

Personal Information Processing Activities and Information Security Safeguards in Public Health Emergencies: Postprint

Authors: Qi Yingcheng

Date: 2023-04-01T00:00:00+00:00

Abstract

[目的/意义] Personal information processing plays an extremely important role in the scientific governance of public health emergencies. However, in China's current response to public health emergencies, problems of illegal and improper processing of personal information exist. Based on this, regulating personal information processing behaviors in public health emergencies and establishing corresponding information security safeguard mechanisms hold significant value and practical significance.

[方法/过程] This paper employs grounded research methodology to identify the types of personal information and personal information processors involved in personal information processing behaviors during public health emergencies, analyzes citizens' risk perception regarding personal information processing behaviors and the objective factors influencing citizens' willingness to accept such behaviors, and proposes strategies for improving the regulatory rules for personal information processing behaviors and the information security safeguard system in public health emergencies.

[结果/结论] China's legislation should further clarify the principles and limitations of personal information processing in public health emergencies, and through measures such as imposing information security safeguard obligations on personal information processors and perfecting legal liabilities for improper processing of personal information, achieve effective regulation of personal information processing behaviors and adequate protection of personal information security in public health emergencies.

Full Text

Abstract

Purpose/Significance: Personal information processing plays an extremely important role in the scientific management of public health emergencies. However, China currently faces problems of illegal and improper personal information processing in responding to such crises. Therefore, regulating personal information processing behaviors during public health emergencies and establishing corresponding information security protection mechanisms holds significant value and practical importance.

Method/Process: This paper employs grounded research methodology to identify the types of personal information and personal information processors involved in personal information processing behaviors during public health emergencies, analyzes citizens' risk perception regarding personal information processing behaviors and objective factors affecting their willingness to accept such processing, and proposes strategies for improving regulatory rules and information security protection systems.

Result/Conclusion: Chinese legislation should further clarify the principles and limitations of personal information processing during public health emergencies, and achieve effective regulation of personal information processing behaviors and adequate protection of personal information security by imposing information security protection obligations on personal information processors and improving legal liabilities for improper processing.

Keywords: public health emergencies; personal information processing behaviors; legal regulation; information security protection

2 Literature Review

2.1 Risk Perception of Citizens in Public Health Emergencies

Zheng Baozhang and Feng Yi found that during the early stages of COVID-19 prevention and control, citizens' personal information was improperly processed in many regions, with information about confirmed patients, close contacts, or individuals returning from high-risk areas being leaked and illegally disseminated, affecting their daily lives and posing significant risks to their personal and property safety [8]. Xu Chuankun and Duan Gang, using personal location information processing as an example, noted that because location information directly contains citizens' private information and implies personal habits, travel patterns, and social status, citizens are unwilling to voluntarily disclose their location information during public health emergencies for reasons including privacy and property protection, which may increase the difficulty of epidemic prevention and control. They argued that improper processing of location information poses serious threats to citizens' rights and interests, necessitating clear legal regulations on such processing [9].

Zhu Jingjie and Wu Dahua discovered that during this public health emergency, citizens provided personal information to communities, workplaces, and disease control centers in accordance with national epidemic prevention requirements, but their information faced risks of improper processing, such as being publicly disclosed without desensitization, potentially harming citizens' privacy interests [10]. Foreign scholars R. Kai and C. Raffaele analyzed the risks associated with government use of contact tracing, surveillance tracking, and proximity tracking technologies to process citizens' personal information during this public health emergency, and dissected public concerns about potential violations of their rights and interests by personal information processing based on these technological means [11].

2.2 Emotional Attitudes of Citizens in Public Health Emergencies

Geng Ruiji and colleagues, based on uses and gratifications theory and cognitive psychology, analyzed public information acquisition behaviors during major public health emergencies and constructed a research model of public information acquisition behavior and fear of missing out under such circumstances [12]. H. Rao and N. Vemprala studied the release, sharing, and dissemination of COVID-19 information on Twitter from January to June 2020, pointing out differences in information behavior between government officials and ordinary citizens during the pandemic [13]. S. Song et al. analyzed Chinese citizens' information avoidance behavior during the COVID-19 period and, relying on S-O-R (Stimulus-Organism-Response) theory, constructed a relationship model between external stimuli (threats and information overload) and citizens' information avoidance behavior [14].

