Ethical Issues in the Trading of Personal Data

Authors: Huang Peng, Huang Peng

Date: 2024-02-17T00:00:00+00:00

Abstract

The "Twenty Data Measures" highlights the right to use data, downplaying the concept of data ownership. In the process of data transactions, how to balance the personal interests and property interests of personal information becomes an issue that requires consideration. This paper employs the term "personal data" to replace "personal information," thereby highlighting its property attributes. Personal information rights and interests, as a type of personality right, contain ethical considerations such as human dignity, privacy, risk prevention, and interest balancing, and can be categorized into sensitive personal data and non-sensitive personal data. Non-sensitive personal data can be traded, with reasons including: controllable risks that do not easily compromise human dignity, and increased overall social welfare. Sensitive personal data is subject to the principle of prohibiting transactions, with transactions being the exception.

Full Text

The Ethics of Trading Personal Data

(School of Philosophy, Fudan University, Shanghai 200433)

Abstract

The "Data Twenty Articles" emphasize data usage rights while downplaying the concept of data ownership. In the process of data trading, balancing the personality interests and property interests of personal information becomes a critical consideration. This paper employs the term "personal data" instead of "personal information" to highlight its property attributes. Personal information rights, as a personality right, embody ethical considerations including human dignity, privacy, risk prevention, and interest balancing, and can be categorized into sensitive personal data and non-sensitive personal data. Non-sensitive personal data can be traded, primarily because the risks are controllable and unlikely to harm human dignity, and because such trading increases overall social welfare.

Sensitive personal data should be prohibited from trading as a principle, with exceptions allowed.

Keywords: personal information rights; personal data; tradability of personal data; ethics of personal data

In December 2022, the Central Committee of the Communist Party of China and the State Council issued the "Opinions on Building a Basic Data System to Better Leverage the Role of Data as a Factor" (hereinafter referred to as the "Data Twenty Articles"). These articles propose establishing a property rights operational mechanism that separates data resource holding rights, data processing and usage rights, and data product management rights. It is widely believed that this tripartite division downplays the concept of "data ownership" and emphasizes data utilization and circulation. Under this property rights mechanism for data circulation, when personal information is traded as data, will it undermine the ethical values that personal information rights aim to protect? Must such transactions themselves adhere to certain ethical norms? How can we achieve a balance between data circulation and the protection of personality interests?

The Civil Code, implemented in 2021, established a new personality right: personal information rights. Personal information refers to various information recorded electronically or otherwise that can identify a specific natural person either alone or in combination with other information. Notably, while general personality rights in the Civil Code are often expressed as "right to life," "right to health," "right to name," or "right of portrait" using the "right of X" formulation, the Code uses "personal information protection" instead, and the subsequent Personal Information Protection Law employs "personal information rights." This wording reflects legislators' concerns that absolute individual control over personal information would hinder data circulation, leading them to adopt a prudent strategy that deliberately downplays the personality attributes in language while highlighting property attributes. In this paper, the concept of "personal data" is equivalent to "personal information" —the concept of "personal data" in the EU's General Data Protection Regulation is essentially consistent with the "personal information" concept in China's Civil Code. Personal information rights encompass both personality interests and property interests, but using the term "data" better emphasizes the property aspect.

Regarding the distinction between information and data, Shannon, the father of information theory, stated in his 1948 paper "A Mathematical Theory of Communication" that "information" broadly refers to anything that can reduce uncertainty; data that eliminates redundancy can become information. In knowledge management, scholars have proposed the DIKW (Data, Information, Knowledge, Wisdom) pyramid system, which divides understanding into four hierarchical levels: data, information, knowledge, and wisdom. Russell Ackoff wrote in his 1989 work *From Data To Wisdom*: "An ounce of information is worth a pound of data, an ounce of knowledge is worth a pound of information, and an ounce of understanding is worth a pound of knowledge." Data differs from

information, knowledge, and wisdom primarily in that it is raw, fragmented, isolated, and unprocessed records that cannot answer specific questions. Compared to "information," "data" is raw material lacking meaning and value, making it more suitable for describing purely objective property. From a legal perspective, Article 127 of the Civil Code states: "Where the law provides for the protection of data and virtual property on networks, such provisions shall apply." Article 3, Paragraph 1 of the Data Security Law stipulates: "The term 'data' as used in this Law refers to any record of information in electronic or other forms." The "data" in these provisions contains no personality attributes.

