A Study on the Consent Rules in Personal Information Processing

Zhibin Hu
School of Law, China Jiliang University, Hangzhou, Zhejiang, China

Abstract: The Personal Information Protection Law (PIPL) adopts the "notice–consent" framework as its core architecture and establishes the information subject's right to self-determination as the value benchmark for personal information processing rules. In light of its institutional function, consent in personal information processing should be positioned as a composite structure that is grounded in quasi-juristic acts and supplemented by the rules governing declarations of will, so as to appropriately accommodate a space for the information subject's autonomous formation within the statutory protection framework. The determination of "contractual necessity" must be subject to the dual constraints of the purpose limitation principle and the principle of minimum necessity, and should be typologically guided by the distinction between core functions and value-added functions. Judicial practice should strictly examine such issues and provide reasonable grounds to prevent the concept of "contract necessity" from being distorted into a generalized channel, thereby weakening the principle of consent. According to the "independent consent" rule, the regulation of standard terms should be carried out from two dimensions: one is to control the control rights, and the other is to control the effectiveness; by cutting off the improper bundling of "consent" and "service", the independence of consent can be ensured; and the "voluntariness" requirement should be subject to substantive review, negating the validity of "compulsory consent" clauses.

Keywords: Personal Information; Consent Rules; Quasi-Juristic Act; Contractual Necessity; Separate Consent; Standard Terms

1. Introduction

In the digital age, the handling of personal information has permeated every aspect of social life. The unequal status between platforms and individuals, the reinforcement of algorithmic technology, and the difficulty in ensuring informed consent have made the consent rules a core issue in personal information protection. Article 13, Paragraph 1, Item 1 of the "Personal Information Protection Law" stipulates that "obtaining individual consent" is the general basis for the legality of personal information processing; Article 14 stipulates that consent must be based on sufficient information and be voluntary and explicit; Article 13, Paragraph 1, Item 2 stipulates that if the processing behavior is "necessary for the signing or performance of a contract by the individual", then the requirement for consent can be waived; Articles 23, 25, 26, 29, and 39 respectively stipulate the "separate consent" system in high-risk situations. Therefore, a rule system based on consent as the principle, with exceptions as the bottom line, and supplemented by separate consent has been formed.

However, the completeness of the norms has not eliminated the differences in actual implementation. Regarding the consent rules, there are at least three controversies: first, the legal nature of "consent" is whether it is an expression of will or a quasi-legal act; second, how to define the boundary of "contract necessity"; third, whether "independent consent" can effectively regulate "mandatory consent" under standard terms. These three issues correspond to three core propositions: "What is consent", "Under what circumstances can consent be waived", and "In what circumstances must strengthened consent be implemented". This paper takes Article 13, Article 14 of the "Personal Information Protection Law" and related independent consent provisions as the research object, analyzes theoretical differences, examines judicial practice positions, and clarifies the interpretation boundaries and normative connotations of the consent rules.

2. Disputes in the Legal Application of the Consent Rules

2.1 The Legal Attribute of Consent Is Ambiguously Defined

Copyright @ STEMM Institute Press

Consent is not only the cornerstone of the legality of personal information processing, but also the carrier that embodies the dignity of the information subject and their right to self-determination. However, relevant laws have not yet clearly defined its legal nature, resulting in ongoing disputes within the civil legal system regarding its relationship with "express consent" and legal behavior rules.

In the context of the constantly evolving digital technology, network service providers often tend to interpret "contract necessity" too broadly, including providing basic functions, optimizing services, and even maintaining the industry business model within the "necessity" scope, sometimes even using this as an excuse to forcibly collect sensitive personal information. Examples include mobile applications collecting address book information and platforms using algorithms to collect personal information, draw user profiles, and provide personalized recommendations. Only where a contract has already been concluded and is valid, where the processing is solely for the purpose of satisfying the information subject's interests, where the processing purpose is directly and closely related to the contract, and where the processing meets the requirement of having the least impact on personal rights and interests may this rule be invoked as a basis for processing.[1] How to clearly delineate the upper limit of the information subject's self-determination and the lower limit of the personal information processor is an urgent issue in the application of the consent rules.

