards in protecting privacy and personal data[2], and proposing comprehensive legislative reforms to effectively protect individual privacy in the digital era.

[2] P. Kimpian, *Rights to Privacy and to Personal Data Protection and Convention 108*, R. Atuguba Akongburo, P. Boshe, S. Dei-Tutu & M. Hennemann (Ed.), AFRICAN DATA PROTECTION LAWS: REGULATION, POLICY, AND PRACTICE (2024), 19-28.

II. THE TREND OF SEARCHING OF ELECTRONIC DEVICES FOR DIGITAL EVIDENCE

Technology has become even more entrenched in our personal lives[3], significantly transforming the way individuals communicate and behave[4]. People can communicate through the internet using various methods, such as texting, video calling, or online meetings, without the need for face-to-face interaction. As a result, people are increasingly reliant on electronic devices like smartphones, tablets, and laptops. Almost everyone uses them daily for communication, work, entertainment, and financial transactions.

In addition to their basic features, smartphones, tablets, or laptops integrate modern applications with various other functions to support daily life, education, health care, and work. These functions include reading

[3] Canadian Bar Association (2022), at 1.
[4] Nguyen Thi Mai Anh, *The Impact of the Fourth Industrial Revolution on the Culture and Lifestyle of Vietnamese People*, available at https://www.tapchicongsan.org.vn/nghien-cu/-/2018/820810/tac-dong-cua-cuoc-cach-mang-cong-nghiep-lan-thu-tu-den-van-hoa%2C-loi-song-nguoi-dan-viet-nam.aspx (last visited July 01, 2024).

the news, learning online, drafting documents, transferring bank payments, booking a car, buying and selling items, investing in stocks, diary-keeping (storing information, images, etc.). For instance, the Zalo application (which includes messaging, calling, diary, and group discussion,…) has up to 74 million users in Vietnam, accounting for more than 74% of the population[5].

Nowadays, more private information is in a single device than used to be stored in briefcases, homes, offices or anywhere else. The private information includes current and historical data on a person's geo-location, call history, text messages, email, photos, contacts, calendar, physical activity, health, finances, shopping history, internet searches and more, which can provide insight into a person's preferences, habits, interests and values[6]. Personal electronic devices may contain more and more private information for the following reasons:

[5] Pham Trung, *Zalo Continues To Be The Most Popular Messaging App In Vietnam*, available at https://nhandan.vn/zalo-tiep-tuc-la-ung-dung-nhan-tin-pho-bien-nhat-viet-nam-post741283.html (last visited July 01, 2024).
[6] Canadian Bar Association (2022), at 3.

- Personal electronic devices are widely used, with

- Personal electronic devices, especially smartphones, have many features including cameras, voice recording, GPS, and communication apps like email, social media, and messaging. These features allow for the storage and recording of a lot of personal information and users' daily activities, which in turn provides valuable data for investigations.

- The information storage capacity of electronic devices is constantly expanding and is completely different from physical storage vessels, enabling the storage of vast amounts of data, including images, videos, messages, emails, and various types of documents.

- Personal electronic devices are constantly connected to the internet and social networks, enabling authorities to monitor and gather information from the suspect's online activities, such as conversations, posts, and online transactions.

- Investigative tools of state agencies are becoming more and more modern, the development of digital forensic tools and techniques allows investigative

agencies to analyze and extract data from phones efficiently and quickly. These tools can recover deleted data, extract hidden information, and analyze online behaviors.

- Countries are increasingly cooperating internationally in the investigation of transnational violations and crimes, which has helped to share information and technology, thereby improving the ability to collect evidence from mobile phones.

The privacy concerns arising from them are completely different than those arising from physical storage vessels like luggage, which shaped the early principles of "briefcase law.

The intimate personal information on the device can date back to the purchase of the phone, or even earlier.

For many professionals – including doctors, lawyers, business executives, human rights activists and journalists – the devices may also contain highly sensitive information about others. Cloud services regularly synchronize significant data stores to one or

more devices and may be difficult or impossible to fully delete.

