Know More, Suffer More

Analysis of the Big Data Discriminatory Price

Jiayi Kang[1], Chenlei Shen[2(✉)], and Yuchen Yue[3]

[1] School of Optoelectronic Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

[2] College of Mechanical Engineering, Jiangsu University of Technology, Changzhou 213000, China

18407249@masu.edu.cn

[3] College of Physical Education, Hunan Normal University, Changsha 410000, China

Abstract. Big data discriminatory price (BDDP) is a kind of misuse of data, where the platform "sets" the user up from the very beginning of the service contract with the user, actively taking the user's surplus for its own benefit in all aspects of information collection, analysis, and utilization. In recent years, the public has become more and more familiar with the concept of big data deception, but people are not sufficiently aware of the ways to defend their rights and are far from being aware of the rights of those who have been discriminated against. In addition to the public's anxiety, governments of various countries also attach great importance to platform infringements in BDDP. The European Union introduced the General Data Protection Regulation in 2018, and the United States has laws that apply to big data practices, including the Fair Credit Reporting Act, the Fair Chance Act, and the Federal Trade Commission Act. China is later than Europe and the US in terms of legislation, having introduced the Personal Information Protection Law of the People's Republic of China and the Data Security Law of the People's Republic of China in 2021, but still confronts many problems in practice, such as the unclear scope of application and unclear related concepts, which need to be flexibly solved by combining more judicial practices and domestic and international experiences. In this paper, we put forward proposals for regulation in terms of departmental supervision, industry self-regulation, and individual rights protection, with a view to forging a better online ecological environment.

Keywords: big data discriminatory price · dynamic price · price discrimination · information security · privacy protocols · algorithmic techniques

1 Introduction

Under the mobile internet circumference currently, users get convenient services through mobile apps and complete various transactions online. Before accessing these services, users are required to submit personal information, sign a privacy agreement, and open relevant permissions, which is a normal process. However, there have been numerous

Jiayi Kang, Chenlei Shen, Yuchen Yue—authors contributed equally.

G. Ali et al. (Eds.): ISEMSS 2022, ASSEHR 687, pp. 3128–3139, 2022.
https://doi.org/10.2991/978-2-494069-31-2_367

reports in recent years of "big data" being used to abuse user profiles, such as analyzing users' consumption records, browsing records, and even identifying the model of mobile phone used by users through algorithms [1], and making automated decisions based on illegal or other normatively unacceptable factors and reasoning under a certain opaque algorithm rule [2]. Such decisions may appear to have been made with the user's "consent", but they clearly violate the user's right to privacy, information, even choice, then run counter to the user's expectation of using the service and the platform's original intention of providing it. So, where does the disagreement between users and the platform over personal data and privacy originate, and where are the hidden threats buried? What are the legal loopholes and business logic that allow platforms to secretly utilize algorithmic technology to violate users' rights and interests, and what are the legal loopholes and business logic that allow this to happen?

Case texts and questionnaire data are used to examine the evolution, regulation, implementation, and character of big data murders. Insufficient regulation and strong economic worth of big data were cited by 26.28 percent and 21.79 percent of those who completed the survey as the major causes for "big data ripening," respectively. Furthermore, it can be shown that after being exposed to "big data," most users choose to reflect on the platform. The platform's "big data killing" exploits unlawfully gathered user information to breach users' legal rights and interests with the use of algorithms and technological black boxes, and hastily takes customers' excess, according to the study of the cases and texts. The necessary provisions give full play to government agencies' roles in protecting individual rights and grievances. According to statistics, "overdrawn consumer trust and lowered company credibility" account for 20.51 percent of the repercussions of "big data killing," making it the primary dispute between businesses and consumers currently, implying that big data killing reduces societal welfare. Big Data, in other words, is lowering societal wellbeing and causing discriminatory and unpleasant issues. Because this is a long-standing issue, restructuring the existing system, developing new procedures, and adopting targeted solutions and steps to solve the present issues would surely defend consumers' lawful rights and restore a clean trading environment on platforms.

