Hindawi
Security and Communication Networks
Volume 2023, Article ID 9850941, 1 page
https://doi.org/10.1155/2023/9850941

Retraction

Retracted: Privacy Protection Dilemma and Improved Algorithm Construction Based on Deep Learning in the Era of Artificial Intelligence

Security and Communication Networks

Received 8 August 2023; Accepted 8 August 2023; Published 9 August 2023

Copyright © 2023 Security and Communication Networks. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] C. Tang, "Privacy Protection Dilemma and Improved Algorithm Construction Based on Deep Learning in the Era of Artificial Intelligence," *Security and Communication Networks*, vol. 2022, Article ID 8711962, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8711962, 9 pages
https://doi.org/10.1155/2022/8711962

WILEY | Hindawi

Research Article

Privacy Protection Dilemma and Improved Algorithm Construction Based on Deep Learning in the Era of Artificial Intelligence

Chenming Tang

Law School, Hunan University, Changsha 410082, Hunan, China

Correspondence should be addressed to Chenming Tang; 1217030101@st.usst.edu.cn

Received 16 May 2022; Revised 9 June 2022; Accepted 16 June 2022; Published 29 June 2022

Academic Editor: Mohammad Ayoub Khan

Copyright © 2022 Chenming Tang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the development of science and technology and the progress of social civilization, people have entered the era of big data. People's personal information, privacy data, financial status, and financial information have become more and more transparent. Personal privacy has also changed from traditional physical privacy to portrait privacy and further changed to digital privacy based on artificial intelligence, big data, algorithms, and other technologies. At this stage, a new type of privacy problem has been formed, that is, deep learning privacy. In order to better protect the right to privacy, we should effectively block the protection dilemma of privacy and improve the construction of algorithms in the era of artificial intelligence, strengthen our own awareness of prevention, understand the current situation of infringing and protecting the right to privacy, fully protect the right to privacy, and promote the legal construction of the right to privacy in the era of artificial intelligence. However, China's traditional privacy protection system cannot fully adapt to this change, and this highlights the lack of rules and hidden dangers of efficiency of privacy protection under the influence of penetrating monitoring, mandatory sharing, structural discrimination, and interactive assimilation of artificial intelligence. Therefore, based on the infringement mechanism of artificial intelligence on personal privacy, we should build a monitoring and identification function filing system, establish a segmentation and selective agreement rule system, build a comparative antidiscrimination rule system, innovate the "cloud blocking" rule system to protect our privacy, and comprehensively address the major challenges posed by new technologies such as artificial intelligence to China's privacy protection system.

RETRACTED

1. Questions Raised: From "Physical Privacy" to "Digital Privacy"

In the CCTV 315 party in 2021, it was exposed that a large number of enterprises use insensitive camera equipment to capture customers' facial information in the internal area of the enterprise and input the facial information into the enterprise's own database without soliciting users' opinions, so as to obtain the corresponding personal privacy data, for example, large enterprises such as Zheng tong automobile and Kohler bathroom and installing smart cameras with face recognition function in sales stores and other areas. In this regard, the relevant market supervision and Administration Bureau began to investigate and ordered the corresponding enterprises to make corrections. The above-mentioned enterprises have also made corresponding commitments; that is, the information captured by the camera will only be used for population statistics, and other information will not be used for preservation and analysis. However, the incident still caused people from all walks of life to ponder and even panic: Is there any evidence to follow for the effective protection of personal privacy in the data environment? In addition, at this stage, there are an endless stream of candid shooting events, human flesh search events, cooked killing events, and so on. China has highlighted the disadvantages in the innovation and application of artificial intelligence technology at the social level, that is, the intangible infringement of human privacy.

However, the infringement of the right to privacy is not formed suddenly. Human privacy form and privacy protection system have experienced a development process from scratch and from weak to strong in history and can be mainly divided into three stages. The historical analysis of the three-stage privacy form and the privacy protection system shows that the historical evolution of privacy protection highlights the technical and institutional characteristics, in which the technological development has a strong driving significance for the innovation of the privacy system.

The first stage is the physical privacy stage. Physical privacy refers to the personal body, organs, objects, residence space, and other physical rational privacy interests, which is evolved from the natural right of existence. According to Louis [1], the "father of privacy," the protection of individual right to survival is the oldest legal principle. The earliest right to survival only protected mankind from different forms of atrocities. With the gradual expansion and improvement of human spiritual world, emotional category, and mental maturity, the right to survival began to mean "the right to enjoy life," that is, "not to be disturbed"; the right to survival began to evolve from personal security to personal physical privacy rights, which is the normal growth of law in the process of civilization [1]. In the stage of physical privacy, people's privacy interests have not been integrated into technical factors, nor constitute the corresponding concept of rights and interests, so there are no corresponding privacy system and its protection system. At this stage, the protection of personal physical privacy is generally carried out through physical means, and its concept and connotation stay in the field of constitutional protection. At the same time, the means of privacy protection in this period are generally private, which does not involve the scope of public power and privacy protection system. Without involving technical factors, personal privacy interests are wrapped and protected by private forces on the physical level (such as covering the body with clothes and the residence with houses). Privacy interests are effectively controlled in private space, forming a solid protective layer.