Therefore, protecting personal privacy is crucial. Mobile phone manufacturers also study how to protect the data in the phone, for example, Apple (USA), a leading electronic device manufacturer, has implemented measures such that if an iPhone or iPad is lost and the wrong password is entered too many times, all data in it will be disabled. At this time, the person who takes the phone can only take the "physical corpse", and the "soul" – the data and privacy inside the phone still belong to the owner. This is a controversial issue between Apple's privacy protection and the US Department of Justice, when in early 2020, US police seized two iPhones of the suspect but both were locked with a password, the US Department of Justice[7] asked Apple to unlock the iPhone to obtain information and data to help investigate the crime, but

[7] THE NEW YORK TIMES, *Magistrate Judge James Orenstein's Order*, available at https://www.nytimes.com/interactive/2016/02/29/technology/document-Orenstein-Order.html (last visited July 10, 2024).

Apple still stubbornly refused and thought that doing it was tantamount to betraying customers[8].

Individuals who violate the law often communicate using personal electronic devices. The information stored on these devices is vital for authorities to establish legal infractions. These types of evidence may include: (1) Text messages and emails: These evidences may contain information about plans, exchanges, or violations; (2) Calls and recordings: Call history and conversation recordings may be used to prove communications related to the violation; (3) photos and videos: photos and videos stored in the phone may contain evidence of criminal crimes or violations; (4) Browsing history: The visited websites can provide information about the intent or plan involved in the infringement; (5) Location data (GPS): Saved location information can help identify behavior or presence at a particular location in connection with the incident; (6) Apps and In-App fata: Messaging apps, social media, and other apps may contain

[8] Ha Van, *FBI mở khóa thành công iPhone và kết thúc vụ tranh chấp pháp lý với Apple*, available at https://nhandan.vn/post-258831.html (last visited July 10, 2024).

important information and data related to the violation; (7) Documents and files: Files and documents stored on a phone may include contracts, financial information, or other documents that may serve as evidence.

Evidence to handle violations increasingly uses electronic evidence, because when committing violations, according to the law of reflection, information and evidence of violations will leave traces in the physical world, including personal electronic devices. The nature of such information and data is evidence and can be used to prove violations. Currently, the electronic evidence required to be provided is shown through the contents, of which 54% are contact data, and 32% are emails[9].

In Vietnam, there is an increasing number of administrative violations occurring through social networks and the internet. These violations include actions such as insulting reputation, honor, and dignity,

[9] Europol, *SIRIUS EU Electronic Evidence Situation Report 2023*, available at https://www.europol.europa.eu/publications-events/publications/sirius-eu-electronic-evidence-situation-report-2023 (last visited July 10, 2024).

spreading false information on social networks, and engaging in online fraud. It is important to clearly define what constitutes a violation, determine whether multiple individuals are involved, and must gather evidence from electronic sources such as messages and emails on personal devices. While science and technology bring great benefits, they also lead to increased reliance on computers, smartphones, and internet systems, causing a growing amount of violation data to be stored in electronic devices. As a result, there is a need for a specific legal framework to safeguard the privacy of personal information when examining personal electronic devices.

III. MEASURES TO SEARCH OBJECTS BEING ELECTRONIC DEVICES ACCORDING TO ADMINISTRATIVE PROCEDURES UNDER VIETNAMESE LAW

Vietnamese law does not have separate regulations on the search of personal electronic devices according to administrative procedures. All objects are covered within the legal framework of the search of objects according to administrative procedures, as specified in

Article 128 of the Law on Handling of Administrative Violations 2012 (amended and supplemented in 2020). This Article, titled *"Search of means of transport and objects according to administrative procedures"* does not distinguish between the search of means of transport and the search of objects. Therefore, the search of objects and means of transport is governed by the same regulations regarding competence and order of procedures.

Regarding establishments applying the measure of searching objects that are electronic devices according to administrative procedures, this measure is applied when *"there is a ground to believe that administrative violation material evidences are hidden in such means of transport and objects"* by a person with statutory authority. This basis can come from various diverse sources such as denunciations of citizens or through monitoring of subjects and subjects being searched focusing on electronic devices such as computers, phones, and other electronic devices that are considered administrative violations. Currently, Vietnam's law on the search of objects being electronic

devices is still bad in certain deficiencies and inadequacies in legal regulations. Accordingly, the Law on Handling of Administrative Violations 2012 does not distinguish between objects in the procedures for examining equipment according to administrative procedures. Specifically, the Law does not clearly distinguish between objects such as bags, suitcases, and objects containing the private life of individuals, electronic data such as phones, computers, and other electronic devices.