R. Fashey and A. Hino proposed that in responding to the COVID-19 pandemic, countries widely used digital contact tracing applications to process large-scale citizen personal information. During this process, public distrust of digital contact tracing applications could lead to refusal of tracking, thereby causing the failure of epidemic prevention measures based on personal information processing. Therefore, deeper analysis of public attitudes toward such personal information processing behaviors is needed [15].

2.3 Information Security Protection Systems in Public Health Emergencies

Chinese scholar Shi Cheng argued that Chinese legislation should clearly stipulate the basic legal principles for personal information processing during public health emergencies, the legitimate grounds for processing, and the legal liabilities for illegal processing to achieve adequate protection of personal information rights [16]. Wang Dongfang, focusing on personal information disclosure during public health emergencies, proposed determining different personal information disclosure pathways based on processing scenarios and specific types of personal information [17]. Zhan Nan believed that personal information protection during public health emergencies involves multiple stakeholders, and that

when collecting and utilizing personal information, both economic and social development needs and personal information protection requirements should be considered. He proposed a personal information lifecycle protection framework oriented toward privacy by design to guide personal information processing during public health emergencies [18].

Shen Weiwei argued that the COVID-19 pandemic has essentially placed China in a state of emergency, adopting numerous stress-based, unconventional digital epidemic prevention measures including personal data collection and national information monitoring, which have caused temporary imbalances between state power and citizens' fundamental rights. Therefore, a legal mechanism for restoring digital emergency states should be established to address the normalization of erosion of citizens' fundamental rights by expanded state power during epidemic prevention and control [19].

3 Research Design

3.1 Research Methods

This study employs semi-structured interview questionnaires to conduct in-depth interviews with research subjects for data collection, providing empirical materials for the research. It then adopts grounded theory to code the collected data, forming concepts and theories through constant comparison and conceptual extraction to objectively and deeply analyze citizens' risk perception and emotional attitudes toward personal information processing behaviors during public health emergencies, thereby proposing corresponding legal improvement recommendations for existing problems.

Grounded theory, proposed by A. Strauss and B. Glase, is a qualitative research method that embraces constructivist ontology and relativist epistemology, 致力于发掘对现象的新认识和理解 [20], advocating theory building based on in-depth interviews rather than a priori self-created theories [21]. In-depth interviews are one of the most commonly used data collection methods in grounded theory, being highly interactive and aimed at collecting interviewees' descriptions of their lived world, analyzing their interpretations of described phenomena, thereby generating research questions and theories from respondents and revealing their feelings and motivations [22].

Citizens' risk perception and emotional attitudes toward personal information processing behaviors during public health emergencies are difficult to directly observe. This study's use of in-depth interviews better enables understanding and observation of such individual experiences, making it suitable for the research questions. The grounded theory approach mainly includes three processes: open coding, axial coding, and selective coding. Finally, theoretical saturation and reliability verification must be conducted. If research conclusions pass verification, relevant theories are formed; otherwise, materials are supplemented and coding continues until verification is passed [23].

3.2 Sample Selection

This study follows two principles in selecting interview samples: First, respondents must be subjects affected by personal information processing behaviors during this public health emergency (the COVID-19 pandemic), such as those who cooperated with epidemic prevention and control by permitting government agencies, enterprises, universities, or communities to process their personal information. Second, respondents' age, gender, education level, and region are randomly distributed. Considering that processing minors' personal information should in principle obtain guardian consent, minors are excluded from the interview scope.

Regarding age group selection, since elderly populations lack mastery of communication devices and information technology, were relatively less affected by personal information processing behaviors during the pandemic, and their subjective feelings and experiences differ from mainstream groups [24], this study primarily selects individuals aged 20-60 as the sample population. In terms of regional risk level determination, the highest risk level appearing in the respondent's district/county during the entire pandemic period serves as the standard. Through pre-interview investigations, basic information for 18 respondents was obtained, as shown in Table 1 .

3.3 Data Collection and Organization

To achieve research objectives, interviews focused on "respondents' subjective descriptions of their risk perception and emotional attitudes toward personal information processing behaviors during public health emergencies." The interview outline was formed based on reading and organizing other literature. Interviews were primarily face-to-face, with 4 respondents interviewed by telephone. Each interview involved one respondent interviewed in depth by the researcher, lasting 10-20 minutes. Original interview data were preserved as recordings and converted to text for subsequent analysis. For statistical convenience, each interview record was numbered.