2.2 The Opposition between "Separate Consent" and Standard Terms

"Separate consent" is a concept in the PIPL that is original from a comparative-law perspective. Article 14 provides that where laws or administrative regulations require separate consent or written consent, those provisions shall prevail. This article does not independently create an obligation; rather, it provides a superior-law basis for setting standards higher than ordinary consent in specific high-risk scenarios. Articles 23, 25, 26, 29, and 39 set separate consent requirements for scenarios such as providing information to third parties, public disclosure, image collection in public places, processing of sensitive personal information, and cross-border transfer. The purpose is to break the dilemma of "all consent" or "no consent" under "bundled consent" and to ensure that the information subject can independently understand matters with a significant impact on rights and interests and can fully consider them. China has not established separately detailed fair-use rules for special circumstances, and as a result, situations arise in which fair-use rules and separate consent rules overlap in application. From the perspective of interpretive theory, in principle, separate consent should take priority over fair-use rules.[2]

However, network service agreements are mostly presented in the form of standard terms. Faced with lengthy and obscure privacy policies, users often can only "agree" in order to obtain services or "disagree" and be denied access, so that "voluntariness" becomes a mere formality. A large number of data controllers still use "strategically vague language" in purpose-limitation clauses, and the current framework fails to meet the expectation of realizing a high degree of informational self-determination; the informed consent mechanism has thus suffered institutional failure in the context of standard terms.[3] The "take it or leave it" model of standard terms forms a structural opposition to the "item-by-item autonomous decision-making" idea of separate consent. The question that arises is whether the separate consent rule can effectively constrain "forced consent" in standard terms.

3. Analysis of the Legal Nature of "Consent"

Regarding the nature of consent, there are mainly two theoretical positions: the declaration-of-will theory and the quasi-juristic-act theory. The declaration-of-will theory holds that consent is an act by which the information subject intends to produce a certain legal effect, that is, authorizing the processor to process personal information through a declaration of will and forming a "quasi-contractual" relationship of information processing between the parties. If consent is defined as a juristic act, the processor's provision of documents such as a privacy policy may be regarded as an offer, and the individual's consent may be regarded as an acceptance, through which the parties establish a contractual relationship, whose effects and consequences should be governed by the contract part of the Civil Code. As for unilateral acts, the drafter of a privacy policy may only prescribe its own obligations and confer rights on individuals whose information is processed on the basis of consent; where a

 Copyright @ STEMM Institute Press

processor imposes obligations or liabilities on individuals through a unilateral act, such provisions are not binding on the individuals.

The theory of quasi-legal act holds that although consent contains information about the subjective will of the subject, its legal effect is directly determined by the legal provisions rather than by the intentions of the parties. If the data processing act does not take obtaining consent as a prerequisite for legality, the data controller cannot claim exemption merely because consent has been obtained. [4] In terms of the basis of legality, consent is mainly a post-event defensive measure rather than a private law authorization; data processing without consent does not automatically constitute an infringement, and the exemption effect of consent is limited because data processing based on consent still needs to meet the legal requirements of a legal act. When the information subject expresses consent, it merely "triggers" the established legal effect set by the law, which distinguishes consent from legal acts that generate legal effect through a declaration of will. The core of the controversy between the two theories lies in the understanding of the effect of consent: the will declaration theory emphasizes "formation", advocating that consent establishes a legal relationship between the information subject and the data controller; while the quasi-legal act theory tends to view consent as a "protective tool", whose effect is determined by the law, but must be initiated through consent to prevent the risk of processing personal information without consent. Some viewpoints hold that consent is usually a quasi-legal act, but in special cases such as in payment associations, it may have the nature of a will declaration, thus forming a dual structure of data transactions. Whether consent within the category of quasi-juristic acts can apply by analogy the relevant regulatory rules governing juristic acts requires targeted analysis in light of the specific configuration of interests.[5]

4. The Boundary of "Contractual Necessity"

Article 13, Paragraph 1, Item 2 of the Personal Information Protection Law stipulates that if the data processing action is "necessary for the signing or performance of a contract in which the individual is involved", the data processor does not need to obtain separate consent. This situation constitutes a legal exception and exempts the need for obtaining consent. In practice, data processors often interpret this clause expansively, including value-added services within the scope of application, which may weaken the effectiveness of the consent rule; therefore, it is necessary to clearly define its connotation and boundaries at the regulatory level.