The second stage is the portrait privacy stage. Compared with the physical privacy stage, the most important intervention factor in this stage is technology. For example, at the end of the nineteenth century, the impact of the media in the process of social change also impacted the protection efficiency of personal privacy. Newspapers and other media deepened social ties, such as the intervention of photography technology, infrared technology, and eavesdropping technology in social operation, breaking the physical and spatial protection of personal privacy information in the stage of physical privacy. At this stage, Blanca [2] proposed the concept of "communication secret right," aiming at the protection of personal privacy in the electronic communication environment. It brings the electronic communication technology different from the traditional background into the consideration of the construction of privacy protection system and emphasizes that "the precision means developed by technological progress seriously interfere with the efficiency and quality of personal privacy protection" [2]. This kind of technical interference has caused two effects: on the one hand, private power is no longer the only means of privacy protection, but also cannot become the most effective tool of privacy protection. On the other hand, the social level began to form the concept of rights and interests related to privacy, which is also an important driving force for the emergence and development of the privacy protection system.

The third stage is the information privacy stage. At this stage, the technical factors as the main erosion force began to change. From photography and portrait technology to information and data technology, these technologies formed a new type of data and network cloud space, causing a more thorough invasion of personal privacy. Specifically, first of all, the construction of cyberspace and the erosion of data technology make personal privacy information spillover to public space and public domain more than portrait privacy. Secondly, it is more and more difficult to control personal privacy information by means of personal protection and relief. Third, in the process of the continuous progress of science and technology, the lack of privacy protection is increasingly reflected. This is also the essence of the "face stealing" event in the information and data age.

In Wu [3], it can be seen that, at different stages of the development of privacy interests, the main focus is on three aspects: first, the erosion of privacy interests by technical factors is gradually intensified [3]. Secondly, personal privacy information is increasingly breaking through the control of personal private power and spreading and spilling into the public sphere. Thirdly, the above impact has gradually increased the requirements for the innovation and improvement of the privacy protection system. See Table 1 for specific changes in privacy related factors.

In Table 1, when discussing privacy protection in the era of artificial intelligence, we should firmly grasp the following three elements: first, as an intervention factor, the technical characteristics and social impact of artificial intelligence technology; secondly, the boundary of private information and data in the public domain and private domain, the changing trend, and corresponding risks in the intelligent era; third, the defects of the traditional privacy protection system under the influence of the above factors, and the improvement and innovation of its rules. This paper intends to make an in-depth discussion on the above three aspects and seek the path of innovation and improvement of privacy protection system in the era of artificial intelligence.

2. The Mechanism of Privacy Infringement and the Dilemma of Privacy Protection in the Era of Artificial Intelligence

The application of artificial intelligence has had three major impacts on Chinese society at this stage: first, the improvement of social operation efficiency; second, the real social problems from the opposite side; third, the outstanding performance of social problems at the legal level. In general, the traditional privacy protection system, the specific principle of self-determination, the rule of informed

RETRACTED

Table 1: Privacy protection factors in different stages.

	Intervention factors	Private relief effect	Degree of private information spillover into public space	Requirements of privacy protection system
Physical privacy phase	—	High	Low	Low
Portrait privacy stage	Camera and monitoring technology	Lower	Higher	Secondary
Information privacy stage	Data and network technology	Very low	Extremely high	High

consent, and the judicial relief mechanism have been seriously impacted. At the same time, artificial intelligence technology has also triggered the demand for new rules, such as cloud blocking rules and segmented selection network protocol rules, which are not clear at this stage.

2.1. Penetrating Monitoring: The Principle of Self-Determination and Consent Is a Mere Formality. The so-called penetrating monitoring means that artificial intelligence technology forcibly extracts information from the protection layer of privacy through personal privacy and traditional privacy protection system. Still, we take the application of face recognition technology as an example. Although face information has been established as one of the types of personal private information by China's legislation at this stage, such as the code for personal information security and the civil code, the above regulations only make qualitative provisions on the behavior of face information collection at the legislative level. At the specific operation level, it does not solve the deep-seated problems exposed by the "face stealing" incident, that is, the passive publicity of personal privacy in the "face stealing era." In Li [4], in the context of the transformation and application of new technologies, the passive openness of the right to privacy refers to the gradual blurring and dissolution of its boundary in the public sphere, and the transformation is a retrogressive change caused by scientific and technological innovation and irreversible [4]. Specifically, under the background of traditional legal norms, there are obvious boundaries and high barriers between personal privacy and public data information. To collect the privacy information of natural persons, we need to cross solid barriers, such as the extraction of residential, letter, and equipment information. Since then, the rise of Internet technology has weakened the protective power of the barrier, and the whereabouts of natural persons in cyberspace will expose their private information, such as human flesh technology [5]. In the context of big data, even static natural persons began to expose privacy. Biometrics and data mining technology began to occupy the commanding height of "information war," and personal privacy barriers began to collapse.