Objects are personal electronic devices that have more special properties and aspects when compared to ordinary objects for administrative procedures. Electronic means hardware, software, information systems, or other means operating based on information technology, electronic, digital, magnetic, wireless transmission, optical, electromagnetic or other similar technologies[10], and digital devices means electronic devices, computers, telecommunications, radio transmission, transceivers, and other integrated equipment used for producing, transmitting, collecting,

[10] The Law on E-Transactions 2023, Art. 3(2) (2023).

processing, storing and exchanging digital information[11]. Thus, according to relevant regulations, electronic devices that can become the object of electronic device examination are extremely broad.

However, electronic devices that are the object of the electronic device examination measure also process and store other data, such as the personal data of the owner, personal data of others, inviolable private secrets, and various other data unrelated to the violations. The examination of electronic devices under administrative violations includes accessing and reviewing data that is not related to the violations on the devices, which may potentially intrude on the privacy of individuals and disrupt their normal activities. However, Vietnam's administrative law currently lacks provisions to address these concerns and ensure the stability of individuals' normal lives during electronic device examinations according to administrative procedures.

The search of electronic means according to administrative procedures shall only be conducted

[11] The Law on Information Technology 2006, Art. 4(11) (2006).

when there are grounds to believe that there is material evidence of administrative violations. However, there is no document specifying which cases are considered *"grounded"* and which cases are *"unfounded"*, leaving the decision to the discretion of the competent person. This ambiguity in Vietnamese legal regulations may lead to potential misuse of power and unwarranted infringement upon individuals' privacy during electronic device examinations in administrative procedures.

Regarding the subject competent to perform the measure of electronic device examination according to the current administrative procedures, the law stipulates that only subjects such as the Head of the Ward Police, the Head of the District Police, the Head of the Police Division for Administrative Management of Social Order, the Head of the Road Traffic Police Division, etc.[12] shall have the authority to search electronic devices of citizens when there are grounds

[12] The Law on Handling of Administrative Violations 2012, Art. 123(1) (2012).

to believe that such objects are exhibits or are directly related to administrative violations.

It can be seen that the Law on Handling of Administrative Violations 2012 has listed a series of subjects who have the authority to search electronic devices. However, this Law has not clarified the specific fields and cases that each subject has certain authority. This, inadvertently, creates a statement that any of the subjects listed under the provisions of Clause 1, Article 123 of this Law can also search a citizen's electronic device without zoning for this search.

When conducting a search of electronic devices, a competent person needs to make a record, witnessed by the owner of the object and 01 witness; in case the owner of the object is absent, there must be (at least) 01 witness. The search of objects must be decided in writing unless there are grounds to believe that if the search is not carried out immediately, the material evidence of administrative violations will be dispersed and destroyed. All cases of search of means of transport or objects (including search of electronic

devices) must be recorded. The search decision and the record must be handed over to the owner of the means of transport or objects or the operator of the means of transport to keep 01 copy.

At first glance, the regulations related to the procedural order are relatively strict and ensure fairness because there is the witness of the owner of the electronic device or another witness. However, this regulation is only suitable for ordinary objects but does not ensure the suitability of electronic devices because electronic devices may have passwords and encryption to ensure the privacy of individuals electronically. Moreover, the law only stipulates that the owner of the witness device is not obliged to unlock or provide a password or encryption to open the device for a competent person to check. Hence, it is necessary for the appropriate authority to conduct a self-test on this electronic device. This prolongs the inspection time, leading to the owner of the electronic device also having to carry out supervision and hinders the normal operation of the person being examined for electronic equipment.

Currently, there is not much public data on the status of electronic device searches in Vietnam. However, based on reports and information from privacy and human rights organizations, searches of personal electronic devices are not uncommon. Many cases of electronic device searches are carried out without a clear legal basis, leading to concerns about the privacy and protection of people's personal data.

In general, based on the analysis and evaluation of current regulations, it is evident that Vietnamese law still has shortcomings and vague information concerning the search of electronic devices according to administrative procedures. Specific regulations for the search of electronic devices are lacking, which results in inadequate protection of users' privacy. The grounds for searching are qualitative, leading to the competent person being able to arbitrarily decide without clear criteria. Jurisdictional regulations are quite broad, allowing multiple competent subjects to search, which can lead to abuse of power and invasion of personal privacy. The specific order and procedures for conducting searches, especially in the case of

searching electronic devices containing sensitive personal data, have not been clearly outlined. In order to protect privacy and personal data in the context of increasingly evolving technology, comprehensive legal reforms are necessary. These reforms should aim to ensure privacy and protect personal data while minimizing the risk of abuse of power and infringement of people's legitimate rights.