4.1 The Normative Connotation of "Contractual Necessity"

Under the framework of "contract necessity", the processing of personal information can be essentially classified as a quasi-legal act, which consists of two levels: the subjective level and the objective level. At the subjective level, the true will of the information subject constitutes the first layer of content, while the expression behavior belongs to the second layer; together, they form the subjective structure. At the objective level, principles such as fairness, public order and morality, and necessity occupy a dominant position, constituting the first layer of normative basis; while the three elements of necessary facts, necessary interests, and necessary values belong to the second layer, providing a more specific analytical framework for determining whether a specific processing behavior is "necessary". [6] The "contract necessity" rule and the "notification consent" rule are the two main bases for enterprises to handle personal information in compliance. Since the former does not require obtaining individual consent, enterprises often prefer to adopt this rule in practice. [7] Court precedents and academic theories have formed a method of distinguishing core functions from added value functions. Any product or service can be decomposed into multiple functional modules: the core function is the necessary function that meets the basic needs of users, while the added value function is the additional extended service function based on the core function. If the processing of personal information is only related to the realization of added value functions, then the "contract necessity" principle cannot be applied. This distinction provides a standard for judging "contract necessity", but its boundaries may be dynamically adjusted with technological development and changes in user cognition. When it is impossible to clearly distinguish the core function from the added value function, the principle of "protect the information subject if in doubt" should be adopted, and the "contract necessity" rule should not be applied.

Copyright @ STEMM Institute Press

4.2 Judicial Practice on the Determination of "Contractual Necessity"

4.2.1 Affirmative Scenario: Information Processing within a Reasonable Limit

Guiding Case No. 266 confirms from the positive side a reasonable standard for determining "contractual necessity." In that case, the plaintiff activated the "use first, pay later" function of an electronic bus ride code and later discovered that a credit account had been opened and related personal information collected. The plaintiff sued on the grounds of misleading, coerced, and non-necessary activation of credit services. The court held that the collection of the personal information at issue was "contractually necessary" and could be carried out without separate consent; however, the company concerned still collected the information by obtaining the user's prior consent, reminded users in a prominent position in the agreement to read it, and used conspicuous markings for the personal information processing clauses, thereby fulfilling its statutory notice obligation, and there was no misleading. The credit service conducted a creditworthiness assessment of the user in advance and provided the bus company only with conclusive information on "whether to grant access," without providing raw credit data or detailed scores; this was necessary to realize the "use first, pay later" function and satisfied the principle of minimum necessity. Three requirements for an affirmative determination can thus be distilled: the information processed must strictly correspond to the principal obligation under the contract, and without such information the main purpose of the contract could not objectively be achieved; the processor must fulfill its notice obligation in a conspicuous manner; and the processing method must comply with the principle of minimum necessity in terms of information type, precision, and manner of provision.

4.2.2 Negative Scenario: Forced Collection of Non-necessary Information

Compared with the restraint shown in affirmative scenarios, judicial practice is more active in denying "contractual necessity," which indirectly reflects the courts' restriction on information processors' forced collection under the pretext of "contractual necessity."

Guiding Case No. 265 provides rules for a negative determination. An English-learning website operated by a technology company forcibly required users to fill in user profile information such as "occupation," "learning purpose," "school age stage," and "English proficiency," and the interface had no "skip" or "refuse" option; users could not complete login without filling in the information. The court held that the technology company's claim that automated push was a basic function lacked support from industry standards, and it delineated the boundary of "necessity" by distinguishing core functions from value-added functions: automated push was merely a value-added function rather than a core service, and the direct collection of user profile information did not constitute a statutory circumstance in which processing could be carried out without obtaining individual consent. Three rules for a negative determination can thus be distilled: the argument for "contractual necessity" must be conducted by taking functional modules rather than the product or service as a whole as the unit of analysis, and value-added functions cannot replace the necessity assessment of core functions; the determination of "necessity" adopts a strict standard, and convenience, commercial benefits, industry practices, and the like are not valid justifications; and where no alternative service method is provided for users who refuse non-necessary information processing, this constitutes forced consent, and such consent does not take legal effect due to lack of voluntariness.

5. Restrictions Imposed by the "Separate Consent" Rule on Standard Terms

5.1 General Application of "Separate Consent"

In order to strike a balance between personal information protection and reasonable use, Chinese legislation has drawn on the "fair use" framework from the "Copyright Law", providing legal basis for handling personal information without obtaining the individual's consent, and granting information processors the freedom to make independent decisions under certain circumstances. Unlike the EU's "General Data Protection Regulation" (GDPR), which divides fair use into general and special cases and provides differentiated rules, China has not made separate detailed provisions for the subdivided fair use scenarios. This may lead to conflicts or overlaps between the fair use rules and the separate consent rules in actual personal information processing. [8] "Separate consent"

 Copyright @ STEMM Institute Press

means that when handling specific personal information processing activities, the processor must notify in an independent and obvious manner and obtain separate consent for that specific matter; this consent cannot be bundled with the consent for other matters or obtained through tacit means.

