Chapter 8
Legal Framework for Personal Data Protection in Vietnam

Hoa Chu

Abstract Building a smart city demands the digital transformation of government working processes and procedures, including the digitization and online execution of most administrative procedures. In practice, smart city governance uses information technology to increase the efficacy and efficiency of providing services to the public. The development of smart cities raises concerns among city residents about transparency in data collection and use of personal data. When governments implement smart city projects, sensors and closed-circuit television (CCTV) are placed in most streets, commercial centers, and public areas to observe the behavior of anyone within reach. The public is concerned about what the data collected from these CCTV systems will be used for and how to ensure that such data is not misused, disclosed, leaked, and exploited for the wrong purposes. The issue of protecting personal data and respecting privacy becomes more and more important when personal data is a special type of information. Therefore, Vietnam is urged to take bold actions to effectively strengthen data protection law. This chapter reviews the Vietnamese legal framework for data protection to highlight that the legal framework for data protection in Vietnam should be reformed for the development of smart cities.

8.1 Introduction

The Vietnamese government in recent years has viewed the smart city as an important element of the fourth industrial revolution, utilizing Information and Communications Technology (ICT) and other means to improve the competitiveness, innovation, creativity, transparency, and effectiveness of urban governance as well as to improve efficiency in land use, energy, and resources for the development, improvement, and advancement of the quality of the urban living environment. These many improvements will stimulate socio-economic growth and development. On August 1, 2018, the prime minister issued Decision No. 950/QD-TTg, approving the scheme for the

H. Chu (✉)
Deputy Director General, Institute of Legal Studies, Ministry of Justice, 60 Tran Phu Street, Ba Dinh District, Hanoi, Vietnam
e-mail: chuvihoa@gmail.com

T. Phan and D. Damian (eds.), *Smart Cities in Asia*, SpringerBriefs in Geography,
https://doi.org/10.1007/978-981-19-1701-1_8

development of smart sustainable cities in Vietnam in the period of 2018 and 2025 with orientations by 2030. This scheme has indicated the goals and roadmap of three phases of smart city development in Vietnam (the period up to 2020; period to 2025; and orientation to 2030). In addition, the project has also shaped seven points of view and principles for smart city development, including the principle "ensure cyber security and data protection."[1]

To turn a traditional city into a smart one requires huge efforts and various tasks. To meet this demand, Vietnam has taken some steps to improve its legal system. However, the legal framework for smart city projects in Vietnam is still at an early stage of development. For example, Decision 950/QD-TTg does not introduce the concept of the smart city, and up to now, Vietnamese law contains no regulation defining the smart city. For that reason, the first of the 10 solutions mentioned in Decision 950/QD-TTg is to review and update the legal system in order to build a legal framework for smart city development in Vietnam. There is room for improvement in the legal framework for smart cities in Vietnam in the following areas: ICT application, urban governance of infrastructure, construction and engineering, and protection of personal data.

In practice, several city or provincial governments in Vietnam have expressed their wishes to transform their provinces or cities into smart cities. To date, 46 out of 63 localities in Vietnam have been planning and implementing smart city projects.[2] These provincial governments have applied information technology in smart city development, including smart city planning, building and managing smart cities, and providing smart city utilities. For example, many localities have completed construction and put into use a Smart City Operation Monitoring Center. The goal of building this center is to supervise and operate smart city services and provide smart city utilities. The Smart City Monitoring Center deploys smart urban services, including five basic smart urban services (citizens' online reporting system, traffic control monitoring, public security monitoring, information monitoring in the network environment, and information security surveillance) and 10 additional smart urban services (environment monitoring and alert system, public service surveillance, smart travel, smart health, smart education, food safety and hygiene, monitoring the spread of COVID-19, open data service, disaster prevention monitoring, and waste truck monitoring system). These smart urban services are aimed at city residents, who benefit from them. However, the same residents who benefit from these services are also raising concerns about their privacy. The Smart City Operation Monitoring Center helps the government supervise and control citizens' social activities and predict

[1] See the 4th viewpoint and principle in Section I Article 1 of Decision No. 950/QD-TTg (Prime Minister 2018).