IV. DISCUSSION ON THE CORRELATION BETWEEN REGULATIONS ON THE SEARCH OF PERSONAL ELECTRONIC OBJECTS ACCORDING TO ADMINISTRATIVE PROCEDURES AND CRIMINAL PROCEDURES

Unlike the search of electronic devices according to administrative procedures, when dealing with criminal cases, the search of electronic devices is a crucial investigative measure for gathering evidence. However, this measure directly impacts the constitutionally protected rights of citizens, such as the right to telephone conversations, telegrams and other forms of private communication. Therefore, without

legal grounds, no agency, organization, or individual is permitted to conduct this investigative measure.

For searches according to criminal procedures, the search of persons, residences, workplaces, places, and means shall be conducted only when there are grounds to identify in the persons, residences, workplaces, places and means of crime tools, means of crime objects, and assets obtained from the crime or objects, electronic data, and other documents related to the case. The search of residences, workplaces, places, and vehicles is also carried out when it is necessary to detect people who are wanted, trace, and rescue victims. Therefore, when there are grounds to judge that in letters, telegrams, parcels, postal items, and electronic data there are tools and means of crime, documents, objects, and assets related to the case, letters, telegrams, parcels, postal items, and electronic data can be searched. In case it is necessary to seize electronic means for exploitation of electronic data in the course of investigation, it must be carried out by a person competent to conduct the proceedings and may invite a person with relevant expertise to participate. In

case it cannot be seized, it must be backed up in the means of storage and confiscated as material evidence.

In Clause 1, Article 99 of the 2015 Criminal Procedure Code, the concept of electronic data is defined as symbols, writings, digits, images, sounds, or similar forms created, stored, transmitted, or received by electronic means. Article 107 of the 2015 Criminal Procedure Code stipulates: *"Electronic vehicles must be seized in a timely and complete manner, properly describe the actual situation and seal immediately after seizure. The sealing and opening of the seal shall be carried out in accordance with the provisions of law".* From there, it can be seen that electronic means, if they want to be seized and searched, must be collected by the law, in the whole process of searching, seizing physical evidence, using technology (hardware and software) recognized by legal agencies, from which new electronic means can be used to exploit the electronic data that exists inside and carry out copying

data storage, preservation, recovery, analysis, search and examination of data as evidence[13].

The search of electronic devices according to criminal procedures aims to collect electronic data in such devices[14]. In the process of collecting, searching, and collecting electronic data from electronic means, it must be recorded in the record and sealed in accordance with the provisions of the criminal procedure law, then such electronic data can be considered as a lawful source of evidence in the process of settling criminal cases. Clause 2, Article 87 of the 2015 Criminal Procedure Code stipulates that what is real but not collected according to the order and procedures prescribed by the Criminal Procedure Code is not legally valid and cannot be used as a basis for settling criminal cases. So, when investigating, exploiting, and collecting evidence, the investigating agency must comply with the regulations on sealing immediately after collection, the sealing and opening

[13] Hoang Trong Luc, *Collecting Electronic Traces From Mobile Phones In Criminal Investigation*, 01 JOURNAL OF PROCURATORATE STUDIES 6 (2022).
[14] Nguyen Duc Hanh, *Electronic Data And Electronic Evidence*, 01 PROSECUTORIAL MAGAZINE 37 (2019).

of the seal must be included in the case file, otherwise, such evidence will not be valid to prove the crime. At the same time, in the process of exploiting electronic data from electronic means, the investigating agency must not be affected to change the data since the seizure of the electronic means and take measures so that the electronic data cannot be tampered with.