In terms of the article's structure, the research first collects and summarizes existing literature, then analyzes the types, target objects, processes, and nature of big data killings in order, and proposes solutions and recommendations from the perspectives of platforms, governments, and users, based on the existing research results.

2 Literature Review on BDDP

2.1 Questionnaire Survey on BDDP

In a March 2019 interview study on BDDP, the Beijing Consumers Association found that 88.32 percent of respondents thought discretionary was a widespread phenomenon, and no one thought it didn't exist. According to the survey, 26.72% of those who had experienced "ripening" chose to file a complaint with the appropriate authorities or consumer organizations, 11.71% chose to argue with the merchant and demand compensation, 8.13 percent chose to expose it on social networking sites or in the media, and the rest took it in stride and admitted to their own misfortune.

In September 2020, Hummingbird Questionnaire conducted a questionnaire survey on people's experience and perception of BDDP, the results showed that in terms of personal privacy scope, respondents considered information such as name, age, weight, social networking platform, and portrait not particularly private; in terms of information leakage channels, online registration, personal operation, and email were considered the main ways; for the "Online Travel The Interim Regulations on the Management of Online Tourism Services", which was just introduced in August, 48.24% of respondents believe that the regulations will effectively alleviate the problems of private security and big data killing, while 7.04% believe that the regulations will not play an effective role.

2.2 Research on BDDP and Legal Regulation

Some researchers argue that considering the introduction of the Personal Information Protection Law and the experiences and shortcomings of legislation and practice in the European Union and the United States of America about the abuse of "big data to kill familiarity," it is possible to regulate Internet platforms from the perspectives of personal information protection and algorithmic regulation. The law also establishes guidelines for algorithmic computing before, during, and after the procedure. The rules should define the criteria for evaluating "substantial effect" under the legislation, clarify the platform's need to explain and preserve the individual's right to appeal and consider the complexity of implementing the right to data portability [3].

Scholars have debated the notion and nature of "big data killing" before making further recommendations. They clarify that big data killing is an abuse of citizens' information and that big data killing is a monopolistic act that takes advantage of market position in his study of the legal aspects of big data killing, with more analysis of the monopolistic nature of big data killing in the section on recommendations [4].

Some academics, on the other hand, advocate for regulation from the start of platform-user conflicts. Big data killings violate consumers' right to fair commerce. First, when a user signs a service contract with a platform, the platform forces the user to accept or reject all of the contract's treaties via a "click contract"; second, after gathering as much information as possible about the user, the platform will exploit the "information imbalance" via algorithms or technical black boxes; second, after gathering as much information as possible about the user, the platform will exploit the "information imbalance" by using algorithmic or technological black boxes to capture the user's benefits; additionally, the platform will use this opaque algorithmic technology to constitute price discrimination by forcing the user to enter into a transaction at an algorithmically regulated price. As a result, this research suggests three countermeasures: controlling algorithmic prices, rectifying information imbalances, and regulating click-through contracts [5].

The relevant departments have also responded positively to the voices of scholars. The Chinese National Development and Reform Commission and nine other departments issued "Several Opinions on Promoting the Standardized, Healthy, and Sustainable Development of the Platform Economy" on 19 January 2022, and the "Regulations on the Administration of Algorithmic Recommendation of Internet Information Services" went into effect on 1 March this year, drawing a lot of attention from the academic

community. According to some industry insiders, future algorithm regulation will be more professional and technical, allowing for the technology's operational practicality.

3 An Analysis of the Type, Process, and Nature of BDDP

Amazon chose 68 best-selling DVDs in September 2000 and differentially priced them depending on potential consumers' demographics, shopping history, browsing information, and other data. For example, Titus was priced at $22.74 for new subscribers and $26.24 for current customers, a difference of $3.50, resulting in a considerable gain in gross profit from the sale of these DVDs. The experiment, however, did not bring Amazon much sweetness, and it was just a month into it when a faithful Amazon user discovered that he had been screwed, followed by many frequent users who discovered the truth and came forward to protest Amazon, and the experiment failed [6]. However, this was only the start of the germination process, and big data killing has allowed this loss to be shown in a more variegated manner.