Through pre-interview investigations, 18 individuals who had experienced personal information processing during the COVID-19 pandemic were ultimately identified as the sample group. The specific interview outline included: Basic information such as age, education level, and regional epidemic severity; Specific experiences of personal information processing during the pandemic, including what personal information was processed by what types of entities and how; Main risk factors perceived regarding personal information processing behaviors during public health emergencies; Objective factors affecting willingness to accept personal information processing behaviors and views on such processing. After interviews, 6 respondents covering various age groups, genders, education levels, and regional risk levels were selected for follow-up visits to ensure that the organization, summary, and extraction of interview content accurately reflected respondents' true thoughts.

4 Research Process

4.1 Open Coding

The first step in grounded theory is open coding, which involves discovering conceptual categories and dimensions from interview data. During coding, this study analyzed each respondent's answers, identified initial concepts appearing three or more times, analyzed their relationships to derive categories and dimensions, and ultimately obtained 17 categories. The open coding process is shown in Table 2 .

4.2 Axial Coding

The second step in grounded theory is axial coding, which aims to discover and establish connections between conceptual categories and dimensions, identifying main categories from initial categories to express various relationships between parts of interview data. By analyzing and summarizing the initial categories from open coding, this study found that some initial categories had closer internal associations and could be grouped together. For example, both sensitive information and directly identifiable information point to types of personal information processed during public health emergencies; concepts such as government agencies, units/schools, and medical institutions all point to types of personal information processors; concepts like improper processing and excessive processing reflect citizens' risk perception of personal information processing behaviors during public health emergencies; and public responsibility cognition factors and risk factors belong to objective factors affecting citizens' willingness to accept personal information processing. Based on these criteria, this study further refined initial categories into 4 main categories, with the axial coding process shown in Table 3 .

4.3 Selective Coding

The third step in grounded theory is selective coding, which aims to further integrate and refine categories formed through axial coding, identifying core categories that encompass the results contained in original data within a comprehensive theoretical framework to form theoretical frameworks or paradigms. Among them, "types of processed personal information" refers to the specific objects of personal information processing during public health emergencies, determining the objects protected by personal information processing regulation rules and information security protection systems, summarized as the "object dimension" core category. "Types of personal information processors" points to subjects conducting personal information processing during public health emergencies, determining the specific subjects to which regulation rules and protection systems apply, summarized as the "subject dimension" core category. "Citizens' risk perception of personal information processing behaviors" emphasizes specific risks perceived by citizens during public health emergencies, determining the main legal risks that regulation rules and protection systems

need to address, summarized as the “risk dimension” core category. “Objective factors affecting citizens’ willingness to accept personal information processing behaviors” reveals citizens’ behavioral logic and emotional attitudes during public health emergencies, summarized as the “emotion dimension” core category, which determines citizens’ demands that regulation rules and information security protection systems must respond to and consider. These categories constitute the main dimensions of personal information processing behaviors during public health emergencies and the main directions for building information security protection systems.

4.4 Reliability, Validity, and Theoretical Saturation Testing

This study established good trust relationships with respondents during interviews, continuously compared concepts and categories during coding, and employed participant verification methods by sending organized interview texts to interviewees for them to evaluate whether the content reflected their true thoughts at the time. The author conducted separate follow-up visits with 6 interviewees, who all recognized the organization, summary, and extraction of interview content. For example, Respondent A3 noted: “The interview text basically made no changes or subjective adjustments to the interview content except for removing individual oral expressions during the interview process, and it objectively and accurately reflects my thoughts.”

This study adopts the Holsti formula for reliability testing, with reliability greater than 0.8 indicating acceptable research conclusion reliability. There were two coders: the author and another graduate student. The specific process was: Training the other coder to fully understand research purposes, category meanings, and coding operation requirements; Coding interview texts uniformly, marking “√” if a category was involved and leaving it unmarked if not;

Counting coding results and calculating reliability using the Holsti inter-coder agreement formula. As shown in Formula (1):

$$R = \frac{1 + (n - 1) \times K}{n}$$

Where R represents reliability, n is the number of coders, and K is the average inter-coder agreement. Since this study had 2 coders, the average inter-coder agreement between them is calculated as shown in Formula (2):

$$K_{AB} = \frac{2M_{AB}}{N_A + N_B}$$

Where M_{AB} represents the number of identical codes between the two coders (16 in this study), and N_A and N_B represent the respective coding quantities of the two coders (17 and 21). The calculated K_{AB} is 0.84, and substituting into the reliability formula yields $R = 0.913$, greater than 0.8, passing reliability verification.