In general, unlike criminal procedures, where specific regulations exist in the Criminal Procedure Code, administrative procedures do not provide a clear order and process for exploiting electronic data. The process of searching electronic devices according to administrative procedures lacks clear guidelines for sealing when seizing and exploiting electronic data in such electronic devices. This raises concerns about the arbitrary access to personal data and the potential infringement of individuals' privacy during electronic device searches conducted in the context of administrative violations. In criminal proceedings, investigating agencies have the responsibility to collect electronic data and exploit all available information on the device, including deleted information, to facilitate

the evidence-gathering process. This process is carried out by trained technical officers of the Ministry of Public Security to ensure data integrity and safety. For each type of electronic device, there will be a different method of data mining, depending on the type of electronic device, the technical officers will decide which method to exploit[15]. However, in administrative procedures, a wide range of personnel without expertise in electronic data exploitation, such as the Chairman of the commune-level People's Committee, the Head of the Forest Ranger District, the Captain of the Mobile Forest Ranger Team and Forest Fire Prevention and Fighting, etc. are authorized to conduct searches of electronic devices[16]. This may lead to the infringement of personal data privacy rights as it could potentially impact unrelated data on electronic devices, thereby undermining the data subject's right to consent to the processing of their personal data.

---

15 Hoang Trong Luc, *Collecting Electronic Traces From Mobile Phones In Criminal Investigation*, 01 JOURNAL OF PROCURATORATE STUDIES, 6 (2022).

16 The Law on Handling of Administrative Violations 2012, Art. 128(2) (2012).

V. DISCUSSION ON THE CORRELATION BETWEEN REGULATIONS ON THE SEARCH OF OBJECTS BEING PERSONAL ELECTRONIC DEVICES ACCORDING TO ADMINISTRATIVE PROCEDURES AND PRIVACY

The right to privacy is identified by United Nations, human rights agencies, and scholars around the world as a basic and essential right to autonomy and self-respect of individuals, protection of human dignity, etc. is a basic human right[17]. The issue of privacy is stipulated in Article 21 of the 2013 Vietnam's Constitution as follows:

> Everyone has the inviolable right to private life, personal secrets, and family secrets; have the right to protect their honor and reputation. Information about private life, personal secrets, and family secrets is guaranteed to be safe by law. Everyone has the right to keep confidential correspondence, telephone, telegraph, and other forms of private communication. No one is allowed to illegally open, control, and seize letters, telephones, telegrams, and

[17] Chu Hong Thanh, *The Law on Privacy Protection*, available at https://lsvn.vn/phap-luat-ve-bao-ve-quyen-rieng-tu.html (last visited June 26, 2024).

other forms of private information exchange.

The Law on Cyber Information Security 2015 also clearly stipulates the responsibilities of agencies, organizations, and individuals in collecting and using personal information. Accordingly, organizations and individuals that process personal information have the following responsibilities: collect personal information after obtaining the consent of the personal information subject on the scope and purpose of collecting and using such information; only use the collected personal information for purposes other than the original purpose after obtaining the consent of the personal information subject; not to provide, share or disseminate personal information that they have collected, accessed or controlled to third parties unless there is the consent of such personal information subject or at the request of competent state agencies. At the same time, state agencies are responsible for the confidentiality and storage of personal information collected by themselves and the personal information subjects themselves have the right to request

organizations and individuals processing personal information to provide their personal information that such organizations and individuals have collected, archives[18].

In addition, Decree 13/2023/ND-CP on personal data protection has just been promulgated, which also has strict regulations on personal data protection. This Decree stipulates 08 basic principles on personal data protection, which are the basic principles for personal data protection[19]. Decree 13/2023/ND-CP also has separated regulations on personal data processing activities to protect the rights of data subjects. However, Decree 13/2023/ND-CP is an exception for the processing of personal data of data subjects, in which the processing of data by competent state agencies for crime prevention and combat and in case of violation of the law in accordance with the provisions of the Basic Law to process personal data without consent[20].

[18] The Law on Cyber Information Security 2015, Art. 17 (2015).
[19] Decree 13/2023/ND-CP on Personal data protection, Art. 3 (2023).
[20] Decree 13/2023/ND-CP on Personal data protection, Art. 17 (2023).

It can be seen that by regulating the search of objects that are electronic devices in the Law on Handling of Administrative Violations, the state has limited the privacy of individuals in some specific cases where this measure is applied. The state's limitation of the right to privacy of individuals has a legal basis from Clause 2, Article 14 of the Vietnam's Constitution 2013, according to which *"human rights and civil rights can only be restricted in accordance with the provisions of the law in case of necessity for national defense reasons, national security, social order, safety, social ethics, and community health"*. The widely accepted view is that most human rights are relative rights and may be limited. There are only a few absolute rights, that is, they are not infringed under any circumstances[21]. The right to respect human dignity, which includes the right not to be enslaved, and the right not to be tortured and ill-treated, is recognized by the majority as absolute and cannot be

[21] Vo Hong Phuong & Vo Minh Ky, *Individual Privacy and Special Procedure Investigation Measures*, 05 JOURNAL OF PROCURATORIAL SCIENCE (2018).

restricted. Thus, the restriction of rights is a normal and common phenomenon in every country[22].