The damage of this penetration monitoring behavior to the traditional legal mechanism mainly lies in the reduced applicability of the consent rules on privacy and information and the principle of self-determination in the civil code [6]. Specifically, the institutional edge of traditional privacy protection is mainly reflected in the "consent principle" in the civil code and the network security law, which highlights the concept of individual autonomy in legislation. However, penetration monitoring is usually comprehensive. Instead of dividing the consent items and handing them over to the obligee, it forces the obligee to passively give up its autonomy through standard terms. This leads to the loss of the creditor's prior right of self-determination and autonomy and also cuts off the creditor's postrelief path.

2.2. Compulsory Sharing: Lack of Privacy Infringement Relief Mechanism. Mandatory sharing means that the artificial intelligence technology controller forces the privacy right holder to integrate into its information collection scope through the monopoly of science and technology and then infringes its privacy right. Mandatory sharing reflects the contradiction between self-determination and efficiency in the field of privacy. The so-called self-determination refers to the principle of self-determination and the principle of consent stipulated by the law, such as the provisions of the code for personal information security: face information belongs to personal sensitive information and private information, and its collection requires the explicit consent and authorization of the subject; Article 1035 of the Civil Code stipulates that the processing of personal information requires the explicit consent of the subject or guardian. Under the background of big data technology, the behavior of data mining and crawling technology to collect and process information is active, massive, and automatic. In Wang [7], the essential purpose of this behavior feature is to realize the value of efficiency, such as the collection and processing of a large amount of data, improving the ability of demand perception, and so on. However, if the consent of the subject is sought for each collection and processing behavior, it will not only erode the above efficiency value, but also reflect great difficulties in reality [7]. Therefore, many data mining behaviors tend to build a unified set of consent and self-determination terms, even if users agree to each mining behavior in the future. But this collection is often formal, which also infringes on the legal value of the principle of self-determination, because if the user does not agree with one of the mining behaviors, they will have to give up the whole set of services, which are necessary in real life.

The risk caused by this impact is the failure of the relief norms for privacy infringement. For example, according to Professor Zhang [8], the right to privacy is a kind of personality right enjoyed by citizens to have a peaceful private life and information protected according to law, not

RETRACTED

disturbed, known, collected, used, and disclosed by others [8]. This concept embodies the dominant and protective characteristics of the right to privacy and also confirms the provisions on privacy in article 1032 of the civil code. At the judicial level, when natural persons accuse criminals of using artificial intelligence technology to infringe their privacy, they need to bear more pressure in providing evidence. First, the plaintiff needs to prove the privacy of the information collected by the defendant using artificial intelligence technology. As mentioned above, in the era of network and data, the boundary between personal private space and public space has been very blurred. In many cases, it is difficult for natural persons to simply prove that a certain information belongs to private information they are unwilling to disclose as in the traditional background. Secondly, the plaintiff needs to prove the defendant's actual infringement, that is, the intrusion, collection, and disclosure of his own peace and private information. However, artificial intelligence technology adopts more professional and technical thinking and means, still taking the face stealing incident as an example. The technical means are often difficult to be known by ordinary individuals. The asymmetry and opacity of technology-based information make it impossible for the plaintiff to collect effective evidence [9]. Thirdly, the use of information is an internal behavior, which is often a process in which the subject in control of artificial intelligence technology combines and analyzes the collected information and data to obtain the corresponding results. This process is more hidden than the collection of information. In this regard, it is basically impossible for the privacy right holder to obtain relevant evidence materials. Generally speaking, in the case of being unable to obtain sufficient and effective evidence materials, the privacy right holder cannot obtain effective right protection through traditional litigation [10].

2.3. Interactive Assimilation: Absence of "Local Cloud" Spatial Blocking Rules. Interactive assimilation refers to the behavior and phenomenon that natural persons voluntarily transmit the information containing personal privacy and preferences to the AI terminal when interacting with AI and assimilate personal private space with AI interactive space. This assimilation comes from Zheng Zhifeng's concept of "setting privacy," which believes that the "social function" and "social nature" contained in artificial intelligence are a new functional essence never carried by traditional technology, which drives the emergence of a new type of setting privacy, namely, "setting privacy." Setting privacy refers to the fact that, in the process of interaction between people and agents, people usually incorporate their interests and preferences into artificial intelligence agents with social interaction functions. For example, the interaction functions carried in smart furniture (smart TV, smart screen, etc.) can allow users to set their preferences. With the deepening of interaction, people's psychological attributes may be mastered by the learning function of artificial intelligence. The private space and psychological space of natural people will be completely open to agents. These settings themselves are the carrier of human privacy. This type of privacy is characterized by being implicit and long-term. Different from traditional privacy, it requires a long-term interaction process and machine learning process to be reflected and forms concealment within the agent [11].

Interactive assimilation is based on mandatory sharing. At this stage, intelligent devices have been integrated into various fields, and the integration of interactive technologies has been gradually realized in people's homes, cars, wearable devices, and so on. In this integration process, people's privacy space is also gradually integrated with the intelligent interaction space, that is, with the cloud space connected by the agent. In other words, fundamentally, as long as the agent interaction technology is adopted, people's private space will no longer exist.

