Pathway to Refine the Informed Consent Rules for Data Collection in the Context of IoT

Shen Xie[1], Cheng Chen[2(✉)], and Huang Shuyi[1]

[1] Department of Marine Culture and Law, Jimei University, Xiamen 361021, Fujian, China
[2] Law School, Fuzhou University, Fuzhou 350108, Fujian, China
chengchen_cy@yeah.net

Abstract. With the development of information technology and the wide popularization of the application of the Internet of Things, the attention of all sectors of society to the protection of personal information is also increasing. In the field of information security of personal protection, establish how to correctly handle the personal information of effective rules, speed up the building, with emphasis on the "informed consent rules" personal information processing rules, it requires powerful legal rules and effective corresponding implementation path, to improve the information processing platform for information processing activities, ensure the citizens' personal information security.

Keywords: Personal Information · Informed Consent Rules · Information Security

1 Introduction

With the rapid development and systematization of the big data network space, namely the "fifth space", the amount of personal information data shows a blowout growth trend. The value of personal information is mainly due to the degree to which it is desired by various data applications such as the Internet of Things, and these popular applications rely on the huge personal information data support, far beyond TeraByte, but ZettaByte as the basic unit of computing. Personal information processing data of this scale shows a high utilization value in the hands of information processors, and then promotes the commercialization process of personal information, making information processors more and more urgent.

In this context, as the subject of the information data object, the owner of personal information has a significant conflict with the information processor and the demand of information commercial application. This conflict is consistent with the phenomenon of "market failure" mentioned by scholars, which is mainly reflected in the information asymmetry between the personal information protection party and the information and data processing party. As an individual information owner, it is difficult to effectively control the use mode and means of his personal information, and often he can only rely on the application platform and processing mode of the data processor to obtain

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2026
Published by Springer Nature Switzerland AG 2026. All Rights Reserved
D.-J. Deng and J.-C. Chen (Eds.): SGIoT 2024, LNICST 633, pp. 141–152, 2026.
https://doi.org/10.1007/978-3-031-93825-2_13

convenience, so that it is difficult to avoid the risk of infringement of personal information rights and interests.

In the current digital age, data and information are closely linked, and information is contained in the data. Although the existing legislation of "personal information" and "personal data", and respectively, formed the "information" and "data", independent of each other of dual architecture, but its core purpose is to maintain the rights and interests of personal information subject, safeguard the reasonable use of data and sharing, in order to promote the healthy development of the digital industry.

Reviewing the past legal process, from the Criminal Law Amendment (IX) to the violation of personal information activities as a criminal behavior, to the introduction of various supporting laws and regulations, China's personal information protection legal system is gradually entering the track of high-speed development. The continuous improvement of administrative regulations and departmental rules, as well as the birth of a series of national standards related to information protection, all demonstrate China's firm determination and unremitting efforts in protecting the security of citizens' personal information. At present, the Personal Information Protection Law, as the main legal framework to protect individual interests, clearly supports the important personality interests contained in personal information, and gives individuals the right to know and right to collect the scope, content and use of their information. through the implementation of the "informed-consent" rule, the law aims to protect the individual's free will and information right to self-determination, so as to alleviate the conflicts between personal information owners and information processors.

Therefore, this paper aims to deeply analyze the difficulties and challenges of the "informed consent rule" in the real application from the perspective of personal information protection, and explore the feasible solutions for its application. By balancing the relationship between personal information protection and information public interest, this paper strives to stimulate the vitality and potential of digital economy while protecting individual personality rights and interests.

2 Overview of the Informed Consent Rules for Data Acquisition

The informed consent rule, which is a measure for the protection of personal information. In the field of data collection, it refers to the normative system in which the information processor must notify the user in a clear and clear way and obtain its clear consent before processing the user information within the scope of authorization. Informed consent rules consof "notification rules" and "consent rules". Although they have their own emphasis, they complement each other. Among them, there is a sufficient progressive relationship between "notification" and "consent", that is, without the clear and effective consent of the individual, the personal information shall not be handled at will, otherwise it will constitute infringement. In addition, this notification must be fully, clear and direct to ensure that the information subject can truly and effectively express its wishes.