[2] Following are some of the localities that have been implementing smart city projects: Ha Noi, Gia Lai, Thai Binh, Da Nang city, Thanh Hoa, Bac Ninh, Binh Duong, Quang Ninh, Thua Thien Hue, Ho Chi Minh city, Lam Dong, Kien Giang, Lao Cai, Quang Tri, Tien Giang, Vinh Phuc, Yen Bai, Binh Thuan, An Giang, Son La, Hai Duong, Ninh Binh, Ba Ria – Vung Tau, Long An, Nghe An, Bac Giang, Ninh Thuan, Thai Nguyen, Vinh Long, Binh Phuoc, Đong Nai, Đak Nong, Đak Lak, Soc Trang, Cao Bang, Hau Giang, Ha Giang, Ben Tre, Binh Đinh, and Ha Tinh (Ministry of Information and Communications 2021).

social trends. Camera sensors were installed in most streets, commercial centers, and public areas around the province to observe the behavior of anyone within reach for supervising purposes. Urban monitoring through camera sensors is raising concerns among city residents about transparency in data collection and use of personal data.

For example, Da Nang has a traffic monitoring system with 200 cameras embedded with artificial intelligence to automatically detect traffic violations (e.g., driving in the wrong lane, red light violation, speeding, parking vehicles on the sidewalk, parking vehicles in contravention of regulations), to trace vehicles' routes, to count traffic flow, and to automatically control traffic lights. A public security monitoring system with 1,800 cameras and about 34,500 cameras installed on private property has been put into use (Ministry of Information and Communications 2021). Hue city uses 500 cameras with sensors applying face recognition and crowd recognition to supervise the city, ensuring urban security and regulating traffic (Nguyen 2020).

The public is concerned about what the data collected from these cameras will be used for and how to ensure that such data is not misused, disclosed, leaked, and exploited for improper purposes. These public concerns may be based on the following observations. First, agencies, organizations, and enterprises do not have consistent and effective information protection measures. Second, personal data storage and processing systems have vulnerabilities that can be exploited by hackers for their attacks, causing significant losses. Third, personal data theft and illegal trading happens quite frequently. Fourth, personal data is exchanged and utilized in multiple sectors resulting in difficulties in management. Fifth, many organizations collect and use personal data without notification or user protection mechanisms.

If privacy-related concerns are not properly addressed, the smart city implementation risks being opposed and may fail to gather support from city residents. The government of Vietnam is aware that building smart cities requires paying special attention to solving legal problems that might arise from striking a delicate balance between the need to collect and process information and data of citizens and the need to ensure privacy and confidentiality.

At the time of writing, the law on personal data protection still has many loopholes. So far, the legal framework on personal data protection and privacy protection in Vietnam has not been comprehensively developed as it has in some countries around the world. For example, the European Union in 2016 issued a separate Data Protection Regulation—GDPR, effective from May 25, 2018. Thus far, Vietnam has not issued a general law on personal data protection. Relevant regulations regarding personal data protection in Vietnam are scattered in many different legal documents. Therefore, this chapter argues that the legal framework for data protection in Vietnam should be reformed for the development of smart cities.

8.2 Current Status of Vietnamese Laws on Personal Data Protection

A review of nearly 70 Vietnamese legal documents[3] relating to the protection of personal data shows that Vietnamese laws on the protection of personal data are rooted in the right to privacy–a fundamental human right. There is a general principle enshrined in all provisions for personal data protection contained in Vietnam's legal documents: personal data is protected, and other subjects can use personal data as long as the data subject permits them to unless otherwise provided for by law; violators are subject to administrative and criminal penalties, and data subjects suffering from personal data intrusion are entitled to damages.

Constitution 2013 first sets out the general principles that everyone is entitled to the inviolability of personal privacy, personal secrecy, and familial secrecy and has the right to protect his or her honor and prestige. Information regarding personal privacy, personal secrecy, and familial secrecy is safely protected by the law (Article 21 2013). Next, there are four codes, 37 laws, and many sub-law documents addressing and related to personal information.[4] For example, Article 72(1) of the 2006 Law on Information Technology provides that organizations' and individuals' lawful personal information that is exchanged, transmitted, or stored in the network environment shall be kept confidential under law. Article 16 of the 2015 Law on Cyber Information Security provides for the principles of protecting personal information on the internet. Article 19 of the mentioned Law stipulates that personal information-processing organizations and individuals shall take appropriate management and technical measures to protect personal information they have collected and stored and comply with standards and technical regulations on the assurance of cyber information security.

However, the implementation of smart cities creates legal issues for personal data protection, which regulation has so far failed to deal with effectively. First, a question arises in smart cities: does the provision that personal data can only be collected and used with the data subject's consent (or prior consent) still matter in the Internet of Things (IoT) System, particularly when the data is collected in public places (i.e., smart transport systems or smart roads)? If the data subject's consent is not obtained in advance, does the law need to provide general provisions on the collection and use of personal data for public management purposes? What are the responsibilities of individuals and organizations using and protecting personal data in these cases? Currently, Vietnamese law does not have any answers to these questions.