The problem caused by this phenomenal change at the legal level is very obvious, because its essence is the problem of technical connectivity. To solve this problem from the practical level, the possible solution is to block the local interactive space from the cloud space, such as intelligent localization technology, verification technology for accessing the cloud space, and local blockchain technology. However, the current legal system does not make any requirements and regulatory norms for this. The current law does not pay attention to the interactive functions and technologies embedded in the smart body but turns the focus to the issue of realistic privacy infringement. In fact, it presents a state of absence in setting privacy. Specifically, in terms of China's domestic laws and regulations, the first generation of personal information protection legal framework cannot be applied to the problem of artificial intelligence interaction. Its "user control mode" in front of artificial intelligence interaction technology reflects the dilemma of China's information privacy protection system in the initial stage. In terms of international laws and regulations, Article 22, paragraph 4, of the EU general data protection law prohibits automatic processing, which provides inspiration, but the effect is still not obvious; Article 25 introduces the privacy design theory, which emphasizes the horizontal multiparty synergy of personal privacy in the intelligent environment, the vertical whole life cycle, and all-round protection of personal information protection. However, this theory has not yet formed a system in reality and lacks operability.

2.4. Structured Discrimination: Secondary Infringement of Privacy. After the 315-face stealing incident, many enterprises promised that the personal information collected by their equipment would not be used for analysis and application, but only for people statistics and other purposes. However, the proof of negation has theoretical difficulties, coupled with the characteristics of professionalism, information asymmetry, and monopoly of data technology, and this proof is more difficult. In other words, users cannot judge whether they are caught in the "Truman effect" and ripening dilemma of data. In many cases, users can respond only on the basis of notification by law enforcement departments. Taking the flying pig app as an example, the

RETRACTED

president of flying pig (vice president of Alibaba Group) said in an interview that the membership system of flying pig app would not have problems such as killing cooked food and privacy infringement. However, in October 2020, flying pig was criticized by Zhejiang Consumer Protection Commission twice, involving big data killing cooked food and false publicity. This contradiction leads to the decline of users' trust in service providers, network platforms, and social devices. At the same time, many privacy violations are hidden in the dark and cannot be fully and timely perceived.

In this way, the right to privacy will be harmed by secondary infringement. The infringement in the first stage is an infringement of the right to privacy; that is, the wrongdoer steals the privacy information without consent by using artificial intelligence technology or collects privacy data on the basis of forced consent sharing, while the infringement in the second stage is to use the illegally obtained privacy information to combine, arrange, and evolve through intelligent analysis technology to form hierarchical information. On this basis, it has caused "implicit bias" and "structural inequality" in the data environment, forming unconscious systematic discrimination [12]. This kind of implicit discrimination and prejudice cannot be regulated by the norms of traditional competition law, because it does not have the formal elements stipulated by traditional competition law. Although the State Administration of market supervision specially drafted and issued the antimonopoly guide on the field of platform economy (Draft for comments) (hereinafter referred to as the draft for comments), it only involves the level of the platform, not the level of artificial intelligence technology adopted by the platform, nor can it be processed through the traditional privacy norms, because its basic information is the "secondary data" processed through personal information and personal privacy data.

Generally speaking, the four aspects of AI invading human privacy are interrelated. Among them, penetration monitoring is an active exploration from artificial intelligence to personal privacy. Forced sharing is the monopoly of artificial intelligence, forcing the obligee to share private information with artificial intelligence. Interactive assimilation is the integration of artificial intelligence space and human privacy space at the potential interaction level. Finally, the privacy information data formed by the above three paths can realize specific application and secondary infringement. The specific logic is shown in Figure 1:

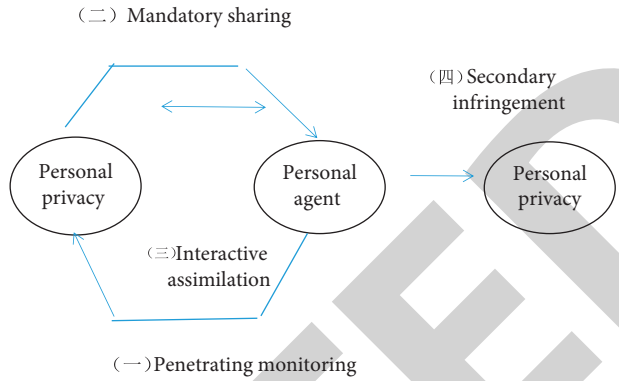

Figure 1: Logic diagram of AI infringement on privacy.