3.1 Types of BDDP and Target Audiences

3.1.1 Types of BDDP - An International Case in Point

The price of a product is determined according to market demand for the product and the purchasing power of the customer, which is a price adjustment policy inherent to the operation of a market economy for many years, and which originated from the dynamic pricing of airline tickets in the United States in 1980 [7]. However, as online platforms have become the main battleground for transactions, this pricing strategy has become an accomplice to merchants using information barriers to seize price decisions from consumers, as well as alleviating supply and demand conflicts and balancing opportunity cost differences, despite its lack of information symmetry and transactional transparency. Merchants may study consumers' price sensitivity and behavioral roll-ups by tracking real transactional data, and so alter their future marketing campaigns to capture more consumer surplus.

Merchants can match prices by comparing the model and operating system of the user's device algorithmically, and in 2012, travel website Orbitz was discovered to charge 30% more for Apple computer users than for other customers. The Wall Street Journal reported in 2012 that the website Staples offered varying rates based on the user's distance from the company's rivals. Users' purchasing history, browsing history, and spending patterns, including return frequency and price sensitivity, are used to price the most significant big data killers [8]. In 2014, a study led by Northeastern University in Boston discovered that major e-commerce sites like Home Depot and Walmart generally maintain prices based on the browsing history of independent customers, and the US Department of Transportation adopted a system that allows airlines and travel agents to collect information about travelers and offer personalized services based on their address, marital status, birthday, travel history, and other factors. This means that platform businesses will present different fares to different people based on this data.

3.1.2 The Target Audience of BDDP- an Example from Within China

The primary forms of big data to kill ripe may be summarized from international instances, thus big data to kill ripe target consumers are mostly aged users, member users, active users, and more costly equipment users [9]: March 2019, a netizen reported in Ctrip to buy air tickets, a short time to return to the operation, the software that no tickets, while other ticket prices are nearly 1500 yuan higher; December 2020, a netizen reported in Ctrip to buy air tickets, a short time to return to the operation, the software that no tickets, while other ticket prices are nearly 1500 yuan higher A netizen reported in December 2020 that Meituan members were “cutting leeks” and that the delivery fee for members was even higher than for non-members. The primary forms of big data to kill ripe may be summarized from international instances, thus big data to kill ripe target consumers are mostly aged users, member users, active users, and more costly equipment users: March 2019, a netizen reported in Ctrip to buy air tickets, a short time to return to the operation, the software that no tickets, while other ticket prices are nearly 1500 yuan higher; December 2020, a netizen reported in Ctrip to buy air tickets, a short time to return to the operation, the software that no tickets, while other ticket prices are nearly 1500 yuan higher A netizen reported in December 2020 that Meituan members were "cutting leeks" and that the delivery fee for members was even higher than for non-members.

3.1.3 Analysis of the Process of BDDP

BDDP is simply an infringement on the privacy of users’ personal information. Users must register and log in to key applications in their everyday lives, release required permissions, and bind personal information to access different services provided by the app in the context of the mobile internet. Users are frequently required to agree to privacy agreements including cryptic wording and long credit agreements as part of the permissions release procedure. Users must bypass the process of reading the agreements and achieve “formal contracts” with platform operators for convenience “due to different comprehension of users and the fact that such agreements are often set in abstract settings [10].” According to the survey, 35.80% of respondents decided to ignore such agreements. This implies that the user has no option but to accept the privacy agreement, and the privacy agreement’s content may be perceived as misinformed or imposed on the user.

According to statistics, after handing over information to a platform for storage and processing, 82.20% of users almost completely lose control over the information, making it difficult to monitor and manage how the information will be processed in the future. Some platforms will use this technical or algorithmic black box to leak user information privately to other individuals, platforms, or even outside the country, exposing a large amount of personal information. The value decreases; or a massive amount of user data is analyzed and collated, and different users are assigned rolls to gradually paint a user portrait; or even the personal privacy of users who have not disclosed their information to the platform is inferred through algorithmic analysis, allowing the platform to profit from the inferred data.