The theoretical basis of informed consent rules lies in the relativity of right grant and restriction. Among them, the "consent" rule gives the information processor the right to process information legally, and also implies the restriction of rights. This thought dates back to Locke's argument of personal freedom that the rights of individuals should not

be subject to borderless limitations. In the field of personal information protection, the informed consent rules set up a layer of "soft shell" for the activities of the information processors, and the information processing can only be conducted with the consent of the information subject. The history of the rule can be traced back to 1970, Germany data protection law, and European and American countries in personal information and digital legal protection exploration is more extensive and frontier, especially in 2016, the general data protection ordinance (GDPR), not only with the informed consent system, also agree to personal information subject requirements for clear and clear definition [1], greatly promoted the international legal community of personal information protection. In addition, the research of Professor Louisa Spector of Germany also provides us with useful reference. She discussed how information processors exchange personal information for digital content or services in the digital age, and explored the role of consent rules and new contracts in protecting personal personality rights and interests [2].

Article 17 of China's Personal Information Protection Law clearly stipulates the "notification and consent rules", marking the establishment of the personal information processing and consent system in China's legal system. In view of the diverse interests carried by personal information, including civil rights such as personal dignity and privacy, the implementation of the informed consent rules set up in the Personal Information Protection Law must be able to comprehensively and meticulously coordinate these interests. However, the details and application of this rule still need to be further explored and perfected. In the face of the strong data processing ability of information processors, the subject of personal information is often in a weak position, faced with problems such as information asymmetry and barriers. Therefore, China will accelerate the introduction of relevant laws and norms, clarify the obligations of information processors, and improve the specific application of the notification and consent rules, aiming to better protect the rights and interests of personal information.

3 The Dilemma Faced by the Informed Consent Rules

3.1 Users' Control of Information Extremely Asymmetric

The purpose of the consent rules is to prevent the information processors from exceeding the limit and improper use of users' personal information, and to protect the personal information freedom through the pre-imposed consent rules.

It should be noted that the user's personal information is in the risk of overexposure every moment, and the natural person's control over his personal information is in a very asymmetric state with the corresponding risks he needs to bear. Mainly reflected in: personal control of information is weak and difficult to fully control; natural person as individuals have a very huge risks. In the stage of acquisition, processing and feedback in the information chain, it is always in a weak and passive position. On the contrary, as the owner and authority processor of a huge database, the information processors can quickly capture, copy and disclose the information data of individual users based on a wide range of platforms and powerful computing systems. In the information age, driven by great computing power and massive big data, the storage and control of personal information are far weaker than that of enterprise platforms and state organs, and the latter's desire to obtain information is far more than the general public imagination,

which is due to the natural profit-driven of capital. According to the survey of scholars, deleting a basic document may be simple, but if you need to delete the file calculated by Ze byte (ZettaByte), the trillions of files are a significant cost for the server and storage hardware, as well as the loss of computing power. The simulated state database generated by massive information accumulation cooperates with high-speed computer and cloud technology system, and even predicts the future consumption trend and predetermined possible users to a certain extent, and it is difficult to guarantee the security of individual information privacy.

Driven by today's rapid development of data information technology, processing applications can automatically and quickly collect and store personal information. In addition, the commercialization speed of personal information is very fast, and the demand of enterprises is large, which causes quantitative change and qualitative change. When the basis of the information reached a certain degree, with now big data cloud computing technology, the parties for its statistical results and basic characteristics and classification, derived the future consumption situation and potential user information are very eager, is bound to produce excessive collection and use, which exacerbated the possibility of personal information is abused. Perhaps, the information processor, as the service partner, should be able to more accurately locate the specific needs of users, and stratify them. Optimize information services while steadily increasing the number of users and user stickiness. However, if massive personal information is used to implement group classification, that is, "killing"; or using past information data for behavior manipulation, seriously endangering the personality rights and interests and information freedom of natural persons, how can individuals block? It is not feasible to rely solely on the "informed consent rules", and it needs to be further made, so that enterprises still need to be calm down in the face of the huge information resources, and collect, process and use the information to earn profits reasonably in accordance with the regulations. This also requires further refinement of informed consent rules, and classifying information at different levels, different ranges and different stages. At present, the application of informed consent rules is still not perfect. In addition to the asymmetry of personal control over information and the risks, it is also reflected in the defects of the "notification" obligation leading to the false consent rules and the improper expansion of the exception of informed consent rules.