3. Construction and Method Verification of Improved Algorithm in Artificial Intelligence Era Based on Deep Learning

3.1. Construction of Improved Algorithm in Artificial Intelligence Era Based on Deep Learning. The arrival of artificial intelligence era makes our life more convenient and efficient, but it also brings a series of negative effects, such as personal information, physical health, and personal preferences under big data, especially the privacy of deep learning. In the intelligent age, everyone's life information is exposed to the network, and the security factor is greatly reduced. Now, we can only improve the algorithm manually to protect the privacy of in-depth learning. With the blessing of computer network technology, we can build an improved algorithm to protect privacy. The analysis of privacy algorithm based on artificial intelligence technology assisted improved deep learning is shown in Figure 2.

As shown in Figure 2, it shows the deep learning algorithms used by various data information. The relevant information data are analyzed and explored through rectangular data and transformed into the corresponding data characteristic matrix through digital analysis and artificial intelligence auxiliary technology. After analyzing the intelligence of overrun learning machine through fuzzy neural network system, the output result is finally obtained through binary calculation and analysis.

3.2. Statistical Methods. The data of this study were processed by SPSS 20.0 statistical software. The measurement data were expressed in $(x \pm s)$, and t-test was performed. The counting data were expressed in $[n\ (\%)]$, line χ^2 test, $P < 0.05$, and the difference was statistically significant.

3.3. Analysis of Coupling Degree of Different Algorithms. The right to privacy in the era of artificial intelligence is different from the right to privacy in the traditional concept. With the rapid development of artificial intelligence technology, through the algorithm of in-depth learning, control and supervise the data information to prevent leakage or improper use. While protecting the right to privacy, we should also strengthen technical supervision, build algorithm improvement, and improve the awareness of privacy protection. Now, we analyze the coupling degree of previous and deep learning algorithms in privacy protection and get Table 2.

Table 2 shows the comparison results of the coupling degree data of two different algorithms in privacy protection. It can be clearly seen that the use of deep learning algorithm has certain advantages in privacy protection, and the coupling degree data of the two algorithms are $T < 10$, $P < 0.05$, which is statistically significant.

RETRACTED

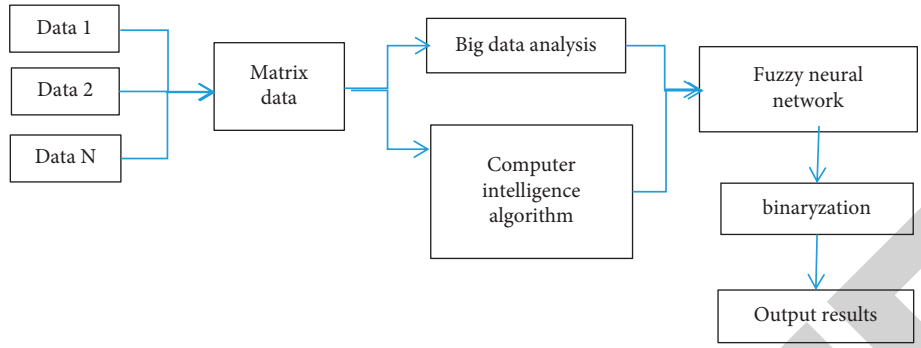

Figure 2: Analysis of privacy algorithm assisted by artificial intelligence technology for improved deep learning.

Table 2: Analysis of coupling degree of different algorithms in privacy protection.

Grouping	Coupling degree	
	Before use	After use
Previous algorithm	71.23	79.56
Deep learning algorithm	88.25	94.42
T	7.252	6.456
P	0.041	0.038

In order to better compare the coupling degree of two different algorithms in privacy protection, the data in Table 2 are visually analyzed, as shown in Figure 3.

As shown in Figure 3, the coupling analysis results of two different algorithms in privacy protection are shown. It is more intuitive to see that the deep learning algorithm is better than the previous algorithm in privacy protection, which indirectly shows that the deep learning algorithm can better prevent information leakage in privacy protection and has obvious advantages.

4. Theoretical Extension and Institutional Innovation of Privacy in the Era of Artificial Intelligence

According to the scientific and technological characteristics of artificial intelligence technology, its practical impact on social operation, and its impact on the traditional privacy protection system, we can analyze the specific countermeasures to the corresponding challenges. In Huang [13], we should firmly grasp the infringement mechanism of artificial intelligence technology on the right to privacy in the process of legislation and law application and make a targeted rule breakthrough [13]. In Qi [14], moreover, in the face of the growing privacy crisis and the basically invalid privacy right, the European Union and the United States have separately constructed personal data/information protection systems with different styles as the pilot mechanism for privacy protection [14].

