A Review of International Models of Consumer Personal Information Protection in the Digital Economy Era: The EU and the US as Examples

Xiangdi Kong¹,²*, Ziqian Wang¹, Kunpeng Song¹,³

¹School of Law of Shandong University of Technology
²The Second Council of the Ecological Law and Economic Law Research Society of Zibo Law Society
³Shandong Zhityouth Law Firm

*Correspondence Author

Abstract: In the era of digital economy, countries and regions around the world have further strengthened the protection of personal information, especially consumer this special group personal information protection. Throughout the development of personal information protection in various countries, it is easy to find that the laws and regulations related to personal information protection that have been enacted and are being enacted by various legislatures are gradually showing a trend of unified legislation and unified regulation. One of the most representative of the EU is particularly strict, and the US consumer personal information protection system is increasingly perfect.

Keywords: Digital economy, Consumers, Personal information protection.

1. Introduction

With the widespread application of new computer technologies such as cloud computing, big data and 5G, social and economic life has undergone radical changes. With the catalytic effect of digital technology, data has become one of the most important factors of production for the current development of human society. Especially, the current rampant global new crown epidemic has prompted the accelerated arrival of the digital economy era. The widely used big data has brought great convenience to the economy and society, but also pushed the protection of personal information to the limelight. As a result, countries and regions around the world in the strategic highland of preemption data at the same time, also from the perspective of enhance the competitiveness of information industry as a whole, further strengthens the protection of personal information, especially the personal information of consumers. In this context, it is necessary to study the protection of personal information from a global perspective and to deconstruct the international experience on the protection of consumers’ personal information with Chinese wisdom, especially for the current fully open national situation.

2. Current Status of International Legislation and Regulation of Personal Information Protection

In order to protect personal information, especially consumer personal information, various countries and regions have issued laws such as Personal Information Protection Law, Data Privacy Law or Data Protection Law. From the perspective of the world, in the 50 years from 1970 when Germany promulgated the world’s first Data Protection Law to December 2020, 63% of countries or regions in the world have promulgated laws such as Personal Information Protection Law, Data Privacy Law or Data Protection Law. And the number of countries and regions that have enacted Data Privacy Laws has increased by 10% from 2019 to 2020 alone[1].

In general, the laws and regulations related to the protection of personal information that have been enacted and are being enacted by various legislatures are increasingly showing a trend of unified legislation and unified regulation. Taking some countries in Europe, America and Asia as examples, although each country takes protective measures for personal information from different paths and according to local conditions, they basically follow the same protection principles, namely, the principle of openness, the principle of restriction, the principle of quality, the principle of security and the principle of rights protection.

However, due to the different legal systems and social environments, looking at the global practice of personal information protection legislation and supervision, the legislation of personal information protection can still be roughly divided into two categories. One is the countries and regions of civil law system, mainly represented by the European Union. The typical feature is that it is based on the right of self-determination of personal information and raises personal information to the right of personality, Formulate unified and strict specifications for information collection, processing, processing and use; and set up a special personal information protection organization for strict supervision; The other is the countries of the common law system, such as the United States. Compared with the civil law system, the countries of the common law system pay more attention to the fairness of practice, take the right of personal privacy as its basic concept, and take it as the basis of constitutional rights, and then form different types of legal norms for different fields. In addition, other countries and regions have continued to explore their own personal information protection practices based on the practices in Europe and the United States, and have continued to improve them with the development of information technology.

DOI: 10.53469/jssh.2022.4(03).10

www.bryanhousepub.org
3. The EU Consumer Personal Information Protection Model

3.1 Overall Characteristics of EU Consumer Personal Information Protection Model

As a multi-national alliance organization, the EU has a complex rule of law environment, and it is difficult to truly integrate between countries governed by their own interests. The EU, which is committed to building integration, put forward the concept of data protection in order to reverse its weak position in the global race of digital economy. It also elevated the right to personal information to the level of a fundamental right, and has since set a legal trendsetter for the protection of personal information worldwide.