[Figure 1: see original paper] DIKW System

Of course, when using the term "personal data," we are not defining "data" in this strict sense, but merely to emphasize its property attributes. On July 6, 2021, Shenzhen introduced China's first regional comprehensive legislation in the data field—the "Shenzhen Special Economic Zone Data Regulations"—which also replaced "personal information" with "personal data." In this paper's discussion, "personal information" is used only when specifically addressing personality interests; "personal data" is used in all other contexts. According to the Personal Information Protection Law, personal data refers to various data related to an identified or identifiable natural person. Personal data includes four elements: (1) natural persons, including personal data of deceased persons and fetuses under certain conditions; (2) identified or identifiable natural persons, meaning those already identified or who can be identified by combining data with other information; (3) relevant data; and (4) anonymized data does not constitute personal data—anonymization refers to the process of processing personal information so that it cannot identify a specific natural person and cannot be restored.

2.2 Sensitive Personal Data

Personal data can be classified according to different criteria, such as direct versus indirect personal data based on whether they directly identify a natural person; communication data, financial data, medical data, educational data, belief data, genetic data based on usage; biometric, religious belief, specific identity, medical health, financial account, and location trajectory data based on life relevance; and individually strong versus individually weak personal data based on the degree of individual specificity. Since this paper addresses the ethical issues related to personal data trading, the classification criterion should be the strength of involvement of personality interests; the solution should also coordinate with existing legal systems as much as possible. The Personal Information Protection Law first introduced the legal concept of "sensitive personal information," defined as "personal information that, once leaked or illegally used, is likely to infringe upon the personal dignity of a natural person or endanger their personal or property safety."Based on whether information is sensitive, personal data can be divided into sensitive personal data and general personal data. According to Article 28 of the Personal Information Protection Law, sensitive

personal data includes but is not limited to: biometric, religious belief, specific identity, medical health, financial account, location trajectory information, and personal information of minors under fourteen years of age.

2.3 Ethical Considerations of Personal Information

Ethics considers how people become human, how to handle relationships between people, society, and nature, and discusses propositions of "goodness," "justice," and "fairness." Personal information is closely related to individuals; improper use can cause negative impacts, while proper use can expand human freedom and facilitate human development. In the process of establishing personal information as a personality right, several important ethical considerations emerge, such as "human dignity," "privacy," "risk prevention," and "interest balancing." These considerations are not entirely independent—for example, "human dignity" serves as the foundation for other considerations. Each concept has a complex and sometimes unclear history and connotation. However, from an applied ethics standpoint, mainstream ethical concepts that have achieved consensus can serve as the basis for judgment, and these four groups of concepts constitute the primary ethical considerations in mainstream personal information policies.

2.3.1 Human Dignity A runaway train is heading toward five people, and you are on a footbridge where you could push a fat man onto the tracks to derail the train and save the five lives. Five patients each need an organ transplant or they will die; can a surgeon take organs from a healthy person to save the five? These are two versions of the "trolley problem." Kant argued that all people possess intrinsic value or dignity because of their rational autonomy; therefore, people should be treated as ends rather than means. Post-WWII reflections on the war led to personal dignity becoming an important ethical foundation for law, as in Article 1 of the 1948 Universal Declaration of Human Rights: "All human beings are born free and equal in dignity and rights." Article 38 of China' s Constitution states: "The personal dignity of citizens of the People' s Republic of China is inviolable." In both Europe and China, legal systems of general personality rights have been developed based on human dignity, initially protecting personal information through privacy rights systems.

In 1982, the German federal government promulgated the Census Act, planning to comprehensively collect citizens' personal information, including personal, occupational, and residential data. Some considered this unconstitutional and filed a lawsuit demanding the law be declared unconstitutional. After review, the German Federal Constitutional Court established the concept of "informational self-determination" through case law. This case marked the beginning of establishing personal information personality rights in Europe. Through subsequent legislative developments in Europe, the right to personal information gradually became an independent personality right. Both the EU' s General Data Protection Regulation and China' s Personal Information Protection Law

take human dignity as an important legislative value and create personal information rights separate from privacy rights.

2.3.2 Privacy In the late 19th century, American scholar Samuel Warren, concerned about his wife' s private life being frequently reported by the media, collaborated with lawyer Louis Brandeis to publish "The Right to Privacy" in the *Harvard Law Review*, first proposing the concept of privacy as "the right to be let alone." Article 12 of the 1948 Universal Declaration of Human Rights, Article 8 of the 1950 European Convention on Human Rights, and Article 17 of the 1966 International Covenant on Civil and Political Rights all establish privacy rights. Unlike civil law countries, the U.S. privacy law system is complex, forming a "big privacy" legal concept through case law that approximates the scope of general personality rights in China; personal information is protected as "information privacy."

