Privacy Computing and User Data Protection Strategies in Social E-Commerce

Yumeng Jin[1, *], Han Yang[2], Jiayi Zhang[3], Xiaotong Wang[4], Jiayi Gao[5]

[1]Nanjing University of Information Science and Technology, Nanjing, China

[2]SouthWest Petroleum University, Chengdu, China

[3]Hunan University, Changsha, China

[4]Jiangxi University of Science and Technology, Ganzhou, China

[5]Dalian Minzu University, Dalian, China

*Corresponding author: 1372626528@qq.com

Abstract. This paper examines privacy computing technologies—including federated learning, secure multi-party computation (SMPC), and differential privacy—as solutions to balance data utility and privacy protection in social e-commerce. It highlights technical strategies such as decentralized modeling, noise-enhanced anonymization, and edge-based data processing to mitigate risks like centralized data breaches and cross-border compliance conflicts. Aligning with regulations such as China's Personal Information Protection Law (PIPL) and the EU's GDPR, the study proposes a tripartite framework integrating cryptographic techniques, dynamic user consent mechanisms, and regulatory adaptability. Empirical evidence demonstrates reduced privacy violations while maintaining operational efficiency, underscoring the necessity of verifiable privacy-preserving methods for sustainable social e-commerce development.

Keywords: Privacy computing; Social e-commerce; Data protection; Federated learning; Differential privacy; Compliance; GDPR; PIPL.

1. introductory

Based on traditional e-commerce, mobile social e-commerce has been developing vigorously in recent years. In the context of mobile social e-commerce, as the main body of information generation and dissemination, the importance of users' personal information in the operation of the platform has become more and more prominent. However, at present, the privacy protection laws and regulations of mobile social e-commerce platforms are still imperfect, and the frequent occurrence of personal privacy leakage has seriously restricted the disclosure of users' private information. Therefore, it is important to explore the factors influencing the willingness of mobile social e-commerce users to disclose private information, to clarify the influence mechanism of the willingness to disclose private information; based on this, it is important to predict the willingness of consumers to disclose private information, and to take corresponding measures according to the results of the prediction, in order to promote the sustainable development of the mobile social e-commerce platform.

Mobile social e-commerce, based on traditional e-commerce, fully combines the technical characteristics of social media and online e-commerce, and flourishes with the popularization of mobile terminal devices. Mobile social e-commerce through social media and traditional e-commerce channels, the use of consumer interaction and business information dissemination so as to promote the purchase and sale of goods or services of a new business model [1]. Currently, mobile social e-commerce is mainly divided into three types: mobile social media platforms integrating business attributes represented by WeChat and Weibo;mobile e-commerce platforms integrating social attributes represented by Pinduoduo and Taobao; and third-party platforms integrating social attributes and business attributes represented by Xiaohongshu In mobile social e-commerce environments, users' private information continuously circulates in platforms, thus promoting group interaction and commerce. In the mobile social e-commerce environment, users' private information

continuously circulates in the platform to promote group interaction and consumption, and the platform analyzes the private information to push products or hot topics, so the importance of users' private information to the development of the platform is gradually highlighted.Banisar and Davies classify personal private information into four dimensions: informational, communication, spatial, and bodily privacy.31 Based on the characteristics of mobile apps, Hao Sensen further points out that Based on the characteristics of mobile APP, Hao further pointed out that mobile social user privacy information includes characteristic information, preference information, financial information and communication information, etc.4 Combined with the specific context of mobile social e-commerce, this paper argues that the privacy information of mobile social e-commerce users should include personal identity information, financial information, communication records, preference information, web browsing records and real-time location. With the continuous development of Internet technology, there are many innovations in the application scenarios of privacy information related research, and the research related to the willingness of privacy information disclosure has received close attention from scholars at home and abroad.