As a criterion for determining when to stop sampling, theoretical saturation testing refers to proving through alternating data collection and analysis that no new theoretical insights can be generated from newly collected data and that no new category characteristics can be developed [25]. In this study, through in-depth interviews with the last 5 respondents and random sampling and coding of these 5 interview materials according to procedural grounded theory data coding methods, the results still conformed to the 脉络 and relationships presented in the model without forming new categories. This indicates that the grounded theory model established in this study meets saturation testing requirements.

5 Discussion and Analysis

Based on grounded theory analysis and coding of interview texts, this study abstracted 4 main categories related to personal information processing behaviors during public health emergencies: types of processed personal information, types of personal information processors, citizens' risk perception of personal information processing behaviors, and objective factors affecting citizens' willingness to accept personal information processing behaviors. These correspond to 4 different dimensions of personal information processing behaviors during public health emergencies: object dimension, subject dimension, risk dimension, and emotion dimension. Observing problems in personal information processing behaviors during public health emergencies and citizens' risk perception and emotional attitudes from these dimensions enables relatively accurate and comprehensive understanding of the necessity of regulating personal information processing behaviors and areas needing improvement in corresponding systems, thereby proposing improvement recommendations for regulation rules and information security protection systems.

5.1 Objects of Personal Information Processing Behaviors in Public Health Emergencies

From the perspective of specific objects targeted by personal information processing behaviors during public health emergencies, for the purpose of responding to epidemic transmission and diffusion risks, information processors may process various types of personal information, including citizens' identity information, contact details, home addresses, health status, and location information. Some information constitutes sensitive personal information because it reveals citizens' physical conditions, physiological characteristics, movement trajectories, and interpersonal interactions. Such information is closely associated with information subjects' personal dignity, and when improperly processed, may endanger their personal and property safety and easily cause damage to personal reputation, physical and mental health, or discriminatory treatment. During interviews, respondents expressed particular concern about sensitive personal information, with processing of such information making them perceive higher risk potential. Additionally, citizens' identity information and contact details are directly identifiable personal information that directly reveals specific infor-

mation subjects' attributes and is more closely related to their personal interests and information privacy. When such information is improperly processed, the threat to information subjects' rights and interests is more direct and severe. Therefore, compared to indirectly identifiable personal information, respondents during public health emergencies paid more attention to processing of directly identifiable personal information and expressed hope for using de-identification technologies to avoid direct exposure of their identity information as much as possible.

In response to citizens' above risk perception and emotional attitudes, China's personal information protection legislation should further implement necessity requirements for personal information processing behaviors during public health emergencies, authorizing relevant organizations and individuals to process citizens' sensitive personal information and directly identifiable personal information only when necessary. In the early stages of the COVID-19 outbreak, government departments and grassroots organizations tended to use directly identifiable personal information when releasing pandemic-related information to achieve sufficient risk warning effects. However, names and contact details of confirmed, suspected patients, and close contacts do not fall within the scope of public right to know and may expose information subjects' private matters they do not wish to disclose. In early 2021, health commissions in Beijing, Shanghai, and other places began to conceal patients' age and gender information or even only disclose their movement trajectories without revealing specific identities [26]. These measures fully guarantee citizens' right to know while effectively protecting information subjects' personal information rights and interests, helping achieve balance between public interests and natural persons' private rights during public health emergencies and deserving adoption by legislative systems.