From the perspective of system positioning, "separate consent" is an upgrade and improvement of ordinary consent. Ordinary consent does not require strict legal form, written, oral or electronic records are acceptable, and the content does not need to be obtained item by item. However, in cases where rights and interests are relatively important, such as when processing sensitive personal information, the legislative body will raise the procedural threshold for the legality basis through separate consent to correct the structural disadvantages faced by information subjects under "bundled consent" and ensure that "voluntariness and clarity" are truly implemented. The notice obligation for sensitive personal information processing has special requirements: the processor should clearly explain that there is an inseparable and necessary connection between the processing of such information and the specific service or function, and should take the personal information protection impact assessment results as a core reference; the consent stage should be separated from the ordinary personal information consent process, and bundled consent should be prohibited. With respect to the consent rule, in order to meet the statutory standard of separate consent, the authorization and consent stage for sensitive personal information and the consent acquisition process for ordinary personal information should be separated from each other, and it is absolutely prohibited to complete the relevant authorization operations uniformly by means of bundled consent. [9]

5.2 Reverse Regulation of "Forced Consent" by Separate Consent

5.2.1 Incorporation Control of "Forced Consent" Clauses

In the context of network services, standardized privacy policies and terms of use are "pre-formulated declarations of data subject consent."[10] The phenomenon of "forced consent" in standard terms manifests as information processors forcing information subjects to make an either-or choice between obtaining services and protecting personal information by means of "no consent, no service," thereby reducing the "voluntariness" requirement of consent to nothing. The basis for controlling standard terms is established on the inequality of bargaining power and the bias toward protecting the weaker party; it aims to prevent the party with superior contractual power from abusing its rights to create "unfair contracts" and to achieve substantive fairness.[11] Article 16 of the PIPL explicitly provides that a personal information processor may not refuse to provide products or services to a natural person on the ground that the natural person refuses to have their personal information processed or withdraws consent, unless the processing of such personal information is necessary for the provision of products or services.

Incorporation control of "forced consent" clauses means activating the independence requirement of separate consent to intercept such clauses at the level of the consensual basis. If a processor bundles non-necessary processing matters with other service terms and makes refusal of the overall terms a condition for refusing service, the standard terms should not be deemed incorporated into the contract because they violate the prohibitive provision of Article 16. From the perspective of incorporation control theory, such clauses do not give the information subject a reasonable period for review in order to treat various processing matters differently, and through bundling they cause the information subject’s consent to non-necessary matters to lose substantive freedom of choice, constituting unreasonable unilateral coercion and therefore cannot become part of the contract. Where a platform fails to perform its duty of prompting and explanation, such clauses may not be deemed part of the contract; where standard terms are obviously unfair, the information subject has the right to request the court to revoke them. At the same time, it is necessary to use the "reasonable person" as a reference standard and construct a system of interpretive obligations for network platforms, so as to safeguard the information subject’s lawful rights and interests in personal information while promoting the stable and compliant operation of network platforms. [12]

5.2.2 Validity Control of "Forced Consent" Clauses

Even if the "compulsory consent" clause has been formally incorporated into the control framework - for instance, when the information processor obtains the user's formal consent through pop-up

Copyright @ STEMM Institute Press

windows or an independent consent form - this clause still needs to undergo strict scrutiny at the level of substantive validity. Usually, the degree of contract formation is used as a normative standard to measure the spirit of "free will" and "balance of performance" in civil law. [13] The core of substantive validity lies in examining whether the consent made by the information subject truly possesses the essence of "voluntariness".

Article 14 of the Personal Information Protection Law stipulates that "voluntariness" is the core legal prerequisite for consent; the national standards further require that the information subject should independently and clearly make the consent after fully understanding the relevant circumstances, and prohibit the use of coercion, fraud or misleading behavior. In the case of "compulsory consent", the information subject has two obvious choices: "agree" and "refuse". However, refusal will result in losing the important reliance on the product or service, and their choice has actually been "locked" by economic or social pressure. When there is a severe imbalance between the two parties, the "either agree or withdraw" model has exceeded the scope of normal commercial negotiations and has evolved into implicit coercion; the authenticity of the "voluntariness" of this consent is questionable, and its validity should be regarded as having defects.

6. Conclusion

The consent rules in personal information processing constitute the first line of defense for protecting the information autonomy of information subjects in the digital age. This article starts from the "essence" and explores the legal nature of consent, the boundaries of "contract necessity", the application of individual consent and its relationship with standard terms, and further analyzes "how to enhance its effectiveness", in order to reveal the coordination mechanism between the differences in interpretation and application of consent rules.