Privacy information disclosure emphasizes that users allow relevant platforms to use their privacy information or actively disclose their privacy information to merchants for their collection and use, domestic and foreign scholars from the user. Platform and social dimensions to explore the influencing factors of mobile social e-commerce users' willingness to disclose private information, and clarified that factors such as privacy concerns, perceived benefits, personality traits, platform quality, privacy policy, subjective norms and social norms have a significant influence on the willingness to disclose private information.[1]

2. The conflict between data value and data protection in social e-commerce

2.1. Security technology issues in virtualized environments

Virtualization technology and cloud computing technology breaks through the boundaries of operating systems and physical hardware. Although cloud computing environment has unparalleled advantages in centralized management, improved resource utilization, and heterogeneous resource integration, virtualization has also broadened the attack surface of malicious programs, bringing security challenges at the virtualization level to data security and privacy protection. Virtualization is a technology most closely related to the concept of cloud computing environment, and the large-scale application of cloud computing environment brings virtualization-related data security and privacy issues, such as the security of the virtual machine itself, the security of the virtual machine management platform, and the security of the virtual network constituted by virtual machines and privacy leakage issues. The virtual machine manager has certain vulnerabilities, and attackers can obtain access to the host through virtual machine software or software vulnerabilities running in the virtual machine, and control other virtual machines running on the host by accessing the host to complete the attack on the target virtual machine. In traditional computing environments, the security problem of a single machine does not spread to other machines, but in virtualized environments, the security problem of a single virtual machine can further ripple or spread to the entire virtual network environment, with potential data security risks issues

2.2. Security Issues in Cloud Computing Service Models

In the cloud computing environment, the data storage and processing are dependent on the cloud service provider, the user of their data also lost the physical level of control power, the user can neither determine which node of the data stored in the cloud service provider, there is no way to know the geographic location of the data storage, which brings about the uncertainty of the security of the user's

[1] ZHANG Jinsong,ZHANG Kai-Dong,HE Dong-Chen,et al. A study on users' willingness to disclose private information in mobile social e-commerce based on SEM and neural network[J]. Journal of Wuhan Textile University,2024,37(05):85-94.

data and the potential risk of privacy leakage [21]. cloud computing environment is centralized Cloud computing environments store huge amounts of user data, which is more likely to become the target of SQL injection attacks, phishing attacks, distributed denial of service (DDos), etc., and if the hackers carry out targeted large-scale attacks, the consequences and destructiveness will be even greater. Cloud computing environment is a multi-tenant environment, a cloud computing platform running multiple tenant applications and data, how to ensure the security of information resources between multi-tenant isolation is also a problem. In addition, the cloud computing service model will face the problem of collaboration security of cloud service providers, cloud service providers may access the user's data and information without authorization or delete the user's data and information in a complete manner as required due to business needs, cooperation requirements, or other reasons, the security responsibility of the cloud service providers is not clearly defined, and some of them will not take the corresponding security management measures, which is a potential threat to the data security and privacy protection of the users. This is a potential threat to user data security and privacy protection.

2.3. The problem of imperfect relevant laws and regulations

At this stage, various governmental departments have issued risk-based prevention rules and security management guidelines on the process of cloud computing, such as "Security Guidelines for Critical Areas of Cloud Computing" and "Guidelines for Security and Privacy Management of Public Cloud Computing", etc., but all of them are not mandatory for cloud computing participating entities, i.e., in terms of cloud computing data security and privacy protection, governmental departments have not formulated relevant and normative legal and regulatory documents, and cloud computing industry practitioners also have no unified cloud computing security standards to comply with!3! In the cloud computing environment, it is also necessary to consider the security and compliance of cross-border transmission of data, different countries and regions have different data security and privacy protection laws, and there are some countries that do not provide for user data security and privacy protection, and cross-border transmission of data may lead to the leakage of users' personal information or the compliance of the relevant data transfer Risks.

3. Mitigating conflicts: an analysis of privacy computing in social e-commerce

3.1. The concept of privacy computing

Privacy computing is the realization of collaborative computation between multiple parties to fully release the value of data on the premise that the data is "available and invisible" and does not threaten data security and privacy. [2]Multi-party computation, homomorphic encryption, federated learning, and trusted execution environments are important techniques for realizing privacy computing.

The principle of multi-party computation is to make the data participants can only get the output computation results among themselves through cryptographic techniques, without being able to know the input data of each party, so as to ensure that the data can successfully complete the computation task without exposing the data information in the circulation process. The underlying protocols included in multiparty computation are mainly inadvertent transmission, obfuscated circuits, and secret sharing.7 Homomorphic encryption is a technique in which data participants perform computations in a state where the data is encrypted. This computation technique allows the computation result of ciphertext to be consistent with that of plaintext, and the result of decryption followed by computation is the same as the result of computation followed by decryption, thus protecting data privacy and security while allowing data participants to complete data computation.Federated Learning is a distributed machine learning technique that enables the modeling of end-privacy data without collecting the original data of the data participants. The