According to the 2012 Law on Handling of Administrative Violations, when dealing with administrative violations, the authorized entity has the right to collect and process personal data (in electronic form) from the violator's electronic device without the consent of the data subject. The Law on Handling of Administrative Violations 2012 does not limit the scope and content of data collected in electronic devices. Competent agencies can completely intervene and collect a lot of data unrelated to administrative violations of individuals, thus leading to the invasion of the privacy of the violator. When examining electronic devices, state agencies may access and process almost all the data of electronic device owners to identify administrative violations. However, this often leads to state agencies processing unnecessary and non-infringing data of electronic device owners, violating the right to personal privacy outlined in the

[22] Bui Tien Dat, *Constitutionalization of the Principle of Limitation of Human Rights: Necessary but Not Enough*, 6 JOURNAL OF LEGISLATIVE STUDIES 3 (2015).

Constitution and other legal documents in Vietnam. In addition, there is no mechanism to monitor whether the person performing the data check controls the data of the individual who is being searched for electronic devices (e.g., through video recording or having witnesses). This leads to the risk of unauthorized backup and dissemination of electronic device owner data for various purposes, resulting in privacy violations and could directly or indirectly affect the agency, other relevant organizations, and individuals.

The collection of evidence from electronic devices such as phones and personal computers to ensure that it does not infringe on human rights, privacy, and personal secrets is a controversial issue, especially if the violator is forced to provide a password to obtain data. Because the electronic device stores information such as images, documents, personal data, and unrelated content, it may include intellectual property or business secrets. Collecting evidence with caution, respect for privacy, and without infringement is challenging as extracting information related to a violation may lead to the disclosure of other personal

information, such as images, documents, and diaries. Currently, there are no specific regulations to protect personal data (such as the requirement to be confidential; the request to be copied to protect the data from being lost or illegally exploited), because the right to confidentiality of letters, telephones, telegrams and other forms of private information exchange is stipulated in the Constitution[23]. The issue of collecting and processing evidence through personal electronic devices is sensitive because it can infringe on human personal and private rights. Notably, even in criminal proceedings, the application of measures "to different extents restricts a number of human rights, certain citizenship"[24]. In Vietnamese laws that address privacy, there is a tendency to prioritize the protection of public order over personal privacy.

In the Anglo-American legal system, privacy is rooted in the values of liberty, especially individual freedom against state power. Privacy protection

[23] Vietnam's Constitution 2013, Art. 21 (2013).
[24] Tran Dinh Nha, "Special Procedure Investigation Measures", Nguyen Hoa Binh (Ed.), NEW CONTENTS IN THE CRIMINAL PROCEDURE CODE 2015 (2016), at 291.

institutions in U.S. law often emphasize the intrusion of state power into an individual's private space because of the fear that an authoritarian, authoritarian state power will stifle an individual's life[25]. Therefore, in most countries around the world, the right to privacy has two main functions: to resist state intrusion into private life. However, this leads to a conflict between protecting privacy and ensuring that law enforcement agencies can obtain information that is critical to protecting national security and public safety. The relationship between protecting privacy and providing information to law enforcement is an ongoing challenge, especially in the context of rapidly evolving technology. Good regulation and proper protection measures can help minimize the risk of infringing on people's rights.

Privacy protection is an important element of protecting individual freedoms although the concept of privacy is becoming increasingly difficult to delineate in the digital age because, in certain situations, privacy

[25] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE LAW JOURNAL 1161 (2004).

may conflict with the right to access information[26] between personal interests and the interests of the community.

Collecting personal information without due process and proper consent may violate individuals' rights. Failing to disclose this violation contributes to a lack of transparency, and demanding passwords can also breach this principle. Nevertheless, law enforcement agencies may need access to information in order to ensure national security and public order, especially in cases of illegal acts such as riots and terrorist acts. Accessing information on a phone can help uncover crucial details, aiding law enforcement in preventing threats and handling emergencies to safeguard public safety. Therefore, requesting a phone password can be a justified action.