Second, big data, the IoT, the cloud, and the other technological infrastructures in smart cities may endanger the privacy of smart city residents and users, posing a risk to personal data and information. Vietnam is yet to have a law on personal

[3] See Appendix.

[4] The Civil Code 2015, The Penal Code 2015 (amended and supplemented in 2017), The Civil Procedure Code 2015, The Criminal Procedure Code 2015, Law on Access to Information 2016, Law on Information Technology 2006, Law on Information Security 2015, Law on Cyber Security 2018, Law on Handling of Administrative Violations 2012, etc.

data protection or a common understanding of "personal data" and "personal data protection." Vietnamese laws currently use about 10 terms, for example "personal information," "private information," "digital information," and "personal information on the internet," with different explanations other than "personal data" (Chu 2021).

For example, "personal information" is used in five legal documents: 2015 Law on Cyber Information Security; Decree No. 85/2016/ND-CP on the Security of information systems by classification; Decree No. 72/2013/ND-CP on the Management, Provision, and use of internet services and online information; Decree No. 52/2013/ND-CP on E-Commerce; and Decree No. 64/2007/ND-CP on information technology application in state agencies' operations. These documents have contradictory explanations of "personal information"; for example, Article 3(13) of Decree No. 52/2013/ND-CP asserts that "personal information referred to in this Decree does not include work contact information and other information that the individual himself/herself has published in the mass media," while Decree No. 72/2013/ND-CP provides that "personal information means information associated with the identification of individuals, including names, ages, addresses, people's identity card numbers, phone numbers, email addresses and other information defined by law," irrespective of whether it has been publicized or not.

Third, current penalties for violations are not deterrent enough. Administrative law and criminal law set out penalties for the intrusion of personal data in the form of human rights or civil rights violations. In Vietnam, non-criminal violations relating to state management are subject to administrative penalties. Administrative penalties concerning personal data protection are scattered throughout many legal documents.[5] The fine could range from VND 2,000,000 to VND 70,000,000 for several personal information intrusion acts, such as retaining users' information for a period exceeding the retention period prescribed by law or agreed upon by two parties; collecting, processing, and using the information of other entities or individuals without obtaining their consent or for illegal purposes; and illegally trading or exchanging private information of users of telecommunications services.

Criminal Code 2015 provides for the "Infringement upon secret information, mail, telephone, telegraph privacy, or other means of private information exchange" in Article 159 and "Illegal provision or use of information on computer networks or telecommunications networks" in Article 288. The maximum penalties are seven years' imprisonment and a fine ranging from VND 20,000,000 to VND 200,000,000. So, the maximum sum of an administrative fine for the intrusion of privacy is VND 70,000,000 (approximately USD 3,000) and that of the criminal fine is VND 200,000,000 (approximately USD 8,600). These fines are quite low compared to

[5] See Decree No. 15/2020/ND-CP, on penalties for administrative violations against regulations post and telecommunications, information technology, and radiofrequency; Decree No. 98/2020/ND-CP, prescribing penalties for administrative violations against regulations on production and trade in counterfeit and prohibited goods, and protection of consumer rights; Decree No. 159/2013/ND-CP Providing for administrative penalties for violations arising in the realm of journalism and publishing; Decree No. 158/2013/ND-CP on Penalties for administrative violations about culture, sports, tourism, and advertising; Decree No. 176/2013/ND-CP on Penalties for administrative violations against medical laws, etc.

the fine of EUR 20,000,000 as laid out in GDPR. They do not correspond to the seriousness of the intrusion of privacy or personal data (Chu 2020).

Fourth, there is a lack of provision in law for protection of sensitive personal data, (i.e., personal data concerning racial origins, political views, religious beliefs, social organization participation, or health records). These are likely to be collected by local authorities for e-government systems, e-health, e-welfare, and so on, in smart cities.