In terms of the overall legal model, the EU’s personal information protection model tends to be uniform and strict, and it has implemented uniform protection and regulatory standards for the handling of personal information including government departments and various commercial sectors. In the 1970s, various EU member states, such as Germany and Sweden, established uniform domestic legislation for the protection of each individual’s information one after another. At the stage of promulgating the EU Directive on the Protection of Personal Data in 1995, each EU member state began to follow the principle of seeking common ground while reserving differences in the protection of personal information, developing to the establishment of the status of personal information protection as a fundamental human right in the EU Constitution in 2009, and then to the implementation of the General Data Protection Regulation in 2018, all reflecting the legislative and regulatory characteristics of EU countries tending to unification and integration in the field of personal information protection.

3.2 The General Data Protection Regulation, the Strictest Personal Data Protection Act in the EU

In terms of legal structure, EU legal documents related to the protection of personal information are generally formulated as a series of directives, rules or guidelines from the dual regulatory dimension of EU harmonization legislation and domestic laws of member states. Among them, the General Data Protection Regulation has the most profound impact. From the introduction of the draft in 2014 to the official entry into force in 2018, it is an important milestone that rests of the EU as a whole than on the member state. The General Data Protection Regulation reinforced the right of data subjects to control their personal information in the form of uniform legislation, and since then, a culture of information privacy around rights-based dialogue has prevailed. However, from the early 1970s to the General Data Protection Regulation, a number of legislative and regulatory initiatives in the EU have focused more on safeguarding the interests of the EU as a whole than on protecting the interests of citizens.

The first paragraph of the General Data Protection Regulation begins with the two core tasks of “protecting personal data rights and promoting the free flow of data”, which are benchmarks in the global context[3]. In terms of scope of application, it applies to data controllers in the EU as well as having extraterritorial effects, and the most important feature of the General Data Protection Regulation is actually its unprecedentedly strict penalties, but its risk-oriented design of legal provisions, in which anonymization and de-tagging and other technical means not only to solve the problem of information security but also to provide support for personal information and corporate data compliance review. This forces operators to pay attention to the issue of consumers’ personal information rights. In terms of the relief of consumers’ personal information, the General Data Protection Regulation adopts a two-step mode of first filing a complaint to the information regulatory agency, and then filing an appeal to the court for reconsideration or judicial review. Meanwhile, in the process of information transfer, consumers are given the right to choose, carry and be forgotten, so as to strengthen their control over their personal information. It opens up more relief paths for consumers when their rights are infringed.

However, the European Commission has disclosed that although the General Data Protection Regulation has made many breakthroughs and founding constructions in the protection of personal information, there are still unavoidable limitations in its actual operation, and we cannot ignore its negative impact on EU enterprises and even the overall economy of the EU. First of all, the enactment and enforcement of the law has aroused citizens’ deep concern about their information and data rights, and after the battle of rights has been waged, information processors and collectors cannot effectively reduce the increasing costs even if they continuously update their data and information capture technologies, especially for those who specialize in analyzing consumers’ specific preferences by collecting and analyzing user data information, and then developing accurate push ads for various businesses. The cost of compliance is increasing at a much faster rate than the profit margin for technology companies. Although the General Data Protection Regulation empowers data subjects to a certain extent to improve consumers’ sense of data security, the economic interests of the companies that make a living from it inevitably suffer, which to a certain extent hinders the flow and sharing of information in the market. Next, strict laws and regulations are often implemented by imposing huge fines. Such punishment mode will deter enterprises with illegal behaviors to some extent, but it is difficult to solve the phenomenon of consumers’ personal information being illegally infringed reasonably and effectively, because it is difficult for enterprises to avoid transferring the cost of their losses to consumers after receiving high fines. So the final loss is exactly is which side is not clear. Finally, ignoring the specificity of the industry and paying too much attention to the protection of personal information will easily lead to uneven allocation of market resources. The retarding of the popularization of new technology due to the uneven distribution of industry information will become the main reason for restricting enterprises’ in-depth business expansion, and the innovation vitality of emerging enterprises will also be greatly affected, which will increase the difficulty of protecting consumers’ personal information.