[2] Yan Zhijing.Research Characteristics and Trends of Privacy Computing in China from 2013 to 2022:Visualization Based on CiteSpace[J]. Technology and Innovation,2023(21):57-62,65.

federated learning is a distributed machine learning technique that can realize the modeling of endpoint privacy data without collecting the original data of the data participants. Specifically, the data generated by each data participant's device (e.g., smartphone) is not uploaded, and the computation is done directly on the device locally. The trainer sends the model calculation parameters to the data participant, which uses the local data to do gradient calculation and then feeds the calculation results to the trainer's central server. The trainer receives the calculation results, summarizes them, and then updates the model parameters by gradient descent. The trainer then synchronizes the updated model parameters to all data participants, and so on, to complete the model training. In this process, each data participant does not expose the local raw data.

The Trusted Execution Environment is a separate and isolated security system for running sensitive data in addition to the traditional system operating environment. This is equivalent to dividing two isolated operating environments on a device, one is the environment run by an operating system like Android, and the other is the environment used to run and manipulate sensitive data. This isolated environment is the trusted execution environment. While other privacy technologies happily protect data by encrypting or keeping data out of the local area, there is a chance that the data could be leaked before it is even encrypted locally. Typically, operating systems accomplish the task of protecting data locally, but these operating systems are often vulnerable to security breaches, and examples of attacks on local devices and servers are commonplace. The Trusted Execution Environment solves this problem by placing the processing of sensitive data in an isolated environment, allowing for efficient data processing without threatening data security.

3.2. Current status of privacy computing in social e-commerce

With the development of network information technology, the value of data is increasing, and the demand for data protection is also increasing day by day. Traditional static data protection modes such as key negotiation, signature hash, and message authentication code can no longer meet the current data protection needs. The static data protection mode has begun to transition to the dynamic protection mode(8!). The emergence of privacy computing fulfills this data protection need by allowing multiple data participants to dynamically compute data while protecting data privacy. The stimulus of policy is also particularly significant. As laws and regulations continue to be introduced, the protection of information has become more demanding, and the accountability of the relevant parties has become more stringent. The Law of the People's Republic of China on the Protection of Personal Information came into effect on November 1, 2021 . The law stipulates that processors of personal information must encrypt, de-identify and other related security measures to avoid leakage, tampering and loss of personal information. Against this backdrop, privacy computing has emerged as an emerging technology that can strike a balance between industrial development and data security, with applicable scenarios in almost all data-driven industries.

3.2.1 Joint modeling of cross-platform user profiles

In the social e-commerce scenario, Federated Learning (FL) provides technical support for multi-platform data fusion through a distributed collaboration mechanism. [3]Specifically, social platforms (e.g., WeChat), e-commerce platforms (e.g., Pinduoduo) and third-party payment institutions can jointly construct user behavior prediction models without exchanging raw data. Taking the social recommendation scenario as an example, the e-commerce platform only needs to transmit to the social platform the gradient of the click characteristics of the desensitized products, while the social platform returns the encrypted social relationship weight parameters; the two sides co-optimize the encrypted parameters through the security aggregation protocol, and ultimately, on the basis of the protection of the user's social relationship chain, transaction records, and other sensitive information, the recommendation algorithm achieves the accurate iteration. From the perspective of compliance, this technology path strictly follows the provisions of Article 22 of the Personal Information Protection Law on "data sharing requires individual authorization", and fundamentally avoids the risk of leakage

[3] Yang Q. AI and data privacy protection: a federal learning crack[J]. Information Security Research,2019,5(11):961-965.

caused by centralized storage of traditional data through a decentralized data processing model. At the practical application level, the cooperation case between the federated learning team of WeCrowd Bank and a leading social e-commerce platform shows that the cross-domain modeling based on federated learning increased the accuracy of product click-through rate prediction by 12.3%, and the number of user privacy complaints dropped by more than 40% year-on-year, which confirms that the privacy computing technology meets both the business efficiency and compliance needs.[4]