5.2 Subjects of Personal Information Processing Behaviors in Public Health Emergencies

From the perspective of personal information processor types, various entities including government agencies, units/schools, medical institutions, communities/property management companies, shopping malls, and stores processed citizens' personal information during the COVID-19 response. Among them, subdistrict offices, property companies, and shopping malls are not institutions with statutory personal information processing authority but only temporarily assumed responsibility for grid-based investigation and monitoring of citizens' health conditions and movement trajectories based on government delegation or authorization. According to respondents' statements, they generally perceived that grassroots organizations had many irregularities in processing personal information and failed to fully fulfill information security protection obligations, resulting in leakage of personal privacy information and infringement of relevant citizens' rights and interests. The fundamental reason lies in the generally weak awareness of personal information security risks among staff in these organizations, most of whom lack professional experience, technical capabilities,

and equipment to properly store, maintain, and manage personal information. Personal information processors hold a trusted fiduciary position in their relationship with information subjects who entrust them with personal information based on trust. Personal information processors should owe corresponding fiduciary duties to information subjects, and Chinese legislation should further clarify personal information processors' information security protection obligations during public health emergencies [27].

Furthermore, when government departments need to authorize or delegate grassroots organizations to process personal information for public health emergency prevention and control purposes, they should ensure that delegates possess adequate information security protection capabilities and adopt sufficient information security protection measures. They should also stipulate delegates' personal information protection obligations and responsibilities through contracts, conduct regular audits and personal information security impact assessments, and require them to accurately record and preserve processing situations. After the delegation relationship ends, they should urge timely transfer or deletion of relevant data [28]. Grassroots organizations and enterprises should also actively conduct specialized personal information protection training to improve staff information security awareness and capabilities.

5.3 Risks of Personal Information Processing Behaviors in Public Health Emergencies

This study found that citizens' risk perception of personal information processing behaviors during public health emergencies mainly manifests as improper processing, excessive processing, and failure of some information processors to adopt necessary security protection measures. Additionally, lack of transparency in personal information processing behaviors exacerbates citizens' uncertainty about personal information processing risks. Meanwhile, respondents generally believed that when their personal information is improperly processed, effective avenues are lacking for holding information processors legally accountable and claiming remedies for their losses.

In response to these risks, Chinese legislation should further improve corresponding information security protection systems. During public health emergencies, based on the urgency and priority of public health and social interests, it is necessary to impose certain restrictions on individual rights and freedoms, but such restrictions must also be constrained by legal provisions and the principle of proportionality [29]. Regarding personal information processing behaviors, they must have legitimacy and cannot improperly process personal information under the pretext of epidemic prevention and control. Personal information processors should only process personal information within necessary scope, strictly follow minimization requirements, and avoid unnecessary processing of citizens' directly identifiable personal information through methods like health codes. Simultaneously, personal information processors should adopt necessary information security protection measures to prevent unauthorized access and per-

sonal information leakage, theft, alteration, or deletion, and regularly evaluate security protection measures adopted in their personal information processing activities [30].

Moreover, Chinese legislation should further improve legal liabilities for illegal personal information processing and remedies for citizens' information rights and interests. At the public law level, personal information processors who illegally process personal information or fail to fulfill necessary information security protection obligations during processing can be subject to legal liabilities including warnings, fines, and administrative sanctions. At the private law level, for situations where natural persons' personal information rights and interests are damaged due to illegal personal information processing, natural persons should be allowed to file corresponding civil lawsuits to claim damages, and a personal information public interest litigation mechanism should be established.

5.4 Objective Factors Affecting Citizens' Willingness to Accept Personal Information Processing Behaviors in Public Health Emergencies

This study found that during public health emergencies, Chinese citizens could actively cooperate with necessary personal information processing by relevant subjects based on their cognition of legal obligations and public responsibilities they bear. However, in this process, based on doubts about the qualifications and information protection capabilities of some personal information processors and concerns about some sensitive and directly identifiable personal information, they might conceal personal information or provide false information when information security risk levels are high.

In response to these objective factors affecting citizens' willingness to accept personal information processing behaviors, China's information security protection system should establish hierarchical personal information protection rules, adopting differentiated regulation strategies for processing directly identifiable versus indirectly identifiable personal information and sensitive versus general personal information. For directly identifiable and sensitive personal information, processing should in principle only be permitted with information subjects' consent, while regulation requirements can be moderately relaxed for non-sensitive, indirectly identifiable personal information. Additionally, legislation should impose continuous security protection obligations on information processors, stipulating that only statutory institutions and personnel have the authority to collect and release pandemic-related personal information within legally prescribed scopes. Any other units or individuals cannot process citizens' personal information under the pretext of epidemic prevention and disease control, otherwise constituting infringement of information subjects' rights and interests and incurring corresponding legal liabilities [31].