Following the basic classification of users, the platform can use "smart" algorithms to analyze each user's desire to buy goods, price sensitivity, and adjust prices through dynamic pricing, so that consumers can complete transactions at the highest acceptable price, thereby obtaining the full consumer surplus [11]; not only that, in some lending platforms, some users' private information can also lead to "price discrimination," preventing them from obtaining the normal borrowing.

3.2 Analysis of the Nature of BDDP

3.2.1 The Difference Between BDDP and Dynamic Pricing

Operators use big data to collect consumer information, analyze their consumption preferences, consumption habits, income levels, and other information, and sell the same goods or services to different consumers at different prices to obtain more consumer surplus. Many people confuse big data with dynamic pricing, believing that big data kills. Because operators "often modify pricing in reaction to changes in the pipeline, product, customer, and time, dynamic price modifications," consumers' experiences are harmed and information security is jeopardized. Operators use big data to collect consumer information, analyze their consumption preferences, consumption habits, income levels, and other information, and sell the same goods or services to different consumers at different prices to obtain more consumer surplus. Many people confuse big data with dynamic pricing, believing that big data kills. Because operators "often modify pricing in reaction to changes in the pipeline, product, customer, and time, dynamic price modifications," consumers' experiences are harmed and information security is jeopardized [12].

For example, instead of taking a taxi home late at night during rush hour, a user of a taxi app stays in the office, makes plans for when they get home, and then taps into the app when the roads are clear, successfully hailing a suitably priced car, which not only gets them home faster than their colleagues who left earlier but also completes many of their to-do tasks in a rather organized manner, thus providing user convenience.

Big data killing differs from dynamic pricing changes in that it infringes on customers' legal rights and even causes them to have a negative consumer experience. The reason for this is the opacity of the pricing mechanism, the black box of algorithms and technology that is not open to the public, and thus the ability of platform operators to seize low-cost information of users to bring them a mine of benefits, the use of relevant laws and regulations are not perfect, the lack of departmental supervision brought about by the grey area, with the algorithm formed under continuous progress for the user, but also for a platform operator, the use of relevant laws and regulations are not perfect, the lack of department. The party with the total technological and information advantage [13], on the other hand, surreptitiously breaches the contract in order to amass cash, control the industry, expand its territory, securely grip the user's information, steal the user's privacy, and increase the market. To achieve capital accumulation, or to monopolize the industry and expand its territory, the party with the absolute technological and information advantage secretly breaks the contract. To achieve capital accumulation, or to monopolize the industry and expand its territory, the party with the absolute technological and information advantage firmly grasps the user's information, steals the user's

privacy, even knows itself better than the user, "coerces" the user to "sacrifice" for its own benefit.

3.2.2 BDDP- First-Degree Price Discrimination

The practice of BDDP concerns issues of prejudice and perception of experience, in addition to weakening consumer rights, severely hurting company credit, and reducing societal welfare levels. In economics, “big data killing” refers to first-degree price discrimination, or complete price discrimination, in which corporations adapt pricing to each customer in order to capture the entire consumer surplus [14]. Merchants are increasingly using targeted pushes to consumers, window alerts, and other methods to achieve price discrimination at more fixed pricing. So, when transactions are not explicitly priced and information is not as interoperable between customers as it previously was, getting ripped off happens discreetly, even if merchants employ big data analytics to adjust pricing at a whim or diminish the degree of consumer welfare. Any customer who wishes to defend their rights fears that they will be unable to do so if they do not actively seek out another consumer to compare rates. As an example, as a regular user, a company employee could borrow $200,000 from a credit platform; however, the system analyzed his profile and discovered that he was a 35-year-old programmer who was not considered to have the ability to repay the $200,000 in a timely manner, so the system offered him a maximum amount he could borrow of less than $200,000, which was one form of price discrimination. The platform violated the user’s privacy by changing the borrowing limit without his authorization after analyzing his personal information, which affected the user’s interests and resulted in a poor user experience

4 How to Deal With It: The Way to Deal with Big Data Killing

Big data killing mainly includes three processes: the signing of privacy agreements, the processing of user information, and the occurrence of infringement.