4. The US Consumer Personal Information Protection Model

4.1 Overall Characteristics of the US Consumer Personal Information Protection Model

In terms of application, it applies to data controllers in the EU as well as having extraterritorial effects, and the most important feature of the General Data Protection Regulation is actually its unprecedentedly strict penalties, but its risk-oriented design of legal provisions, in which anonymization and de-tagging and other technical means not only to solve the problem of information security but also to provide support for personal information and corporate data compliance review. This forces operators to pay attention to the issue of consumers’ personal information rights. In terms of the relief of consumers’ personal information, the General Data Protection Regulation adopts a two-step mode of first filing a complaint to the information regulatory agency, and then filing an appeal to the court for reconsideration or judicial review. Meanwhile, in the process of information transfer, consumers are given the right to choose, carry and be forgotten, so as to strengthen their control over their personal information. It opens up more relief paths for consumers when their rights are infringed.
Information Protection Model

The protection of personal information in the United States is based on the concept of “privacy”, and there is no comprehensive privacy protection law, but rather a decentralized legislative model, in general, the US privacy protection system is more effective and flexible, and its advancement is reflected in the fact that the US not only establishes data protection standards in the field of public law in the form of statutory law, but also sets restrictions and protection obligations for users of information data in the field of private law. Based on the basic protection principles of “specific purpose, openness and transparency, and protection of rights and interests”, the US has enacted separate legislation for personal information of government departments and commercial sectors, and has made use of its judicial remedy system, especially the Federal Trade Commission, the Federal Communications Commission, the Consumer Financial Protection Bureau, etc., as a basis for the protection of privacy. The Federal Trade Commission, the Federal Communications Commission, and the Consumer Financial Protection Bureau are the agencies that regulate and enforce the law in order to achieve the goal of protecting consumers’ personal information. Among them, the Federal Trade Commission has assumed most of the functions of protecting consumers’ privacy.

On the whole, the US differs from the EU’s preventive model of enacting laws beforehand, but adopts the post-facto enforcement and punishment and litigation compensation to deter unlawful business practices, which is the main reason for its flexibility, and also has reference significance in responding to consumers’ constantly updated demands. In particular, the US is not as strict as the EU in dealing with new industries that may be touched by the privacy protection process, and instead chooses to rely on industry self-regulation to solve the problem more cautiously.

4.2 The California Consumer Privacy Act, an Important Link in the US Information Privacy Protection Legal System

In the US, the boundary between the right of personal information and privacy was unclear at the beginning, and the right of information privacy was elevated to a constitutional right. The judicial mode of “finding one and solving one” gradually enhanced the market discourse power of information subjects until the Consumer Privacy Bill was passed in the Obama administration. The FTC proposed the ideal principle of “consumer consent” for the first time in the process of law enforcement, and adopted the protection framework of “notice-consent” for the protection of consumer information. State legislature, however, are the first to focus on to protect the privacy of consumer information excessive caused the increase of operating costs related to, in order to better promote based on the data of the emerging industry development and innovation, and not make social members into privacy and precision marketing, the parliament will be the focus of the privacy protection of California transferred information circulation link. In 2018, the California Consumer Privacy Act, which will take effect in 2020, has become the most stringent regional act related to information privacy protection in the United States and an important link in the legal protection system of information privacy in the US.