6 Research Conclusions

At the theoretical level, this study constructs a path for personal information processing behaviors during public health emergencies through grounded theory methodology, analyzing types of personal information processed, types of personal information processors, citizens' risk perception, emotional attitudes, and objective factors affecting willingness to accept personal information processing behaviors during epidemic prevention and control. This theoretical analysis can provide theoretical basis and reference for improving regulation rules for personal information processing behaviors during public health emergencies.

At the practical level, as emergency management in any country should include at least legislation and implementation [32], and against the backdrop of China currently formulating the Personal Information Protection Law, this study's legal regulation recommendations for personal information processing behaviors during public health emergencies can provide reference for relevant legislative improvements and guidance for scientific and standardized personal information processing by government departments and social organizations in future public health emergency responses. Compared with existing research, this study adopts the innovative grounded theory methodology to obtain research materials on citizens' risk perception and emotional attitudes toward personal information processing behaviors during public health emergencies, providing an empirical foundation for theoretical improvement recommendations and helping ensure that legal system proposals truly respond to citizens' and society's real needs.

However, this study still has limitations. First, information loss cannot be completely avoided during interview data organization, potentially causing some deviation in concept and category induction. Second, this study only employed qualitative research methods, making research methods relatively thin. Future research should focus on quantitative analysis of personal information processing behaviors and protection systems during public health emergencies to achieve combination of qualitative and quantitative research, ensuring more adequate scientific support for research conclusions.

References

- [1] Regulations on Public Health Emergency Response [EB/OL]. [2021-02-05]. http://www.gov.cn/gongbao/content/2011/content_{1860801}.htm.
- [2] ZHANG Z D, RANTALA J, VIRRANTAUTAUS K. A fuzzy multiple-attribute decision-making modelling for vulnerability analysis on the basis of population information for disaster management [J]. *International Journal of Geographical Information Science*, 2014, 28(9): 1922-1939.
- [3] KOSUGI M, UTSU K, TAJIMA S, et al. Improvement of twitter-based disaster-related information sharing system [C]//2017 4th International Conference on Information and Communication Technologies for Disaster Management. Arlington: IEEE, 2017: 1-7.

- [4] STUART J B. Information management research and practice in the post-COVID-19 world [J]. *International Journal of Information Management*, 2020, 55: 102175.
- [5] BEAUNOYER E, DUPERE S, GUITTON M J. COVID-19 and digital inequalities: reciprocal impacts and mitigation strategies [J]. *Computers in Human Behavior*, 2020, 111: 106424.
- [6] JIN S, ZHANG L B. Research on personal information protection under public health emergencies: taking the COVID-19 epidemic as background [J]. *Information Studies: Theory & Application*, 2020(6): 16-22.
- [7] HUI Z B. Preliminary exploration of information release and management of public emergencies in China under new media environment [J]. *Library and Information Service*, 2011, 55(3): 18-26.
- [8] ZHENG B Z, FENG Y. Research on privacy protection under big data background: from the perspective of personal information use in COVID-19 epidemic prevention and control [J]. *Study & Exploration*, 2021(4): 74-78.
- [9] XU C K, DUAN G. Exploration on policies and regulations of citizen location information application in public health emergency prevention and control [J]. *Guangxi Social Sciences*, 2021(1): 106-111.
- [10] ZHU J J, WU D H. The dilemma and solution of personal data public disclosure in major infectious disease epidemic prevention and control: taking COVID-19 epidemic prevention and control as example [J]. *Electronics Intellectual Property*, 2021(4): 78-90.
- [11] KAI R, RAFFAELE C, SANDRA P, et al. Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level [J]. *European Journal of Information Systems*, 2020, 29(6): 731-745.
- [12] GENG R L, XU J G, JIN Y, et al. Research on public information acquisition behavior and fear of missing out under major public health emergencies: taking COVID-19 as example [J]. *Library and Information Service*, 2020, 64(15): 112-122.
- [13] RAO H R, VEMPALA N, PATRICIA AKELLO P, et al. Retweets of officials' alarming vs reassuring messages during the COVID-19 pandemic: implications for crisis management [J]. *International Journal of Information Management*, 2020, 55: 102187.
- [14] SONG S, YAO X, WEN N. What motivates Chinese consumers to avoid information about the COVID-19 pandemic?: the perspective of the stimulus-organism-response model [J]. *Information Processing and Management*, 2021, 58: 102407.
- [15] FAHEY R A, HINO A. COVID-19, digital privacy, and the social limits on data-focused public health responses [J]. *International Journal of Information Management*, 2020, 55: 102181.