4.1. Penetrating Monitoring Technology Filing System. The filing system of penetrating monitoring technology refers to the fact that the application of agent monitoring and identification technology should have certain technical and professional conditions, and the application behavior should be dynamically filed. The purpose of filing is to file professional and technical behaviors with relevant management authorities for reference, and the penetrating monitoring behavior of artificial intelligence at this stage meets this conditional requirement. International theories generally believe that, at this stage, the threat of artificial intelligence to human privacy has reached a more serious level and adopt a prohibited attitude towards it. According to the article "Face recognition is the" plutonium "element in the field of AI" by Luke stark, a researcher of Microsoft Research Institute, the functions of artificial intelligence such as face recognition and dynamic monitoring are similar to the professional and dangerous existence of plutonium, which can only be used when it is extremely professional and necessary. For example, the monitoring technology of artificial intelligence can be used in the investigation of national security and major cases, but its advantages and disadvantages cannot be effectively divided at this stage in the use of civil field. For example, in China's "face stealing incident," the United States has had an impact and impact on the artificial intelligence recognition and monitoring technology on the basic rights such as racial justice and personal peace rights. For example, a female college student was identified as a suspect in the Sri Lankan bombing by the American face recognition system, which fully highlights its danger. Based on this, the recognition and monitoring function of artificial intelligence is called "the most dangerous monitoring tool invention in human history" by Woodrow hazogg (2018), a professor at the school of law of Northeastern University, which even calls for a "comprehensive ban." In practice, many business entities also began to practice the restrictions on AI monitoring and identification technology. For example, IBM decided to refuse to implement Jim Crowe law; Amazon announced to suspend the provision of face recognition technology services to the government and public security institutions; Microsoft imposes strict restrictions on the application of face recognition technology.

In China, artificial intelligence technology, as the most important embedded technology of data-based social operation mode, on the one hand, reflects its practical application value; on the other hand, it is very difficult to peel it off at the social level at this stage. In this case, complete prohibition is impossible and unnecessary, and its use should be restricted based on its professional and technical

RETRACTED

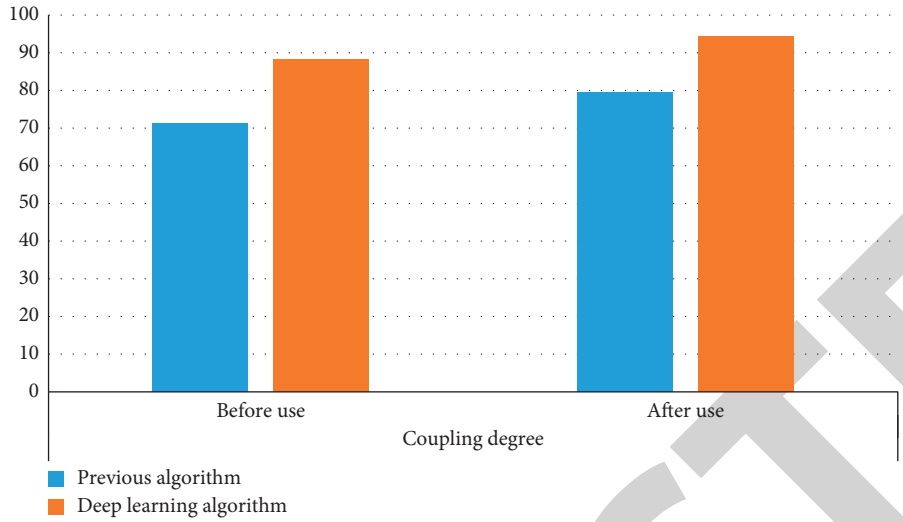

Figure 3: Visual diagram of coupling analysis of different algorithms in privacy protection.

characteristics. The most effective operation is the construction of the filing system.

Specifically, first of all, strictly regulate the use of artificial intelligence monitoring and identification technology. That is, some restrictive functions of artificial intelligence can only be used in necessary and professional and technical fields such as case investigation and national security. For general civil purposes, the above special functions cannot be used. Secondly, the agent with embedded identification and monitoring function should be registered for reference before it is put into use. For general matters, it can be filed independently, and for matters with strong technical nature, it can adopt the agent filing system. Thirdly, the specific AI identification and monitoring behavior should also be dynamically reported, and the operation situation and damage estimation report should be uploaded in real time, so as to protect the privacy and other personal rights and interests of users and ordinary natural persons. Finally, according to the filing situation, the artificial intelligence monitoring and identification behavior is connected with the specific subject, so as to realize the effective responsibility distribution and attribution. When the legal subject status of AI is unknown, the relevant imputation is a major problem at the legal level, and the filing system can solve this problem and solve the ethical dilemma of "escaping to technology neutrality" at the theoretical level.

4.2. Build Segmented and Selective Network Protocol Rules. For the problem of mandatory sharing, there are not enough norms to curb and prevent it at this stage. The only relevant specifications include the prohibition of default authorization and function binding in the data security management measures (Exposure Draft) of the state Internet Information Office, as well as the mandatory specifications for the provision of core functions; The antimonopoly guide on the field of platform economy (Draft for comments) drafted and issued by the State Administration of market supervision prohibits the "one out of two" of the platform. However, at the operational level, the solution to the problem of mandatory sharing has not yet achieved the expected effect. At the same time, at the theoretical level, the above norms highlight the legislative differences and ambiguities in the characterization of the mandatory sharing of artificial intelligence in China. For example, the measures for the administration of data security (Draft for comments) identified mandatory sharing as a binding act, while the antimonopoly guide on the field of platform economy (Draft for comments) characterized mandatory sharing as an exclusive agreement, which belongs to unfair competition. This not only shows that compulsory sharing is a complex behavior, but also shows its important impact on all fields of society. It should also be discussed separately in the field of privacy protection.