4.1 Active Cooperation of the Platform

First, in terms of privacy agreements, most of the current agreements are in the form of “click contracts”, and users must accept all the terms if they want to obtain services. Although some information must be collected by the platform in accordance with the law, such as using the online travel APP to purchase a ticket, booking a hotel, the platform needs to identify the user’s identity information, including the documents, name and gender, nationality and birthday, etc., and also needs to obtain channel information to maintain communication with the user, such as contact numbers, etc., but there are still some contents in the agreement that involve sensitive information.

For example, for the personalized identification of users, the latest version of the Qunar APP privacy agreement (November 12, 2021) has a clause that “we may also know your travel plans, style, and preferences, including meal requirements…”. The platform did not highlight what the user was expected to know about the user’s personal preferences and personality traits in these conditions, which might have made it easy for even a comprehensive study of the agreement to ignore such elements.

At the same time, by summarizing the types of big data killing, it can be found that in addition to using the algorithm to analyze the user's consumption habits and personal preferences, so as to implement "killing", the platform also has the behavior of killing based on the user's device information, location information, and record information, which is also involved in the privacy protocol of Qunar APP, and the protocol of Qunar APP explains the collection of personal logs, including device information, search browsing and operation records, and the intention of collection. The instructions in the agreement are vague, "We provide you with security through this information, protect your personal and property safety from infringement, and better prevent security risks such as phishing websites, fraud, network vulnerabilities, computer viruses, network attacks, and network intrusions…", so why should we use this information to prevent risks, and how to use this information to prevent risks, the platform does not make any brief explanation of this.

Users are reminded of this and must agree to it in order to enjoy more convenient services. A general overview of the privacy agreement reveals that the terms and conditions of the information collection are filled with the statement "If you refuse to provide it, you may not be able to receive our customer service," and users must agree to it in order to enjoy more convenient services. All responders accounted for 72.54% of the total. As a result, the platform cleverly collected entries, but users were confused, originally hoping to obtain quality services, and did not want to become a knife fish meat.

Based on the analysis of the problems in the privacy agreement, the platform should:

(1) eliminate the "click contract". One-click consent is risky for users, it is not easy to express consent and supervision for the purpose and way of information processing, and it is necessary to maintain continuous communication with users in the future of the service, and it is not necessary to request consent only once.
(2) Request different permissions for users individually. Only basic personal information is collected when the user registers as a member or obtains the identity of a tourist, and only when the user applies for a service, the platform can obtain other information of the user after seeking consent, including sending a pop-up window and SMS reminder, and there should be a similar clause of "permission to use" in the reminder to the user and ensure that the user has the right to withdraw consent. It should be noted here that the platform can improve the personalized portrait of users through the process of providing services, under the supervision of the government, and use the information provided by users to enrich and three-dimensional users' Internet images, to provide users with more specific information and privacy protection under general rules, and make more efficient and personalized content recommendations [15].
(3) Streamline privacy protocols. Retain the most basic and necessary permission applications, and report to the relevant departments to review and approve the privacy agreements formulated by important Internet platforms in the industry.

For the algorithm processing after the information is collected, and the user's requirements for the interpretation of the algorithm to the platform, the platform should:

Fig. 1. Cloud of policy words

(1) Make a schematic diagram of algorithm processing process. Give the user a general impression of the process.
(2) Before and after the formulation of the algorithm interpretation template. Before the algorithm is implemented, the processing intention is actively explained to the user, and after the algorithm is processed, the interpretation service is actively provided to the user, and the specification of the interpretation is classified.

4.2 Effective Government Supervision

Figure 1 is a "word cloud" generated by using the word frequency query function of the text analysis software NVivo11 [16], as can be seen from Fig. 1, security, information, network, management, and data account for a relatively large proportion and are in the center of the diagram. It shows that the focus of the Chinese government's policy on the problem of killing big data is in these important dimensions.