In China, "privacy" is one type of personality right. The Civil Code, in Part Four "Personality Rights," Chapter Six, provides "privacy rights and personal information protection" in parallel, demonstrating the close connection between the two personality rights. The Civil Code defines privacy as a natural person' s private life tranquility and private spaces, activities, and information that they do not wish others to know; private information can fall within the scope of personal information. Nevertheless, due to strong American influence, expanded use of the legal concept of "privacy" is common outside legal documents, such as so-called "privacy agreements" that actually refer to personal information protection agreements. Even without considering the popularity of the broad privacy concept, "privacy" as a negative liberty right gives it independent ethical consideration value in China' s personal information policies.

2.3.3 Risk Prevention Ulrich Beck proposed that modern society is a risk society; this uncertain, increasingly globalized risk creates societal demands for security. The "precautionary principle" was first proposed in 1970s German environmental law and, through Germany' s introduction, gradually entered international environmental law. Its core idea is "scientific uncertainty should not be a reason for inaction or delayed action" —when in doubt, safety is better than regret. Facing similar dilemmas, the precautionary principle is increasingly applied in technology governance. Misuse of personal information can lead to fraud, cyber violence, privacy leaks, discrimination, threats to personal safety, theft, capitalist surveillance, power control, and human objectification. The EU' s General Data Protection Regulation mentions the concept of risk multiple times and is considered to adopt a "risk-based approach." Article 11 of China' s Personal Information Protection Law states: "The state shall establish and improve the personal information protection system, prevent and punish acts infringing upon personal information rights···" which scholars consider an embodiment of the precautionary principle. The Personal Information Protection Law establishes a set of institutional measures for risk prevention, such as internal controls, personal information protection officers, compliance audits,

and personal information protection impact assessments.

2.3.4 Interest Balancing Jhering believed that the purpose of law is to pursue social interests; "father of interest jurisprudence" Heck believed that "law is the resultant force of material, national, religious, and ethical interests that coexist in various legal communities and compete for recognition." This aligns with the claims of normative ethics. If data is called the new oil, then personal data can be said to be crude oil. Society' s demand for data circulation is at least as strong as the need to protect personal personality. The rapid development of big data, artificial intelligence, and other emerging technologies has driven data to become a new production factor. The issuance of the Data Twenty Articles has further stimulated enthusiasm in the data trading market. According to the Shanghai Data Exchange' s "2023 China Data Trading Market Research and Analysis Report," China' s data trading market size grew from 61.76 billion yuan in 2021 to 87.68 billion yuan in 2022, an annual growth rate of approximately 42.0%, with a projected compound annual growth rate of about 20.3% for 2025-2023.

Meanwhile, data security issues have become increasingly severe. Facebook' s leak of over 50 million users' information data was used by Cambridge Analytica to push campaign advertisements; Didi was fined 8.026 billion yuan for data processing activities that seriously affected national security; Chinese citizens' personal information was leaked and sold overseas; China' s Judgments Online platform significantly reduced the scale of published documents partly due to data security concerns. The concept of balancing personality interests, data circulation interests, and data security interests is reflected in law. Article 1, Paragraph 1 of the EU' s General Data Protection Regulation states: "This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data." Article 1 of China' s Data Security Law states: "This Law is formulated to regulate data processing activities, ensure data security, promote data development and utilization, protect the legitimate rights and interests of individuals and organizations, and safeguard national sovereignty, security, and development interests." Article 1 of the Personal Information Protection Law states: "This Law is formulated to protect personal information rights, regulate personal information processing activities, and promote the rational use of personal information, in accordance with the Constitution."

3. The Tradability of Personal Data

The concept of personality rights was created to defend human dignity; therefore, personality rights cannot be waived, transferred, or inherited. At the same time, personality rights contain property attributes, as exemplified by personality elements such as portrait, voice, and name, which have been widely commercialized through authorization. Other elements, such as human organs, cells, tissues, body, health, and reputation, are prohibited from commercializa-

tion. The Civil Code establishes two principles for coordinating the spiritual and economic interests of personality rights: (1) spiritual interests are core; and (2) spiritual interests take precedence over economic interests. Regarding personal data, current arguments for its tradability mainly include: no legal prohibition, informational self-determination, and economic value. However, these arguments do not fundamentally address why some personality right elements are prohibited from trading while others are permitted.