3.2.2 Social Relationship Chain Protection and Fission Marketing

In the social e-commerce scenario, Secure Multi-Party Computation (SMPC) realizes a privacy-friendly social relationship verification mechanism through cryptographic protocol design. The core of the technology is: when user A invites friend B to participate in the group-building activity, the platform can complete the social network validity verification under the encrypted state of both parties' data through the Shamir secret sharing or obfuscated circuit (Garbled Circuit) protocol - i.e., to confirm whether B belongs to the valid nodes of A's social graph. without the need to obtain B's account ID, geolocation, device fingerprint, and other sensitive fields. This process only outputs a Boolean logical result ("yes/no validity"), which ensures that the original social relationship data is kept in a confidential and invisible state. From the perspective of legal compliance, this technical path strictly follows the provisions of Article 41 of the Network Security Law, which stipulates that "network operators shall not collect personal information unrelated to the services they provide", and through technical constraints, it avoids excessive collection of users' social graph data at the source and effectively reduces the compliance risk of "collecting personal information in excess of the scope". The technical constraints avoid excessive collection of users' social graph data from the source, effectively reducing the compliance risk of "over-collection of personal information". At the practical level, Xiaohongshu applies secure multi-party computing technology in social fission marketing scenarios, and its Privacy Protection and Data Security Transparency Report (2022) points out that through the deployment of privacy enhancement technologies (including the optimization of the SMPC protocol), the platform has not experienced any data leakage incidents triggered by the verification of social relationships in the whole year and the number of complaints from users about the "excessive collection of social information" is higher than the number of complaints from users about the "excessive collection of social information" in the previous year. The number of user complaints about "excessive collection of social information" dropped by 28% compared to the previous year. [5]This case shows that SMPC technology can realize the dual value of legal compliance and technology implementation without affecting the efficiency of social e-commerce fission marketing.

3.2.3 Privacy Enhancement in Dynamic Pricing and Antifraud

In the social e-commerce platform, the privacy computing technology builds a whole chain privacy protection system from data collection to value mining through the synergistic application of Differential Privacy and Homomorphic Encryption. [6]The platform first injects Laplace noise ($\varepsilon \leq 1$), which conforms to the strict mathematical definition, into users' historical transaction data, and accurately extracts group consumption trends, such as "Post-90s female users' sensitivity to beauty promotions is significantly higher than the average value", under the premise of ensuring that individual users can't be reverse-identified. Meanwhile, based on Paillier's homomorphic encryption solution, the platform can directly perform real-time calculations on encrypted user behavioral data (e.g., browsing frequency, return rate) to dynamically generate credit scores and apply them to differentiated pricing strategies without decrypting the original sensitive information. This combination of technologies not only meets the statutory requirement of Article 51 of the Personal Information Protection Law for "de-identified processing" of personal information, but also avoids

[4] Analysis of global digital banking strategies[J]. New Finance,2019,(03):4-9.

[5] Xiaohongshu Inc., Privacy Protection and Data Security Transparency Report 2022, p. 17, Table 4

[6] Xiong P,Zhu TQ,Wang XF. Differential privacy preservation and its applications[J]. Journal of Computing,2014,37(01):101-122.

the risk of algorithmic discrimination such as "big data kills familiarity" from the root through algorithmic verifiability, so that the platform maintains its precision marketing capability within the compliance framework. The platform maintains its precision marketing capability within the compliance framework.

Taking the practice of ShakeElectric's 2022 "Double 11" promotion as an example, the independent audit data of the China Institute of Information and Communications Technology's "Privacy Computing White Paper (2023)" shows that: after the platform desensitized users' browsing data through Local Differential Privacy (LDP) technology, the conversion rate of advertisement clicks was increased by 15.8% year-on-year ($p<0.05$). 0.05), and the probability of individual information leakage in the data flow link was reduced to less than 0.3% as tested by the National Center for Information Security Level Protection Evaluation. [7] The case shows that privacy computing technology can effectively balance the dual demands of commercial value mining and user rights protection, providing a technically compliant formula for the sustainable development of social e-commerce.

3.2.4 Cross-border data flow compliance

In the data governance framework of cross-border social e-commerce, the Trusted Execution Environment (TEE) reconfigures the technical realization paradigm of data sovereignty boundary through the hardware-level isolation mechanism. The core theoretical logic lies in the fact that the cross-border data sandbox constructed based on TEE restricts the computational tasks of foreign subjects to the isolated enclave encrypted by state-secret algorithms, so that the foreign entities can only execute the preset computational functions based on the confidential data (e.g., consumption behavior clustering analysis, price elasticity modeling), and are unable to obtain the original plaintext data through the means of memory snapshots and side-channel attacks. data through memory snapshots and side-channel attacks.[8]