The California Consumer Privacy Act shall be under the jurisdiction of the principle of concise and focused, the jurisdiction of the main range of entities including California region to profit as the main purpose to collect processing data information of enterprises, through the study of the specifications of relevant enterprises and the consumer empowerment, to strengthen the consumers’ personal information control rights, safeguard the rights and interests of consumers’ personal information. The California Consumer Privacy Act applies different principles to the collection and use of information. In the collection process, it applies notification doctrine, while in the use process, it applies notification consent doctrine. Moreover, the act also gives consumers the right to stop enterprises from selling their personal information at any time, that is, the right to opt out[4]. This clause to a certain extent, make up for the loopholes “notice - agreed to” protect the framework, is also because of its beyond the US used privacy protection act, so become the California consumer privacy act the terms of the most influential. To give consumers more autonomy, the bill also establishes the right to delete information[5].

Since the Enactment of the California Consumer Privacy Act, the US has achieved a transformation in the mode of privacy information protection. From the beginning of the focus on the commercial use of personal information value to focus on strengthening the protection of consumers’ information privacy rights and interests. But the US and the EU and other countries have the same dilemma, namely the balance between privacy and protection of the rights and interests of information needs and social enterprise innovation needs the contradiction between economic development, due to the California Consumer Privacy Act generally applicable to compared with the small and medium-sized enterprises, the content of the bill also tend to strengthen consumer rights, to increase the obligations of the enterprise, This undoubtedly increases the compliance costs and operating costs of enterprises. Although The California Consumer Privacy Act has implemented a moderate rule exemption system for the collection and utilization of personal information in specific industries and fields, it still cannot fundamentally solve the existing dilemma of global personal information protection. Nor can it balance the relationship between promoting the circulation of data information and protecting consumers’ information rights and interests.

5. Review of Consumer Personal Information Protection Models in the EU and the US

As the latest achievement in personal information protection, the EU seeks to achieve guidance on the institutional practice of member states through the General Data Protection Regulation, a unified act on the protection of personal information rights that is both economic and administrative in nature. Since the General Data Protection Regulation not only focuses on the infringement of public rights on personal information, but also does not ignore the infringement of private subjects, it is regarded as a comprehensive personal information protection mechanism by the EU, so it urges member states to implement it in accordance with the
requirements of the law. However, this kind of “one size fits all” coercive means deprives member states of their right to speak and ignores the particularity of the information legal environment of each member state, which may be hindered in the implementation stage of the system. The EU stresses “one-stop service” legislative principle, but too carefully is more likely to limit the provisions of the laws of the power, the digital age change speed, curing laws make it hard to adapt to change, and frequent repair method is detrimental to the authority of law, leading to protect personal information under the “old law” unable to respond to the new era of the personal information of the infringement behavior. Therefore, although the unified legislation of the European Union has strictly protected consumers’ right to personal information, it has restricted the free circulation of personal information, and its own lag makes it difficult for solidified regulatory measures to keep up with the pace of the information age.

The US law regards consumers’ right to know as the nature of personal information rights. Users may not have all the rights related to information, but they have a series of rights on information disclosure, such as the right to know and the right to consent, which makes it an embryonic form of personal information protection to some extent. The protection of American consumers’ personal information right is based on the right to privacy. As a defensive right, the protection mechanism can only be promoted when the actual damage result has been caused. It tends to be a kind of relief after the event, but neglects the timely protection before and during the event. Due to the separation of the federal and state levels, the two levels of legislation are independent from each other and appear to be lax, which also creates a block pattern to protect consumers’ personal information rights. No matter what the level of legislation is, there has not been a unified special act on personal information protection, but there are provisions related to personal information protection in some federal and state laws. It can be seen that the United States is concerned with the broad characteristics of legal protection of consumers’ personal information rights. At the same time, the US legislature believes that compared with private subjects, public rights are more threatening to personal information. Although it demarcates the public and private boundaries in the protection of consumers’ personal information rights, it obviously pays more attention to the standardization of public rights in the planning of defense measures. If it is implemented for a long time, it can indeed play a role in regulating the improper infringement of personal information rights by public power. However, due to its rigid emphasis on one corner and lack of overall centralized and coordinated perspective, it is likely to cause friction with private subjects in the application level of the system.

References


[4] California Consumer Privacy Act, & 1798. 120 (a) (b).