This paper argues that, first, non-sensitive personal data can be traded. The main reasons are:

First, risks are controllable and unlikely to harm human dignity. Taking internet users' historical click behavior, viewing duration, browsing history, and follow status as examples, to use this data for personalized recommendation functions in applications like Douyin, the platform must obtain individual informed consent; disclose personal information processing rules, specifying the purposes, methods, and scope of processing; ensure the quality of personal information; store personal information for the shortest time necessary to achieve the processing purpose; take necessary measures to ensure the security of processed personal information, such as designating a personal information protection officer, conducting regular compliance audits, conducting pre-emptive personal information protection impact assessments, and filing algorithms; accept supervision from cyberspace authorities and bear legal responsibility for violations. Individuals have the right to withdraw consent, as well as rights to know, decide, access, copy, transfer, request correction or supplementation, deletion, and demand explanation regarding data processing. These rights, obligations, and regulatory measures can reduce potential social harm.

Second, trading increases overall social welfare. Through the utilization of personal data, we enjoy better internet products, such as Douyin short videos, NetEase Cloud Music, and Toutiao. Personal credit needs that traditional financial systems cannot easily meet are also more widely satisfied through credit evaluation based on personal data like consumption, repayment, and overdue records. Through precision marketing, individuals can receive personalized product recommendations. Smart products trigger corresponding functions based on our status: health reminders, do-not-disturb modes, exercise statistics, and sleep analysis. Public figures and experts can also obtain more commercial returns through personal data trading. Action actors can digitize their martial arts movements, celebrities can digitize their voice and image characteristics, and artists can digitize their artistic styles, all creating substantial value. This contractual arrangement, where individuals transfer some of their personal information rights for the benefit of all—albeit to varying degrees—aligns with Rawls' s concept of justice as fairness.

Second, for sensitive personal data, prohibition should be the principle, with permission as the exception. The main reasons are:

First, risks outweigh benefits. (1) As defined, once sensitive personal data is

leaked or illegally used, it is likely to infringe upon personal dignity or endanger personal or property safety. The illegal trading of sensitive personal data was until recently a massive underground industry with an annual "output value" approaching 100 billion yuan and remains a governance challenge. Fully liberalizing sensitive personal data commercialization would enable criminals to find ways (through inducement of consent, control of commercial entities, etc.) to "legally" obtain data for illegal purposes. Even though civil, administrative, and criminal law can strictly regulate data processing activities, once damage occurs, it is irreversible. The characteristic of data's infinite replicability also exposes the public to uncertain and significant risks—safety is better than regret. (2) Non-trading uses already meet public interest needs. Sensitive personal data can be used without consent when: necessary for concluding or performing a contract where the individual is a party, or for implementing human resource management according to legally formulated labor rules and collective contracts; necessary for fulfilling statutory duties or obligations; necessary for responding to public health emergencies or protecting natural persons' life, health, and property safety in emergencies; necessary for news reporting, public opinion supervision, and other acts in the public interest within reasonable scope; processing personal information that individuals have voluntarily disclosed or that has been legally disclosed within reasonable scope; and other circumstances stipulated by laws and administrative regulations. (3) Technological development has made it possible for "raw data not to leave the domain, data to be usable but not visible." Privacy computing is "a category of information technology that enables data analysis and computation while protecting data from external leakage, representing an integration of data science, cryptography, artificial intelligence, and other technical systems," mainly including secure multi-party computation, homomorphic encryption, federated learning, and other technical solutions. Privacy computing technology is gradually maturing and has become a hot topic in the market, with many application scenarios already emerging; it is projected that by 2025, China's privacy computing industry basic product and service market will reach 9.59 billion yuan. If privacy computing technology continues to develop to enable complete anonymization, it can achieve similar utilization effects without trading sensitive personal data, significantly reducing the necessity of directly trading such data.

Second, considerations for allowing exceptions. Current law adopts a definition-plus-typological-listing approach for sensitive personal data. Facial information, for example, is considered sensitive personal data. However, critics argue that data "sensitivity" depends on context—facial information used for phone unlocking and payment has low "sensitivity," while its use for identity registration and purchase intention analysis in shopping malls has high "sensitivity." Helen Nissenbaum proposed the "Contextual Integrity" theoretical framework, using reasonable information norms in different contexts as the standard for judging the legitimacy of personal data circulation. This theory has certain rationality and has been applied. In August 2023, the Cyberspace Administration of China's "Regulations on the Security Management of Facial Recognition Technology

Application (Trial) (Draft for Comments)"sets different regulatory requirements for facial recognition based on different usage scenarios. The Shanghai Data Exchange has also explicitly proposed the "no scenario, no transaction" principle for data trading. However, as a legal policy, the "contextual integrity" theory is too principled, and assessing legitimacy on a case-by-case basis would be impractical.

Therefore, when adopting the "sensitive personal data" criterion for tradability, we must also recognize that some legally listed sensitive personal data may not be so "sensitive" in certain contexts, making absolute prohibition unnecessary.

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