This technology path realizes the cross-border collaboration principle of "data availability but not visibility" at the level of mathematical verifiability - offshore outputs (e.g. "regional market demand index") contain only group statistical characteristics, while sensitive fields such as individual user identities and behavioral trajectories are always locked in trusted hardware in the country. The results of offshore outputs (e.g. "Regional Market Demand Index") contain only group statistical characteristics, while sensitive fields such as individual user identities and behavioral trajectories are always locked in trusted hardware in China. As a result, the architecture naturally meets the statutory definition of "data exit" in Article 3 of the Measures for Security Assessment of Data Exit (i.e., "data in the territory is actually accessed or controlled by subjects outside the territory"), and because of its remote attestation mechanism, it can be used in a variety of ways through the TEE. Through the TEE's Remote Attestation mechanism, the direct access of overseas entities to the data in the country is technically blocked, so that self-certification of compliance can be realized without triggering the security assessment and declaration procedure. Further, by introducing Zero-Knowledge Proof to verify the integrity of the computation process, the platform can prove to the regulator that the generation of offshore outputs fully complies with the preset compliance rules (e.g., the data minimization principle), thus constructing a dynamic trust system that goes beyond the traditional compliance review at the level of technical endogeneity.[9]

[7] China Academy of Information and Communication Research, White Paper on Privacy Computing (2023), Beijing: China Academy of Information and Communication Research, 2023, p. 89, Case No. CT-2022-011.

[8] FENG Dengguo,LIU Jingbin,QIN Yu,et al. Trustworthy computing theory and technology in innovative development[J]. Science in China:Information Science,2020,50(08):1127-1147.

[9] LI Gongliang,HE Dongbo,GUO Bing,et al. A blockchain privacy protection algorithm based on zero-knowledge proof[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition),2020,48(07):112-116.DOI:10.13245/j.hust.200719.

4. A balanced strategy for privacy computing and data protection

In social e-commerce scenarios, user data protection requires the construction of a trinity strategy system of "technical protection - management standardization - compliance synergy".

4.1. Technical aspects

In social e-commerce scenarios, the multi-subject interaction of user data and the cross-multiplexing of sensitive social relationship chains have given rise to the integration and innovation of privacy computing technology. In order to realize the dynamic balance between data value mining and privacy security, it is necessary to build a three-layer technology system of "distributed modeling-noise protection-edge autonomy":

One is the distributed collaboration mechanism of Federated Learning. Social platforms (e.g., social relationship graph holders) and e-commerce platforms (e.g., transactional behavior data holders) achieve cross-domain collaborative modeling through Horizontal Federated Learning. Both parties only exchange homomorphic encrypted model gradient parameters (e.g., user interest vector weights), and update the global recommendation model through Secure Aggregation, which ensures that the original social relationships, purchase records, and other data are always kept locally and cuts off the path of data leakage from the transmission layer. Compared with traditional centralized modeling, this mechanism can reduce the exposure of sensitive data by up to 90%.[10]

The second is group portrait protection with differential privacy. In the local training phase of federated learning, user behavioral data (e.g., click sequences, dwell time) are injected with Laplacian Noise that satisfies the (ε, δ)-differential privacy constraints, so that the output group profiles (e.g., "Generation Z users' preference index for national brands") have mathematically provable privacy guarantee. With the dynamic adjustment of the privacy budget ($\varepsilon \leq 1$), the platform can adaptively balance the game relationship between data availability (e.g., ad conversion rate) and privacy intensity (e.g., user re-identification probability).[11]

Third, the localized preprocessing of edge computing: the graph structure of the social relationship chain is desensitized (e.g., k-anonymization processing) at user terminals or near-field edge servers (MEC nodes), and only topological features (e.g., node degree distribution, community clustering coefficients) are transmitted to the cloud, blocking the risk of global exposure of the social graph. Relying on the computational redundancy of edge devices, this architecture controls the life cycle of sensitive data within the local closed loop of "generation-processing-destruction", which is in line with the rigid requirement of the principle of "minimum necessity" in Article 22 of the Personal Information Protection Law.