Regarding the legal nature of consent, simply classifying it as "intentional expression" or "quasi-lawful act" cannot fully meet the actual needs. This article advocates adopting the "quasi-lawful act principle, combined with the limited application of the rules of intentional expression", striving to achieve a dynamic balance between the rigidity of legal benchmarks and the flexibility of case adjustments.

Regarding the controversy over the boundary of "contract necessity", it is essentially a dispute over the interpretation of the concept of "necessity". This article combines the purpose limitation principle and the minimum necessity principle, and adds a typological distinction between core functions and additional value functions, constructing an operational argument framework applicable to "necessity".

Initially, the personal consent rules were designed to address the problems caused by "bundled consent" under standard terms. However, when online services again embed individual consent into the binary choice of "accept or withdraw" through mechanisms such as "prohibition of providing services without consent", formal notification may also become formalism. In this context, the provisions of Article 16 of the Personal Information Protection Law - "Products or services shall not be refused because of refusal or withdrawal of consent" - not only set up procedural obstacles for incorporating control rights, but also fundamentally indicate that the right of the subject to obtain core services should not be premised on giving up non-essential information rights and interests.

Ultimately, the maturity of the legal rule system in the field of personal information protection does not depend on the quantity or refinement of the rules, but on whether these rules can rebuild the truly dialogic interaction relationship between information subjects and data processors - this relationship should not be the command-style model of "either agree or accept", but should be achieved through continuous dialogue, allowing people to hesitate, refuse and reconsider.

Acknowledgments

The successful completion of this thesis is inseparable from the guidance, support and companionship of many people. Here, I would like to express my most sincere gratitude.

I am grateful to all the teachers in the Law School for their teachings and assistance in professional courses and academic training, which have enabled this thesis to be further improved.

During the process of writing the thesis, I also received encouragement and support from many classmates and friends. Thank you to all your friends for helping with data collection, discussion of viewpoints, and companionship during daily life. It was your care and encouragement that enabled me to keep moving forward even when facing difficulties.

 Copyright @ STEMM Institute Press

I am grateful to my family. You have always been my most solid support. I am grateful to my parents for their years of silent dedication and unconditional support. Your understanding and tolerance have given me the courage and strength to pursue my studies.

References

[1] Yang Xu. The Restrictive Application of the Rule of Necessity for Contract Performance in Personal Information Processing. Law Science, 2023, (06):85–98.

[2] Li Aijun, Sun Yandong. On Personal Information Processing Not Based on Individual Consent and the Systematic Interpretation of the Separate Consent Rule. Journal of Northwestern Polytechnical University (Social Sciences), 2023, (03):112–127.

[3] Green D. Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation. International Journal for the Semiotics of Law – Revue internationale de Sémiotique juridique, 2024, 38(2):1–29.

[4] Zou Yang. The Legal Effects of Consent Rules in the Personal Information Protection Law. Police Science Research, 2022, (02):5–21.

[5] Lin Hengmin. On the Private Law Nature and Normative Application of Consent by Personal Information Subjects: Also on the Non-Uniformity of Consent under the Civil Code. Comparative Law Research, 2023, (03):142–154.

[6] Sun Zhiyu, Li Yan. On the Dual Structure and Element Determination of "Necessary for Contract" in Personal Information Processing. Social Sciences in Guangdong, 2024, (02):239–250.

[7] Guo Peng, Li Zhanpeng. On the Expansive Application of the Rule of Contractual Necessity in Personal Information Processing. Electronics Intellectual Property, 2024, (06):4–14.

[8] Li Aijun, Sun Yandong. On Personal Information Processing Not Based on Individual Consent and the Systematic Interpretation of the Separate Consent Rule. Journal of Northwestern Polytechnical University (Social Sciences), 2023, (03):112–127.

[9] Han Xuzhi. Notice and Consent in the Processing of Sensitive Personal Information. Local Legislation Research, 2022, 7(03):67–82.

[10] Damian C, Inge G, Peggy V. Pre-formulated Declarations of Data Subject Consent—Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections. German Law Journal, 2019, 20(05):679–721.

[11] Han Shiyuan. Regulation of Unfair Contract Terms in Chinese Law. Law and Economics, 2017, (04):17–32.

[12] Yang Xianbin. Validity Determination of Standard Terms for Personal Information Processing by Network Platforms. Political Science and Law, 2021, (04):14–25.

[13] Xie Gen. The Normative System for Content Regulation of Standard Terms. Chinese Journal of Law, 2013, 35(02):102–118.

Copyright @ STEMM Institute Press