Therefore, for compulsory sharing, on the one hand, we should clarify the nature of its behavior in the field of privacy; on the other hand, we should set up corresponding rules dedicated to compulsory sharing to protect the privacy rights and interests of the opposite party. From the perspective of legal theory, the network protocol involved in compulsory sharing is an agreement signed between network service providers and intelligent technology providers and users. In essence, it belongs to the contracting behavior between equal civil subjects, so it has the nature of contract. From the content of the contract, the right of the privacy right holder is to enjoy network or intelligent services, and the obligation is to transfer some personal information rights and privacy rights. The right of the provider is to obtain some information and data, while the obligation is to provide network and intelligent services. According to Article 5 of the civil code, when engaging in civil activities, civil subjects should follow the principle of voluntariness and establish, change, and terminate civil legal relations according to their own will, which embodies the principle of voluntariness in the signing of civil acts and civil contracts. At the same time, this principle should be applied to every clause of civil contract. However, the network protocol in the problem of mandatory sharing does not provide a choice

RETRACTED

space for the voluntary principle but uses the mandatory behavior of one of two to force the opponent to provide information transmission interface. Therefore, at the rule level, we should set divisive and selective agreement rules; that is, divide the functions and protocols of network services and intelligent services, correspond different aspects of personal information collection behavior with different network and intelligent service functions, and return the option to the privacy right holder, who can choose the specific content of the right to be transferred. Although the establishment of this rule will improve the signing efficiency of network agreements, it protects the right of self-determination and choice of privacy people from the legal level.

4.3. Construction of Artificial Intelligence "Cloud Blocking" Rule System. The essence of "cloud blocking" is to isolate the cloud storage space constructed by artificial intelligence from the user's local database, so as to protect the user's personal privacy from overflowing the local space. As mentioned above, AI interaction technology and functions make intelligent settings a new privacy carrier. The connection with cloud space makes the integration and assimilation of natural person's privacy space and cloud space, which is very unfavorable to the protection of personal privacy. In this regard, the most effective way is to set the blocking rules between cloud space and local space, separate cloud space from local space, and take the local intelligent interaction space as a certain extension of personal privacy space; that is, expand the boundary of personal privacy protection.

However, the above cloud blocking rules have not yet formed a system at this stage. International concerns about the interactive function of artificial intelligence generally focus on the data security at the national level, such as the transnational storage standards stipulated by the safegabor alliance of the European Union and the security level requirements for accessing the safegabor alliance. In China, the corresponding norms on cloud computing still follow the relevant legal norms and relevant policy provisions of the traditional telecommunications industry. For example, in terms of qualification requirements, the Telecommunications Regulations of the people's Republic of China and the measures for the administration of telecommunications business license stipulate franchise terms, as well as the access and qualification requirements for telecommunications business license. In 2012, the circular on further standardizing the market access of Internet Data Center (IDC) business and Internet access service (ISP) business (hereinafter referred to as the circular) further put forward the process requirements and technical evaluation requirements (four items) for market access. It can be seen that China's approach is as follows: on the one hand, interpret cloud computing as "telecom value-added services" and apply the above specifications, which only involves access specifications and qualification requirements. On the other hand, strictly follow the rules of licensed operation and use administrative norms to regulate the market. However, the specific "cloud local" connection requirements and specifications have not been clarified either at the international level or in China. It adheres to a prudent attitude of supporting and partially limiting new things and opening up, and there is no restriction on market capacity in terms of economy. This is obviously not conducive to the quality and efficiency of user privacy protection, because in the cloud space, the technology controller is in an absolute dominant position, and the simple ex ante specification is not enough to limit it.

Therefore, China should appropriately upgrade the legal level of notice at the legislative level or clarify cloud computing and cloud interaction as a separate legal concept, rather than following the traditional concept of telecom value-added services. At the same time, the "cloud blocking" rule should be added to the relevant legal system. On the one hand, artificial intelligence is allowed to save the interaction results and convolution neural network learning results in the local storage space and strictly distinguish them from the cloud space. On the other hand, add corresponding connection verification in terms of access and technical qualification, allow users to verify themselves when connecting cloud space with local space, and give users the right of self-determination in connection and assimilation. This will not only help effectively control the personal private space from serious overflow and effectively protect the boundary of private space, but also help protect the user's right of self-determination in the traditional "consent rule" system. At the same time, at the technical level, it provides guarantee for the application of intelligent technology after cloud blocking, so that users can continue to use interactive functions without connecting to the cloud, so as to fully ensure the release of scientific and technological benefits.