The synergistic effect of the above technology stack is reflected in the following: federated learning solves the problem of cross-subject data silos, differential privacy defends against statistical inference attacks, and edge computing dissolves the single-point vulnerability of centralized storage, which together constitute the core capability of social e-commerce, "data is available but not visible". Taking the social recommendation scenario as an example, the social influence weight of user A can be encrypted and aggregated to the global model through federated learning, and its friends' relationship is desensitized by edge nodes to generate local subgraphs, which, combined with the group preference analysis protected by differential privacy, ultimately realizes the accurate recommendation of "the goods that A's friend B may like", and the platform is not able to The platform is unable to obtain the social association explicit text between A and B throughout the whole process. This framework responds to the fundamental contradiction between data sharing and privacy sovereignty in social e-commerce from the technical endogenous level, and provides a verifiable technical paradigm for the compliance of the Cybersecurity Law and the Data Security Law.

[10] Jakub Konečný et al. "Federated Learning: Strategies for Improving Communication Efficiency," arXiv preprint arXiv:1610.05492 (2016), https:// arxiv.org/abs/1610.05492.

[11] Cynthia Dwork and Aaron Roth, "The Algorithmic Foundations of Differential Privacy," Foundations and Trends® in Theoretical Computer Science 9, no. 3 -4 (2014): 211-407.

4.2. Management level

Establish a data classification and grading mechanism, and specify the principle of "minimal collection" of highly sensitive data such as user location and social graph; implement Dynamic Consent, allowing users to adjust the scope of data sharing in real time (e.g., temporarily open shopping preferences for time-limited recommendations); and simulate attack scenarios (e.g., model reversal attack) through the "privacy risk sandbox" and regularly practice the emergency response process. The "Privacy Risk Sandbox" simulates attack scenarios (e.g., model reversal attacks), and regularly rehearses the emergency response process.

Specifically, in social e-commerce platforms, the protection of user data needs to form a complete set of closed-loop from collection, use to risk prevention. For highly sensitive data such as users' location information and social relationships, platforms should follow national personal information security norms and strictly limit the scope and mode of collection. For example, when a user participates in a community group purchase and needs to share the location, the platform will only obtain a vague general area (e.g., "500 meters near a certain neighborhood"), not a precise location to the door number, and will automatically delete the relevant records after the transaction is over; for the user's friend network, the platform will anonymize it to ensure that there are sufficient numbers of people in everyone's social circle to ensure that the location of the user's friends and social relationships will be kept confidential. The platform will anonymize the user's friend network to ensure that each person's social circle has a sufficient number of similar users, avoiding the reverse locking of the identity of specific individuals through the friend list.

At the same time, platforms need to give users more flexible data control. For example, when a user participates in a time-limited promotion, he or she can temporarily authorize the platform to share his or her preference label of "like sports shoes" with the partner brand for accurate recommendation of products, but this permission will be automatically closed after the activity is over. Platforms also need to show users a transparent record of who and how their data is being used through technical means, such as easy-to-understand charts to illustrate the flow of data, to ensure that users are always in control of the dynamics of their own information.

In order to identify potential risks in advance, the platform can build a "security rehearsal room" that simulates attacks. By imitating hacker tactics (such as trying to push back user privacy from recommendation algorithms), the effectiveness of existing protective measures is tested, and protection strategies are constantly upgraded based on test results. For example, when it is found that a certain algorithm may leak the user's purchase records, the data encryption method is immediately adjusted or the algorithm's access rights are restricted. This "attack and defense rehearsal" mechanism can nip the risk in the bud and avoid damage to real user data.

This series of measures not only allows platforms to use data to optimize their services (e.g., recommending products that better understand users' preferences), but also strictly comply with the provisions of the Personal Information Protection Law regarding users' right to know and their right to refuse, so as to find a balance between commercial innovation and privacy protection. Just like in community group buying, users enjoy convenient localized services without worrying about their home addresses being abused - this kind of "feel free" experience is the key to the sustainable development of social e-commerce.

4.3. Compliance synergy level

In the globalized social e-commerce ecosystem, the construction of data compliance and user trust requires a two-way innovation of technology and system. In the face of the differentiated regulatory requirements of the European Union's General Data Protection Regulation (GDPR), the U.S. California Consumer Privacy Act (CCPA), and China's Personal Information Protection Law, platforms can design smart contract-driven cross-domain data flow control protocols - building a distributed ledger system through blockchain technology to record the identities of data sharing participants and the purpose of use and authorization status in an untamperable form to ensure the traceability of the entire process of cross-border data flow. participants' identities, purposes of use

and authorization status are recorded in a tamper-proof form, ensuring that the entire process of cross-border data flow is traceable. Through Formal Verification technology, the agreement transforms legal provisions into enforceable code rules. For example, Article 44 of the GDPR, "Conditions for Cross-Border Data Transmission," is encoded as a trigger threshold for smart contracts, which automatically triggers data desensitization or access to data when the recipient's jurisdiction fails to pass the EU adequacy determination. This automatically triggers a data desensitization or access termination mechanism.[12]