Fifth, Vietnam does not have a comprehensive law on personal data protection. Instead, this matter is governed by various laws and decrees (about 70 documents). Nevertheless, all current related provisions are in the form of general—rather than specific—principles. Besides, they are not only insufficient but also contradictory, causing difficulties in law enforcement. For instance, Article 3(17) of the 2015 Law on Cyber Information Security provides that "processing of personal information means the performance of one or some operations of collecting, editing, utilizing, storing, providing, sharing or spreading personal information in cyberspace for commercial purpose." This definition is broader than that in the Articles 21 and 22 of the 2006 Law on Information Technology, which excludes the "collecting" and "utilizing" of personal information. The Law on Information Technology 2006 requires individuals and organizations to notify the personal information subjects of the scope, the purpose, the form, and the place of the collecting and utilizing of personal information before doing so, while the Law on Cyber Information Security 2015 only requires them to have the scope and the purpose notified (Prime Minister's 2020, Working Group 2020, p 24).

Sixth, personal data protection law continues to have some gaps. First and foremost, there are no definitions of "personal data" and "personal data protection." Hence, it is necessary to put forward these definitions and build a common understanding.

- Lack of Penalties for Selling Personal Data

Recently, the selling and buying of personal data have become more common, and the limits of current legal provisions prevent the problem from being dealt with effectively. According to Joint Circular No.10/2012/TTLT-BCA-BQP-BTP-BTT&TT-VKSNDTC-TANDTC on the Application of the Criminal Code provisions on some information technology and telecommunications related crimes, the act of selling and buying personal information does not constitute crimes without proof of it "inflicting serious consequences." For years, the police department for high-tech crime prevention (C50) has made many investigations regarding the selling and buying of personal information on the internet. Due to legal obstacles, those cases often get transferred to departments of information and communications for administrative violation handling (Thi 2018).

- Shortage of Provisions on Criminal Liabilities for the Infringement of Protected Rights to Personal Data

Article 159 of the 2015 Criminal Code provides for the "infringement upon secret information, mail, telephone, telegraph privacy, or other means of private information exchange"; Article 288 designates the "illegal provision or use of information on computer networks or telecommunications networks." However, these two articles have not been updated to include existing illegal acts relating to personal data (Prime Minister's 2020, Working Group 2020, p. 26). For example, Article 159 of the Criminal Code deals with the following acts: appropriation of another person's mails, telegraphs, telex, faxes, or other documents which are transmitted on the postal or telecommunications network in any shape or form; deliberately damaging, losing, or obtaining another person's mails, telegraphs, telex, faxes, or other documents which are transmitted on the postal or telecommunications network; listening or recording conversations against the law; searching, confiscating mails or telegraphs against the law. Article 288 of the Criminal Code deals with the following acts: trading, exchanging, giving, changing, or publishing lawfully private information of an organization or individual on the computer or telecommunications network without the consent of the information owner. In practice, neither of these articles have been updated to include current illegal acts relating to personal data protection, such as stolen social media accounts, personal data theft and illegal trading, and collection and use of personal data without notification or user protection mechanisms.

- Lack of Provisions on Cross-Border Transfer of Personal Data

Practices suggest that private enterprises can participate in supplying public services to smart cities' citizens under Public Private Partnership (PPP) contracts. Who would control the data generated then? How should the cross-border transfers of personal data by enterprises be regulated?

8.3 Recommendations: Making Law on Personal Data Protection

It is urgent to codify the provisions scattered in various legal documents. These provisions themselves are also insufficient. The new law should incorporate the following:

First, the legislation should straightforwardly define the concept of "personal data" and "sensitive personal data" and distinguish between "personal information" and "personal data." Personal data is interpreted to be data on individuals or relating to the identification or ability to identify a specific individual. For example, fundamental personal data should encompass full name, middle name, birth name, alias (if any); date of birth; date of death or missing; blood type, gender; place of birth, birth registration place, habitual residence, temporary residence, hometown, contact address, email address; academic level; nation; nationality; phone number; ID card

number, passport number, citizen identification number, driver's license number, license plate number, personal tax code number, social insurance number; marital status; and data that reflects activities or history of activities on cyberspace. In addition, sensitive personal data should include personal data on political and religious opinions; health conditions; genetics; biometrics; gender status; finance; the individual's actual geographical position in the past and present; social relationships; personal data about life, sexual orientation; personal data about crimes, criminal acts, and other personal data as specified by law and in need of necessary security measures.

Second, the new law should improve the provisions on transparency in collecting and utilizing personal data in smart cities. It is necessary to keep the balance between the need to collect and process citizens' information and data to operate a smart city and the need to ensure the right to privacy. To this end, the new law should provide procedures for collecting and sharing personal data.