[26] Thai Thi Tuyet Dung, ACCESS TO INFORMATION AND PRIVACY IN VIETNAM AND A NATION (2012), at 185.

VI. PRACTICES ON THE APPLICATION OF THE MEASURE OF SEARCHING OBJECTS BEING PERSONAL ELECTRONIC DEVICES ACCORDING TO ADMINISTRATIVE PROCEDURES IN VIETNAM AND SOME COMMENTS

In Vietnam, there are typical practical situations regarding the issue of searching objects that are electronic devices according to administrative procedures and this can be considered an infringement of privacy.

Case 01:

The Ministry of Health issued Decision No. 2666/QD-BYT dated 29/05/2021. In the content of this decision, it is proposed to sanction administrative violations of people who have smartphones but do not install the Bluezone app and turn on Bluetooth[27]. This is considered a measure related to prevention and control[28]. Regarding this issue, when going out in any

[27] Minh Chung, *Phạt người có smartphone không cài Bluezone: Chưa ổn!*, available at https://plo.vn/share629313.html (last visited July 23, 2024).
[28] Ngo Nguyen Thao Vy, *From Crisis to Control: ...Data Protection Concerns in Singapore and Vietnam through the Lens of Techno-*

case, it can be understood that the competent authority can ask citizens to prove that they have installed the Bluezone application on their phones and have Bluetooth enabled. However, in this case, if citizens do not clearly provide their phones, they will be considered a violation of regulations on prevention and control. In this case, no one wants the competent authority to open or be forced to open their phone to check whether the phone is installed with Bluezone, especially in today's phones contain many other private information and the provision of the phone for such a check will lead to the infringement of other confidential information of the citizen who owns it whether or not it is on the phone is a matter directly related to privacy and the right to protect personal data.

Case 02:

A citizen in Hanoi was recorded for violations related to security and order, the press reported that this person confirmed that, when invited by the police to the ward, this group of people had their mobile phones

Solutionism and Efficient Violation of Privacy Rights, 2 LAW AND DEVELOPMENT REVIEW (2024).

confiscated and were required to provide passwords to search objects[29]. Then there was a situation of revealing a sensitive video stored in the phone of an individual in the group on the Internet and this video was not related to the security and order issue that the police were investigating.

In the above two situations, issues such as sanctioning authority, procedures for searching objects that are personal phones and the requirement to provide phone passwords to ensure the process of searching phones to have grounds for sanctioning, have been facing many obstacles, especially the non-cooperation on the part of the searched person, as well as concerns about personal data being leaked during this procedure. However, with the current law, the procedure for searching a phone is no different from other ordinary objects such as bags and luggage. The law also does not take into account other legal issues such as the infringement of data and information

[29] Danh Trong, *Công an điều tra, truy nguồn phát tán vụ nữ diễn viên bị lộ 'clip nóng'*, available at https://tuoitre.vn/cong-an-dieu-tra-truy-nguon-phat-tan-vu-nu-dien-vien-bi-lo-clip-nong-20210528191203966.htm (last visited July 23, 2024).

contained in the phone and in fact, in case No. 02 has led to the problem of infringement on the privacy of the person being searched as well as other relevant persons whose data in the phone is searched by administrative procedures.

The situation that the Ministry of Health requires sanctions for not installing software on smartphones, this will lead to competent people having to analyze the procedures for sanctioning this behavior to ensure that it is implemented correctly and appropriately. Because, according to the provisions of the Law on Handling of Administrative Violations 2012, to determine the violation, there must be evidence, so to know whether the software is installed, it is necessary to check the phone according to administrative procedures, in practice it is not easy to do because the majority of phone owners refuse to open their phones for fear of revealing personal information. Therefore, if the phone cannot be opened, there will be no basis for sanctioning, which leads to the provision of sanctioning the above act is not feasible.

For the competent authority to temporarily seize the phone and request the password to search the object. According to the law, the search of objects must have a record, the presence of the owner and a witness. As for whether to provide a password or not, this depends on the point of view of each individual whether to provide it or not, but in terms of law, no regulation requires phone owners to provide passwords when searching phones according to administrative procedures. In principle, the competent authority has the right to oblige citizens to provide passwords for electronic devices. This issue existed in the 4th and 5th Amendments of the U.S. Constitution whereby citizens have the right to resist coercion of self-incrimination, so citizens have the right to refuse to provide passwords. Accordingly, if the competent authority wants to perform a search of mobile devices, they need to have a phone search warrant and they must extract it by themselves with their expertise and expertise.