3.2 Information Processor' Notification Obligation Defective

With text barriers to prevent users from knowing. In the digital age, people's lives are clearly running out of smartphones and the apps installed. According to the survey, as China enters the era of rapid development of data and information, in the statistics of various application stores, the number of high-frequency software downloads exceeds 100 million times, and social platforms such as WeChat and Weibo exceed 200 million times. As is known to all, the first stage for individuals to enter the software use process is to log in and enter their personal account. In order to further use the software, they must agree to the collection of personal information by the software platform. This leads to the information processor in the face of so many user groups in the process of login, the production of privacy policy informed and informed consent, enterprise compliance management documents cannot alone for different groups or different application

requirements, information processing will not carefully told individual, mostly adopt the way of formatting, unified inform users directly, save time and resource cost, reduce the enterprise platform of cloud force demand loss, increase user viscosity. According to incomplete analysis and statistics, the number of words in WeChat privacy policy, JD privacy policy and Taobao personal information protection policy is about 12,000 words, and some travel software privacy policies are more than 20,000 words. Faced with such a large number of words, it is difficult for even professional lawyers to understand the corresponding privacy policies and software collection scope of personal information within a few hours. Take WeChat, the most downloaded app, for example, the WeChat privacy policy has about 11,107 words, which takes about 56 minutes to read the full privacy policy, or 200 words per minute. This is just a complete understanding and avoidance during the use of information to prevent information leakage. This inevitably leads to the notification obligation of information processors seems to be detailed and detailed, but in fact, it is the use of professional text barriers to isolate the general public. If you want to use a high degree of software, you must click "agree" to continue, quite "if you want to cross this way, you must stay to buy money" taste. It should be noted that in the highly technical Internet service, it itself has certain monopoly characteristics. Assuming that users are dissatisfied with the conditions covered by the privacy policy and "do not agree" with the privacy policy of the application platform, they will not be able to continue to use the services of the software [3]. This makes the privacy policy a bully format clause. This makes reading the privacy policy and "voluntary click consent" the biggest lie in today's data age.

The agreement rules are a mere formality. According to the end of 2021, the National Computer Network Emergency Technology Coordination Center and the China Cyberspace Security Association released the illegal collection and Use of Personal Information, the problem of App showed a downward trend, with the proportion falling from the highest 26.1% in 2019 to 6.7% in 2021. This is inevitably related to the personal Information Protection Law issued in that year, and also related to the increased supervision of government departments. But as mentioned above, does the simple privacy policy mean that the notification obligation of the information processor is fully fulfilled? As the party with the biggest profit benefit, the information processor naturally occupies the data high ground, and the individual information owner can only agree to its collection and processing in a passive and passive way. In the era of big data, the individual information owner inevitably against the privacy on attitude, but know the privacy policy requires time and cost, lead users passive knowledge about the interests of personal information, and more because unable to refuse the convenience of technology, can only compromise, this produces the "privacy paradox". SISING to say, the researchers investigated and concluded that although the platform consumers are very concerned about the degree of privacy protection, most users ignore the privacy disclosure and continue to accept the information provided by Internet applications using privacy. Under the pressure of such data pressure and the innate advantages of the platform resources, the consent option in the "inform the consent rule" is probably mostly a mere formality.

It should be noted that the purpose of the privacy policy is to let individual users understand the various risks they need to take externally in the use of the software, and

then to consider whether to continue to use the service. However, the protection policy of enterprise personal information in reality always lacks direct prompt and notification. As an information processing party, how to collect information, as well as the collection method, purpose and means have always been concealed and obscure under the obscure professional terms. Accordingly, most of the current privacy policies on the market not only lack the functions they should play, but also become a burden for users. Accordingly, enterprises also use the professional technical barriers in their policies to transfer possible practical risks to the subject of personal information. To sum up, the notification obligation of information processors is flawed, not only because the privacy policy content is too obscure, but also has too hidden content hints and the intentional transfer of risk bearing by enterprises.

3.3 Applicable Exception to Improper Expansion of Informed Consent Rule

The original intention of the informed consent rules is to regulate the excessive collection and processing of personal information, which is a layer of protection shell for the information rights and interests of citizens with laws and regulations. However, in the face of multiple interests, it also needs to open the gate to balance the interests of various parties for stability. Although it is the original intention of personal information protection to protect the personal dignity and rights of information subjects, in addition to the protection of personal interests, the processing of personal information also involves the interests of other fields, such as public interests, national security, economic benefits, etc. Informed consent rules cannot be absolutized, and they need to unify the value of all parties and take comprehensive consideration. However, the exception expansion of informed consent rules should maintain a sense of boundaries and cannot be arbitrarily expanded. The inquiry of the exceptions to the informed consent rules can be integrated as the conflicts and contradictions between the interests of different legal principles. In conclusion, the problem of improper expansion of the informed consent exception is mainly reflected in the following two aspects:

Improper expansion is based on the risk control principle. From the perspective of risk prevention. In the field of public health, in order to prevent the improper spread of risks, based on the necessity of risk prevention and control, personal information is processed directly with without the approval of the subject of personal information, which reflects the risk prevention principle in the field of environmental law. This “risk prevention” is to build a series of risk regulation framework system to deal with those risks that are difficult to predict through past rules and experience. Therefore, the core focus of the risk prevention principle is: how to deal with the uncertainty of scientific knowledge, so as to strengthen the timeliness of the legal norms supporting the risk prevention principle. Especially in the outbreak scenario, with the continuous occurrence of similar events, whether risk prevention is only limited to the uncertain field of environmental science risk remains to be further discussed. In any case, with the continuous development of society, the principle of risk prevention has not been limited to the field of environmental protection, it has expanded to public health and national defense. In particular, it is worth mentioning that the EU countries have expanded the scope of application of the risk prevention principle in the process of legal practice, integrating deterministic hazards into the regulatory boundary of the principle, rather than limiting the scope to scientifically

uncertain risks. The expansion of the risk prevention principle will lead to the public health emergency, the temporary policy measures to weaken the self-determination of citizens' personal information will produce certain public power over private rights, lead to its separation from the constraints of laws and regulations to a certain extent, and infringe on the basic personality rights of natural persons.

The improper expansion is based on the public interest reservation doctrine of the applicable exception. The application of informed consent from the public interest follows Article 13, paragraph 1 of the Personal Information Protection Law, that is, personal consent is not required when processing public information or processing information for the purpose of implementing news reports. It is an embodiment of the principle of the public interest". That is, these two exceptions to the consent rule do guarantee the legitimacy of personal information in the public domain, and it is true that its legitimacy comes from the principle of public interest reservation. For example, in the course of the outbreak, the application of the exception to the informed consent rule has expanded rapidly based on the protection of citizens' right to personal health and the interests of the public society. In restaurants, stations, hospitals and other places where people gather, you can always see the gate-type health code inspection mouth, and its technical basis is to check the personal information data of the scanning personnel, including the communication number, itinerary and other personal information. In the face of such a huge accumulation of personal information data, whether the epidemic can be controlled is not within the scope of this paper, but it is difficult to describe whether the information processor properly handles the public's personal information, and whether the collection, analysis and disclosure comply with the regulatory scope of the Personal Information Protection Law. Admittedly, for the national public health security and the basic health of the surrounding people, it is the retention of public safety in the exception of the informed consent principle and the principle of risk prevention and control. However, in the process of epidemic prevention and control, there are some localities that improperly expand the principle of risk prevention, and introduced too strict and strong epidemic prevention policies and measures, which improperly reduced the basic personality rights and interests of citizens. The existence of the "health code" is based on epidemic prevention and public health. However, in the process of collecting personal information unrelated to the anti-epidemic measures, it is difficult to grasp whether the relevant units and third parties strictly abide by the relevant laws and regulations on personal information protection. The exception of informed consent has a good starting point. For the public interest and prevent the spread of uncertain or certain risks, sacrifice small local interests for the overall balance of interests, but the practice of improper expansion exception principle will only tear apart the registration of informed consent principle, and aggravate the abuse and infringement of irrelevant information. For example, all kinds of mall, station, restaurant, small program began to collect personal information, in the name of "epidemic prevention", ignoring the laws and regulations to collect personal information, and then sell to a third party to earn profit, which seriously violated the basic personal dignity of natural persons and information self-determination, is a serious infringement.

In general, when it is difficult to actually use academic means to evaluate and measure the specific certainty limits of risk prevention and control, and it is difficult to accurately

grasp the coverage of public interest, exceptions to the abuse of informed consent rules are common, which need to be strictly controlled. The main body of relevant departments should be in line with the implementation attitude of "cage power", carefully use power to prevent infringement. Nowadays, the epidemic prevention and control has entered the stage of normalization, and the extensive use of big data will inevitably produce a large amount of personal information disclosure. The improper expansion of the risk prevention principle and the principle of public interest reservation must be corrected immediately, so as to protect every citizen's basic personal dignity and right of self-determination.