Third, it is necessary to improve the provisions on (1) rights and obligations of parties concerning personal data, including rights of data subjects; obligations of the government and subjects collecting and processing data; obligations of third parties; and (2) acts prohibited. Vietnamese law recognizes the general principle of prohibiting the providing, trading, transferring, storing, using of information that violates the provisions on information safety and security. Nonetheless, all current legal documents center on the protection of national and military secrets. The new law should specifically provide for acts prohibited in collecting and processing personal data to create a legal base for setting out penalties (Chu 2020).

Appendix of Documents Reviewed

1. Circular No. 10/2016/TT-BGDDT dated April 5, 2016, issuing Regulations for student affairs in formal higher education programs.
2. Circular No. 35/2016/TT-NHNN dated December 29, 2016, on safety and confidentiality over the provision of banking services on the Internet.
3. Circular No. 57/2015/TT-BYT dated December 30th, 2015, detailing Decree No. 10/2015/ND-CP for childbirth by in vitro fertilization and conditions for surrogacy for humanitarian reasons.
4. Constitution dated November 28, 2013, of the Socialist Republic of Vietnam.
5. Decision No. 58/2007/QD-BGTVT of November 21, 2007, promulgating the regulation on inspection of quality, technical safety, and environmental protection in manufacture and assembly of motorcycles and mopeds.
6. Decree No. 10/2015/ND-CP dated January 28, 2015, on giving birth through in vitro fertilization and conditions for altruistic gestational surrogacy.
7. Decree No. 111/2010/ND-CP of November 23, 2010, detailing and guiding several articles of the law on judicial records.
8. Decree No. 123/2015/ND-CP dated November 15, 2015, on guidelines for law on civil status.

9. Decree No. 137/2015/ND-CP detailing several articles of, and providing measures for implementing, the Law on Citizen Identification.
10. Decree No. 158/2013/NĐ-CP of November 12, 2013, on penalties for administrative violations about culture, sports, tourism, and advertising.
11. Decree No. 159/2013/ND-CP dated November 12, 2013, providing for administrative penalties for violations arising in the realm of journalism and publishing.
12. Decree No. 176/2013/ND-CP dated November 14, 2013, penalties for administrative violations against medical laws.
13. Decree No. 20/2012/ND-CP dated March 20, 2012, prescribing the database on the execution of criminal judgments.
14. Decree No. 23/2015/ND-CP dated February 16, 2015, issuing copies from master registers, certification of true copies from originals, authentication of signatures, and contracts.
15. Decree No. 52/2013/ND-CP of May 16, 2013, on e-commerce.
16. Decree No. 56/2008/ND-CP of April 29, 2008, stipulating the organization and operation of tissue banks and the national coordination center for human organ transplantation.
17. Decree No. 64/2007/ND-CP of April 10, 2007, on information technology application in state agencies' operations.
18. Decree No. 72/2013/NĐ-CP of July 15, 2013, on the management, provision, and use of internet services and online information.
19. Decree No. 76/2012/ND-CP of October 03, 2012, detailing the implementation of several articles of the law on denunciations.
20. Decree No. 85/2016/ND-CP dated July 01, 2016, on the security of information systems by classification.
21. Decree No. 98/2020/ND-CP of August 26, 2020, prescribing penalties for administrative violations against regulations on production and trade in counterfeit and prohibited goods, and protection of consumer rights.
22. Decree No.15/2020/ND-CP of February 03, 2020, on Penalties for administrative violations against regulations post and telecommunications, information technology, and radiofrequency.
23. Decree of Government No. 35/2007/ND-CP of March 08, 2007, on banking e-transactions.
24. Joint Circular No. 06/2008/TTLT-BTTTT-BCA of November 28, 2008, on the assurance of infrastructure safety and information security in the post, telecommunications, and information technology activities.
25. Law No. 03/2007/QH12 of November 21, 2007, on prevention and control of infectious diseases.
26. Law No. 06/2012/QH13 of June 18, 2012, on Deposit Insurance.
27. Law No. 07/2012/QH13 of June 18, 2012, on Prevention of Money Laundering
28. Law No. 08/2012/QH13 of June 18, 2012, on Higher Education.
29. Law No. 100/2015/QH13 dated November 27, 2015, Criminal Code (amended in 2017).
30. Law No. 101/2015/QH13 dated 27 November 2015, Criminal Procedure Code.