4.4. Construction of Comparative "Antidiscrimination" Rules. The secondary infringement of artificial intelligence on the right to privacy is the secondary application of the data processed according to the stolen privacy information data. It mainly includes economic behaviors such as structural discrimination and illegal behaviors such as selling information. However, the sale of private information has strict norms such as Article 253 of the criminal law, so it is more necessary to explore the norms of structured discrimination. As mentioned above, structural discrimination is in the normative blank area of civil law and economic law (Anti Unfair Competition Law) in China at this stage, because in terms of civil law privacy, the data on which discrimination is based is processed secondary structured data. In terms of anti-unfair competition law, there are no relevant norms to regulate it, and there are no corresponding standards. In January 2021, the China Consumer Association proposed to add relevant provisions on intelligence and algorithm application to specifications such as price law, which shows that China has not established a corresponding standard system at this stage. Therefore, China should set antidiscrimination rules in the digital field, and the main principles and operational standards should focus on comparability.

Taking the killing of ripening according to personal privacy data as an example, the killing of ripening behavior

RETRACTED

uses artificial intelligence technology to analyze personal consumption preferences and other privacy data and provide dynamic low prices for privacy owners. It is necessary to judge whether there is discrimination in their behavior through comparison. We should take comparability as the central principle and time, space, and region as the standard to analyze whether there is unreasonable dynamic pricing behavior of network service providers with intelligent technology as the core and set the corresponding proportion red line. When the proportion is exceeded, it can be judged that there is secondary privacy infringement and discrimination. Finally, we should set the rule of inversion of burden of proof at the judicial level and set corresponding punishment measures for secondary infringement.

5. Conclusion

The human rights to privacy and privacy protection system have experienced multiple baptisms of technological development, and at this stage, a relatively mature system, laws, and regulations and the portrait privacy system formed by the development of social civilization have gradually formed. As technological innovation enters the era of intelligence and data, new technological factors not only provide dividends for social development and operation efficiency, but also promote the innovation and development of privacy protection system and related theories in China and even the world as a core driving force. In this process of innovation and development, we should firmly grasp the balance and boundary between the release of technological functional value and the protection of human rights, which is not only the new requirements and challenges brought by technological "destructive innovation," but also the continuous game between natural human rights and social development. In this study, cloud space and intelligent technology based on deep learning algorithm and artificial intelligence have been gradually integrated into the life and social operation structure of natural people, and the application technology has been gradually skilled, and the trend of deep integration has been gradually highlighted. Make it better realize the protection of privacy. So as to solve the dilemma and protection of privacy protection. At the same time, as the most important and difficult legal issue in this development trend, the protection of the right to privacy is the first barrier to the further development of human civilization. Therefore, it is the right and obligation of every citizen to protect their privacy through legal means, so as to better protect our digital privacy in the era of big data.

Data Availability

The data underlying the results presented in the study are available within the manuscript.

Disclosure

The authors confirm that the content of the manuscript has not been published or submitted for publication elsewhere.

Conflicts of Interest

The authors declare that there are no potential conflicts of interest in our paper.

Authors' Contributions

All authors have seen the manuscript and approved to submit to your journal.

References

[1] D. Louis, *Brandeis the Right to Privacy*, p. 12, Peking University Press, Beijing, China, 2014.
[2] R. Blanca, *Ritz Privacy in Electronic Communication,* p. 6, Shanghai Jiaotong University Press, Shanghai, China, 2017.
[3] H. Wu, "Du Yanyong Ethical governance of artificial intelligence: from principle to action," *Research on Dialectics of nature*, vol. 37, no. 4, pp. 49–54, 2021.
[4] X. Li, "Technical science and ethics of artificial intelligence," *Social Science Forum*, vol. 25, no. 4, pp. 179–203, 2019.
[5] Y. He, "Governance of intelligent society and construction and proof of risk administrative law," *Oriental Law*, vol. 32, no. 1, pp. 68–83, 2019.
[6] H. Wu, "Institutional arrangement and legal regulation in the era of artificial intelligence," *Legal Science (Journal of Northwest University of Political Science and Law)*, vol. 35, no. 5, pp. 128–136, 2017.
[7] Q. Wang, "Legal regulation path of artificial intelligence: a framework discussion," *Modern law*, vol. 41, no. 2, pp. 54–63, 2019.
[8] X. Zhang, *Legal protection of Privacy*, People's publishing house, Beijing, China, 1997.
[9] L. Yang, "The role of civil liability in risk control of artificial intelligence development," *Journal of law*, vol. 40, no. 2, pp. 25–35, 2019.
[10] X. Dai, "Dimension expansion and topic transformation of data privacy: from the perspective of legal economics," *Jiaotong University Law*, vol. 26, no. 1, pp. 35–50, 2019.
[11] S. Cheng, "Ten philosophical challenges of intelligent society," *Exploration and contention*, vol. 30, no. 10, pp. 41–48, 2017.
[12] C. Li, "Legal governance of artificial intelligence discrimination," *Chinese law*, vol. 35, no. 2, pp. 127–147, 2021.
[13] S. Huang, "Artificial intelligence and intelligent sociology," *Gansu Social Sciences*, vol. 45, no. 5, pp. 56–62, 2019.
[14] H. Qi, "Is the right of privacy out of date -- the dilemma and Countermeasures of privacy protection in digital society," *Journal of Changsha University of Technology (Social Science Edition)*, vol. 37, no. 2, pp. 104–114, 2022.

RETRACTED