4 Optimized Path for Implementation of Informed Consent Rules

There are indeed various problems in the application of informed consent rules. Some scholars point out that in order to get rid of the current predicament, China's personal information protection law should focus on strengthening the consumer law protection and public law protection to find a way out, that is, the private law "consumer legalization" according to the actual situation. However, this paper does not support the abandonment of the independent protection force of private law, let alone the idea of abandoning the rule and placing the protection of personal information after the event. To solve the problem of conflicts and flaws in the process of personal information protection, there must be front rules guide information processor face will collect information resources, can in accordance with the provisions of the law, in accordance with their own privacy policy, as the use of information resources for profits, to facilitate the life of science and technology feedback to the people. Therefore, we should adhere to the protection of personal information, with the informed consent rules as the core rules, to ensure the personal dignity of citizens and the freedom of information self-determination. In conclusion, this paper will explore the optimization path for the implementation of informed consent rules from the following three aspects.

4.1 Classified Protection of Personal Information According to Specific Scenarios

In the outline of the 14th Five-Year Plan, it is proposed to strengthen the establishment of data classification and classification protection system, so as to ensure the security of data and information privacy. Among them, the hierarchical protection of data refers to the scientific division of data resources according to data attributes, characteristics, quantity, quality, format, importance, sensitivity and other factors, and supporting corresponding security risk control measures, so as to release the value of data resources while protect data security and personal privacy. This will not only help to cope with the new situation and new challenges, but also grasp the new opportunities of digital development, so as to expand the new space for economic development, and further promote the healthy development of China's digital economy.

In combination with the views proposed by Professor Helenisenbaum in the article "Integrity in private presence", the process of processing personal information is classified and protected according to the "theory of situational integrity", believing that the applicable scenario of personal information is specific, and different cases should

be applied to different level standards. That is to say, in the face of different specific scenarios, the degree of risk borne by the personal information subject should be comprehensively judged to determine whether the processing behavior meets the regulations, and corresponding standards should be constructed, so that managers and processors can provide different degrees of personal information protection according to different standards [4]. In this regard, the starting point and foothold of "privacy protection" mentioned by Professor Nisenbaum in his later article should also be for the realization of "scene justice", that is, the interactive processing and circulation of personal information in specific situations [5].

Therefore, the protection of personal information in China should be combined with specific scenarios to classify the information protection. It should be not only differentiated based on the sensitivity and confidentiality of the information, but also based on the anonymity of the information subject, the specific information source address and the age of the subject. At the same time, combining with the theory of professor, can according to the personal information subject in the face of information processing information disclosure degree of specific risk, scenario, case, specific analysis may bear the degree of the risk and possible influence and threat force, the personal information refinement into different levels and categories, forcing information processing not wide and extensive collection of personal information, classified collection and processing can improve the efficiency of the processing information. Of course, this also requires the participation of state forces, formulate relevant information standards and corresponding levels, use regulatory and law enforcement forces to strengthen the compliance of enterprises and platforms at all levels, and implement a specific, corresponding and hierarchical information processing database. In this way, in the face of personal information protected by classification in specific scenarios, the dominant position of information processors and the means of transfer risks will be greatly limited, and the imbalance between personal information subjects and information processors will be alleviated to a certain extent. When a similar information processor excessive use or excessive disclosure of personal information, according to the level and category of regulatory supervision will appear easy and fair, also can be reversed transmission enterprises face such situation, because hierarchical had to give up the so-called "delete than save" concept, it must according to the standard and level in accordance with the provisions of the personal information, further safeguard the security of citizens' personal information.

4.2 Strengthen Supervision and Optimization Notification Tips

In view of the notification content, it is normal to understand, but why are there so many platform enterprises in the face of the legal provisions "clear, not ambiguous" at the same time, still choose to "bring private goods", not explicit? This requires both external forces and internal supervision. According to the "Personal Information Protection Law" Article 17 clearly stipulates that the personal information should inform the individual of the personal information processing purpose, processing method, the type of processing and the preservation period. Of course, this only stays at the level of declaration, and supervision should be further strengthened. Combined with the experience of the EU, such as the experience of GDPR, establish an independent data protection agency with the involvement of state organs, and implement national governance with prevention and

control as the main framework. This also fits the view of some scholars, that is, in the field of personal information protection, when the private law is relatively weak, we should strengthen the introduction of the public sector, start the strong external supervision mode, and prevent the bad phenomenon caused by the low self-discipline of enterprises.