Currently, there is no difference in the search of mobile phones compared to other normal objects such as bags, documents, etc. The same search procedure

has been facing obstacles in the current context, especially the function of the phone is not only a means of communication but also a secret of the private life and private life of each individual.

Meanwhile, on the same issue related to the search of places where material evidences are hidden, the law stipulates a very different difference between the search of places where material evidences are hidden and houses are also houses, and the search of places where material evidences are hidden are shops and warehouses. If it is a house, the house search must be carefully considered by the Chairman of the district-level People's Committee before deciding to search, due to the important nature of the house, it is the private space of all family members, which needs to be respected and protected, which is considered one of the basic rights, the inviolability of the individual, the search must follow very strict procedures to minimize the infringement of human rights to residence and private life. If it is a warehouse or shop, the authority to decide is made by many subjects, possibly the Head of the ward police, the Chairman of the commune-level

People's Committee, etc. Thus, it is necessary to search phones only in criminal cases, while administrative violations should only be searched in special cases to protect privacy and avoid wasting more social resources when settling disputes related to the protection of this right.

VII. SOME PROPOSALS FOR IMPROVING VIETNAMESE LAW ON THE SEARCH OF OBJECTS BEING ELECTRONIC DEVICES ACCORDING TO ADMINISTRATIVE PROCEDURES

Firstly, the measure of searching objects according to administrative procedures according to the provisions of Article 128 of the Law on Handling of Administrative Violations 2012 is time to add a separate legal framework for the search of personal phones, should not share the same authority and procedures as other ordinary objects to protect privacy. Specifically, Clause 6 is added to Article 128 in the case of searching objects being electrical or personal mobile devices, the district-level People's Committee presidents shall be the competent persons to consider

and decide. The owner of the personal mobile device has the right to provide or refuse to provide the password of the mobile device.

Secondly, it is necessary to supplement regulations on the search of letters, telegrams, parcels, and postal items to detect acts of administrative violations:

> When there are grounds to judge that there are tools and means of administrative violations in letters, telegrams, parcels, postal items, electronic data, objects, and assets related to acts of administrative violation may be searched for letters, telegrams, parcels, postal items, and electronic data.

Thirdly, it is necessary to supplement regulations on the right of electronic data owners to be requested to protect personal electronic data unrelated to administrative violations stored in confiscated electronic means; the right to copy personal data that is not related to the violation.

Fourth, it is necessary to take measures to cooperate with online service providers, especially for service providers with servers abroad. In addition to community standards, online service providers also

have provisions for cooperation with the judiciary of other countries with certain conditions.

Fifth, Vietnam needs to develop and promulgate a specific and detailed legal framework for the search of electronic devices according to administrative procedures to ensure the privacy and protection of citizens' personal data. This comprehensive legal framework will help protect privacy and personal data because electronic devices store a lot of important personal information such as emails, messages, photos, videos, and other private documents. Conducting searches without specific regulations can lead to abuse of power and infringement of personal privacy. Furthermore, this is in line with technological advancements, the rapid development of technology requiring the law to keep up with the protection of individual rights. The current legal framework is insufficient to address complex issues related to technology and digital information. A comprehensive legal framework will ensure transparency and accountability of parties involved in electronic device examinations by clearly outlining the responsibilities

of law enforcement agencies and the interests of the people. Thereby, the detailed legal framework could help prevent abuses of power by the authorities, and at the same time protect the legitimate rights and interests of the people during law enforcement processes.

VIII. CONCLUSION

This Article examines the current legal regulations in Vietnam regarding the search of electronic devices according to administrative procedures and evaluates the effectiveness of these regulations in protecting privacy and personal data. The Article highlights challenges and shortcomings in the current legal framework, especially the lack of specific regulations on the search of electronic devices, which poses a risk of violating personal privacy. This not only causes privacy issues but also creates difficulties in enforcing the law in a transparent and accountable manner. The rapid development of information technology and the widespread use of electronic devices have placed an urgent requirement on a comprehensive and clear legal framework for the protection of personal information.

From there, this Article proposes that Vietnam needs to make adjustments in legal policies concerning the examination of electronic device according to administrative procedures as well as develops a common legal framework for this purpose.