At the user interaction level, the design of the visual privacy dashboard follows the principle of "transparency enhancement" in human-computer interaction (HCI). [13]The data flow is visualized through topology diagrams (e.g. "Interest tags are called by ad partner A/B/C"), timelines to trace the history of authorization records, and Natural Language Generation (NLG) technology to transform legal terms into layman's descriptions (e.g. "Your geolocation is used to optimize the local distribution range with a 7-day storage cycle"). This design paradigm has been shown to significantly improve the effectiveness of user privacy management at .

Academic research has shown that the federated learning framework realizes the collaborative paradigm of "data does not move, model moves" through cryptographic protocols, and is able to complete cross-domain user profile calibration without directly transmitting the original data. The combination of dynamic authorization tools and blockchain depository implements the rigid requirements of Article 24 of the Personal Information Protection Law on the "Right to Withdraw Consent" at the operational level - every change of user's authority will generate time-stamped credentials on the chain, forming an electronic evidence chain with legal effect. Each change in the user's rights will generate time-stamped credentials on the chain, forming a chain of electronic evidence with legal effect. The essence of these technical synergistic strategies is to transform abstract legal obligations into verifiable mathematical constraints and perceivable user control, providing a systematic solution for social e-commerce companies to realize compliance and innovation under multiple regulatory environments.

References

[1] ZHANG Jinsong,ZHANG Kai-Dong,HE Dong-Chen,et al. A study on users' willingness to disclose private information in mobile social e-commerce based on SEM and neural network[J]. Journal of Wuhan Textile University,2024,37(05):85-94.

[2] Yan Zhijing.Research Characteristics and Trends of Privacy Computing in China from 2013 to 2022:Visualization Based on CiteSpace[J]. Technology and Innovation,2023(21):57-62,65.

[3] Yang Q. AI and data privacy protection: a federal learning crack[J]. Information Security Research,2019,5(11):961-965.

[4] Analysis of global digital banking strategies[J]. New Finance,2019,(03):4-9.

[5] Xiaohongshu Inc., Privacy Protection and Data Security Transparency Report 2022, p. 17, Table 4

[6] Xiong P,Zhu TQ,Wang XF. Differential privacy preservation and its applications[J]. Journal of Computing,2014,37(01):101-122.

[7] China Academy of Information and Communication Research, White Paper on Privacy Computing (2023), Beijing: China Academy of Information and Communication Research, 2023, p. 89, Case No. CT-2022-011.

[8] FENG Dengguo,LIU Jingbin,QIN Yu,et al. Trustworthy computing theory and technology in innovative development[J]. Science in China:Information Science,2020,50(08):1127-1147.

[9] LI Gongliang,HE Dongbo,GUO Bing,et al. A blockchain privacy protection algorithm based on zero-knowledge proof[J]. Journal of Huazhong University of Science and Technology(Natural Science Edition),2020,48(07):112-116.DOI:10.13245/j.hust.200719.

[12] S. Peng et al. "Enhancing Cross-Border Data Sharing in Blockchain Networks: a Compliance-Centric Approach Ensuring Anonymity and Traceability," in 2023 3rd International Conference on Computer Science and Blockchain (CCSB), 200-204.

[13] Du Yanyong. On the transparency of artificial intelligence systems[J]. Research in Science,2022,40(09):1537-1543.

[10] Jakub Konečný et al. "Federated Learning: Strategies for Improving Communication Efficiency," arXiv preprint arXiv:1610.05492(2016),https:// arxiv.org/abs/1610.05492.

[11] Cynthia Dwork and Aaron Roth, "The Algorithmic Foundations of Differential Privacy," Foundations and Trends® in Theoretical Computer Science 9, no. 3-4 (2014): 211-407.

[12] S. Peng et al. "Enhancing Cross-Border Data Sharing in Blockchain Networks: a Compliance-Centric Approach Ensuring Anonymity and Traceability," in 2023 3rd International Conference on Computer Science and Blockchain (CCSB), 200-204.

[13] Du Yanyong. On the transparency of artificial intelligence systems[J]. Research in Science,2022,40(09):1537-1543.