31. Law No. 102/2016/QH13 dated April 05th, 2016, Children Law.
32. Law No. 103/2016/QH13 dated April 05th, 2016, Press Law.
33. Law No. 104/2016/QH13 dated April 06th, 2016, on Access to Information.
34. Law No. 105/2016/QH13 dated April 06th, 2016, on Pharmacy.
35. Law No. 13/2012/QH13 of July 20, 2012, on Judicial Expertise (amended in 2020).
36. Law No. 19/2012/QH13 of November 20, 2012, on Publishing.
37. Law No. 21-LCT/HDNN8 of June 30, 1989, of people's health.
38. Law No. 25/2018/QH14 dated June 12, 2018, on Denunciation.
39. Law No. 28/2009/QH12 of June 17, 2009, on judicial records.
40. Law No. 38/2005/QH11 of June 14, 2005, on Education, amended in 2009.
41. Law No. 38/2019/QH14 dated June 13, 2019, on Tax administration.
42. Law No. 40/2009/QH12 of November 23, 2009, on medical examination and treatment.
43. Law No. 41/2009/QH12 of November 23, 2009, on telecommunications.
44. Law No. 47/2010/QH12 of June 16, 2010, on credit institutions; Law No. 17/2017/QH14 dated November 20, 2017 amendments to some articles of the Law on credit institutions.
45. Law No. 49/2010/QH12 of June 17, 2010, on Post.
46. Law No. 50/2005/QH11 of November 29, 2005, on Intellectual property.
47. Law no. 51/2005/QH11 of November 29, 2005, on E-transactions.
48. Law No. 54/2014/QH13 dated June 23, 2014, on Customs.
49. Law No. 54/2019/QH14 dated November 26, 2019, on Securities.
50. Law No. 58/2014/QH13 dated November 20, 2014, on Social Insurance.
51. Law No. 59/2014/QH13 dated November 20, 2014, on Citizen identification.
52. Law No. 64/2006/QH11 of June 29, 2006, on HIV/AIDS prevention and control.
53. Law No. 67/2006/QH11 of June 29, 2006, on information technology.
54. Law No. 67/2011/QH12 of March 29, 2011, on Independent Audit.
55. Law No. 75/2006/QH11 of November 29, 2006, on a donation, removal, and Transplantation of human tissues and organs and donation and recovery of cadavers.
56. Law No. 81/2006/QH11 of November 29, 2006, on the residence.
57. Law No. 81/2015/QH13 dated June 24, 2015, on State Audit Office of Vietnam.
58. Law No. 86/2015/QH13 dated November 19, 2015, on Cyber Information Security.
59. Law No. 89/2015/QH13 dated November 23, 2015, on Statistics.
60. Law No. 91/2015/QH13 dated November 24, 2015, Civil Code.
61. Law No. 92/2015/QH13 dated November 25th, 2015, Civil Procedure Code.
62. Law No. 93/2015/QH13 dated November 25, 2015, on Administrative Procedures.
63. Law No.24/2000/QH10 of December 09, 2000, on Insurance Business (amended in 2010, 2019).
64. Law No.59/2010/QH12 of November 17, 2010, on Protection of Consumers' Rights.

65. Ordinance No.04/2002/PL-UBTVQH11 of November 04, 2002, on the organization of The Military Courts.

References

Article 21 (2013) The constitution of the socialist republic of Vietnam. https://constitutionnet.org/sites/default/files/tranlation_of_vietnams_new_constitution_enuk_2.pdf

Chu HT (2020) Report on legal framework for personal data protection in VietNam. Paper presented at the workshop on Sharing best practices in personal data protection on cyberspace, with focus on disadvantaged and vulnerable groups in VietNam, Hanoi, 09 December 2020.

Chu HT (2021) What solution to handle the situation of buying and selling personal information?. http://baochinhphu.vn/Phap-luat/Giai-phap-nao-xu-ly-tinh-trang-mua-ban-du-lieu-thong-tin-ca-nhan/433995.vgp

Ministry of Information and Communications (2021) Report on the state of smart city implementation in Vietnam

Nguyen AD (2020) Personal data protection in smart city—Experience and recommendations from Thua Thien Hue's case. Paper presented at the workshop on personal data protection and privacy in digital transformation and development of the digital economy: discussion and policy recommendations, Hanoi, 15 July 2020.

Prime Minister (2018) Decision No. 950/QD-TTg approving the project for sustainable smart urban development in Vietnam from 2018 through 2025, with a vision to 2030

Prime Minister's 2020 Working Group (2020) Report on legal regulation review in preparing for the Fourth Industrial Revolution

Thi C (2018) The situation of buying and selling personal information is rampant. https://kiemsat.vn/tran-lan-tinh-trang-mua-ban-thong-tin-ca-nhan-50866.html