In view of the difficulty of reading and the way of prompting, in addition to meeting the provisions of the Personal Information Protection Law that the data processor should disclose the personal information processing rules, the Identification Method of Illegal Collection and Use of Personal Information should also be stipulated in strict accordance with the presentation mode of the privacy policies of the information processing application platform of App. For example, if there is a "privacy policy collection rules difficult to access, such as into the App main interface, need more than four clicks to access", "privacy policy collection use rules is difficult to read, such as text too small too dense, color too light, fuzzy, or did not provide simplified Chinese version", can be identified as "not open collection use rules", which is in violation of regulations, should be subject to corresponding regulatory penalties. To sum up, in the face of the vigorous development of data under the new situation in China, the protection of personal information should be supported together with international experience and internal administrative forces, and the support of both sides can maintain personal information security and self-determination. At the same time, from the perspective of information security, the information processor itself should also establish the corresponding full range of chain guarantee measures, such as collection, analysis, storage, circulation, interaction, deletion and destruction, to effectively protect the security of citizens' personal information. If there is any danger of personal information leakage, it should inform and remedy it in time, establish an efficient and stable personal information disclosure plan disposal management system, and strictly check the personal information and privacy security of every person.

4.3 Exceptions to Precise Restriction Rules Applicable

Application to the expansion of the public interest retention principle based on the principle of risk prevention and control. We should strictly follow the identification of risks and hierarchical response, and not arbitrarily expand the scope of the application of informed consent rules whenever it is uncertain and difficult to deal with past historical experience. According to the public interest and the urgent needs of the risk prevention and control, the information processor can skip or bypass the rule restrictions to some extent when informing the consent rules. However, no matter how to explain and compare the importance of the legal interests of the two, it cannot be denied that this is the violation of the basic rights under the Constitution to a certain extent. Therefore, in the face of the exception application of informed consent rules, it is necessary to strengthen the control of the scope of application of informed consent rules, and accurately limit the application of exceptions. We can consider the specific identification and case processing in parallel ways, comprehensive evaluation and discussion, public participation and network collection when necessary, and effectively implement information protection in place to prevent the abuse of power. We should not judge future risks from the past perspective, nor should we ignore long-term development because of our immediate interests.

A thorough analysis of the legislative intention of the Personal Information Protection Law, its provisions are all personal information security as the priority, strengthening the protection of personal information security is the primary purpose, followed by the exception to the balance of public interest and risk prevention and control. Therefore, it is necessary to limit and balance the exception application of informed consent rules to a certain extent. Safety value is the top priority option, adhere to the application of informed consent rules within a reasonable range. If it is indeed necessary to apply the exception principle, it must conform to the legislative purpose of the exception to the informed consent rules, and conform to the constitutional laws, social order and good customs, and carefully apply them if the means are legitimate and necessary and to the least harm.

5 Conclusion

The importance of personal information security is self-evident. The infringement of personal information is not a simple "skin scratch" [6], which involves the basic rights and interests of the broad masses of the people, and can not be underestimated. In the face of such a rapid data speed and the increasing commercialization of personal information, the introduction of the personal information protection law is only the first step in a long journey. For the dilemma of informed consent rules under the perspective of personal information protection, there are asymmetric risk sharing, excessive advantage of information processors, defects of insufficient self-discipline or weak external supervision, and improper expansion of informed consent rules. All these need to further deepen the legal and regulatory system, chain docking, case analysis and treatment in order to effectively strengthen the protection of basic rights and interests of the people. Therefore, it is necessary to optimize the personal information, and optimize the notification method and prompt content, strengthen the domestic supervision; limit the exception of the safety value of personal information as the priority, take the principle of risk control and public interest within a reasonable scope, and safeguard and develop the legitimate rights and interests of the general people in cyberspace, so that citizens can enjoy more participation, security and happiness in the development of digital economy.

Acknowledgements. This work was supported by Fujian Province Science and Technology Innovation Strategic Research Project (No. 2024R0049).

References

1. Macenaite, M.,Kosta, E.: Consent for processing children's personal data in the EU: Following in US footsteps. Info. Comm. Technol. Law **26**, 146 (2017)
2. Daten als Gegenleistung - Verlangt die Digitalisierung nach einem neuen Vertragstypus. Specht Louisa. Juristen Zeitung (15–1) (2017)
3. Kokolakis, S.: Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. Computers & Security **64**, 122–123 (2017)
4. Nissenbaum, H.: Privacy as contextual integrity. Washington Law Review **79**, 127–128 (2004)

5. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press, p. 105 (2009)
6. Solove, D.J.: Privacy and Data Security Violations: What's the Harm? (2014). https://teachprivacy.com/privacy-data-security-violations-whats-harm/, [2022-03-06]