- [16] SHI C. Legal basis for personal information use in epidemic prevention and control [J]. Library Development, 2020(3): 82-90.
- [17] WANG D F. Limits and optimization paths of personal privacy information disclosure in major epidemic prevention and control [J]. Information Studies: Theory & Application, 2020(2): 11-24.
- [18] ZHAN N. Research on personal information protection in major epidemic prevention and control: based on privacy protection by design theory [J]. Journal of Modern Information, 2021(1): 101-110.
- [19] SHEN W W. On the restoration mechanism of digital emergency states: taking COVID-19 epidemic prevention and control as example [J]. Tsinghua University Law Journal, 2021(2): 121-142.
- [20] ZHAN N. Research on personal information management behavior based on grounded theory [J]. Library Science Research, 2016(15): 11-20.
- [21] QI X P. Construction of administrative judges' difficult case adjudication model [J]. Tsinghua University Law Journal, 2018(12): 191-206.
- [22] JIA R N, WANG X W. Research on social media user switching behavior characteristics based on grounded theory [J]. Research on Library Science, 2018(17): 26-33.
- [23] MA X C, FENG Y. Research on factors influencing new media information quality based on grounded theory [J]. Information Studies: Theory & Application, 2017(4): 32-36.
- [24] WU Q. Research on influencing factors of rural elderly's epidemic prevention information search during public health emergencies [J]. Library Tribune, 2020, 40(9): 106-114.
- [25] ZHU S B, DENG X Z. Research on influencing factors of elderly people's online health information seeking behavior [J]. Library and Information Service, 2015, 59(5): 60-67, 93.
- [26] Epidemiological investigation reports "don't mention people," respecting personal privacy rights [EB/OL]. [2021-03-15]. http://www.xinhuanet.com/comments/2021-01/25/c_{1127020349}.htm.
- [27] LIU G. Research on the public law framework of personal information protection: taking public health emergencies as example [J]. Gansu Social Sciences, 2020(4): 155-162.
- [28] ZHOU H H. Exploring incentive-compatible personal data governance: the legislative direction of China's personal information protection law [J]. Chinese Journal of Law, 2018(2): 3-23.
- [29] LIU H Z. Limits on restriction of citizens' fundamental rights in anti-epidemic actions [J]. Human Rights, 2020(2): 11-24.

- [30] JACK M B. Information fiduciaries and the first amendment [J]. UC Davis Law Review, 2016, 49(4): 1183-1234.
- [31] ZHAO H. Restriction and boundaries of individual rights under epidemic prevention and control [J]. Comparative Law Review, 2020(2): 45-58.
- [32] ZHANG H B, TONG X. Structural changes in China's emergency management and their theoretical generalization [J]. Social Sciences in China, 2015(3): 58-84, 206.

Qi Yingcheng

1 School of Law, Jilin University, Changchun 130022 2 Big Data Management Research Center, Jilin University, Changchun 130022

Abstract: [Purpose/significance] The processing of personal information plays an extremely important role in the scientific management of public health emergencies. However, there are problems of illegal and improper processing of personal information in the process of responding to public health emergencies in China. Based on this, it is of great value and practical significance to regulate personal information processing behaviors in public health emergencies and establish corresponding information security protection systems. [Method/process] This paper uses grounded research method to identify types of personal information and personal information processors involved in personal information processing behaviors in public health emergencies, analyzes citizens' risk perception of personal information processing behaviors and objective factors affecting citizens' willingness to accept personal information processing behaviors, and proposes strategies for improving regulation rules and information security protection systems for personal information processing behaviors in public health emergencies. [Result/conclusion] Chinese legislation should further clarify the principles and restrictions on personal information processing in public health emergencies, and achieve effective regulation of personal information processing behaviors and full personal information security protection by entrusting personal information processors with information security protection obligations and improving legal responsibilities for improper personal information processing.

Keywords: public health emergencies; personal information processing behaviors; legal regulation; information security protection

Note: Figure translations are in progress. See original paper for figures.

Source: ChinaXiv — Machine translation. Verify with original.