The two new decrees promulgated in 2021: the Personal Information Protection Law of the People's Republic of China and the Data Security Law of the People's Republic of China have innovative and historical provisions in many aspects, but the official implementation time is still short, there are not many examples of penalties according to them, and there have been controversies over some of its regulations. For example, the Scope of Application of the Personal Information Protection Law is unclear in some cases: when discussing its extraterritorial effects, its "standard for the place where the processing takes place" and "the actual results of providing products or services to natural persons in China" cannot effectively regulate the processing of Chinese citizens' information outside China and the acts that infringe on the information security of

Chinese citizens when providing products or services to Chinese citizens [17]. As for the Personal Information Protection Law and the Data Security Law, neither of them provides legal support for the user's claim that the user submits an algorithmic explanation to the operator: before or after the infringement occurs, there is no specific description of what form the operator should provide, and what content can effectively solve the user problem.

In terms of government regulation, existing studies all believe that there are legislative, judicial, and regulatory problems in the field of big data killing. Relevant departments should:

(1) Establish a long-term expert group on the issue of "big data killing". Focus on the shortcomings of existing legislation, conduct judgment and implementation analysis of typical cases, and put forward targeted improvement opinions.
(2) Step up the formulation of special laws or regulations. Combined with judicial practice and actual conditions, adopt the opinions of discussion, amend some of the provisions of the current law based on judicial time, and supplement more detailed regulations for new types of infringement, including the judgment of automated decision-making, the specific interpretation of the right to interpret algorithms, try to confirm the rights of data, and make it more frequent and newer.
(3) Establish or designate specialized agencies to carry out supervision work. Specialized agencies clarify their responsibilities and make stricter judgments on big data killing behavior in accordance with existing laws and regulations [18]. Adhering to the purpose of protecting the weak, try to determine responsibility on the "principle of no-fault liability". At the same time, we will try to establish a technical supervision mechanism [19] for the platform processing process and cultivate more relevant talents to help build a mechanism.
(4) Explore decentralized convergence. Now there is also a discussion between blockchain technology and the current credit system, and the government should increase its efforts to support the development of high-end technologies such as blockchain, help solve the technical problems that restrict development, thereby enriching the credit system, and actively study the integration of decentralized ideas with the current system [20].

4.3 Users Actively Protect Their Rights

In terms of personal rights protection and appeal, users should:

(1) Understand the rights protection pipeline. From the results of the questionnaire survey, consumers are still not very clear about the channels of rights protection, and various media or platforms should actively publicize and popularize this kind of key knowledge.
(2) The facilitation of proof is guaranteed. In the existing cases, there are many complaints of big data killing, the specific reason is insufficient evidence, the court is difficult to determine whether the platform behavior constitutes big data killing, if you want to protect the right of consumers to appeal, you must ensure the convenience of collecting evidence, which also requires the platform to actively disclose

some of the necessary background data, which can also become the basis for the platform to defend or appeal while facilitating consumers to add evidence.

5 Conclusion

The phenomenon of big data killing originated at the beginning of this century, and there are different types of classic cases and legal texts at home and abroad. The case and text are summarized and analyzed, the target group is surveyed, and the type of big data killing mainly includes the platform to analyze the price of the user's use of the device, the user's geographical location, the distance between the user and the competitor, the browsing consumption record left by the user, the user's consumption habits, etc., label the different groups of people, and then adjust the pricing through the algorithm, so the target users of the big data killing are mainly the old users of the platform, member users, active users, and users with more expensive devices.

Through the study of the whole process of big data killing, the concepts of "dynamic pricing" and "price discrimination" involved in big data killing, it is recommended that the regulatory side try to set up a special agency and innovate the regulatory mechanism; Platform enterprises fully cooperate with departmental supervision, actively rectify problems in privacy protocols and algorithm collection, actively disclose some algorithm data, and improve user personalized portraits; Individuals should establish a sense of rights protection, understand the ways to protect rights, and actively protect their own information privacy and security; In terms of system, it can promote the development of blockchain technology, solve related technical problems, and explore its integration with the current credit system to break through the bottleneck of regulation.

In the process of research, many materials, literature, texts, and cases were consulted, supplementing the knowledge, and understanding of relevant principles and legal practices, and doing our best to use the knowledge and experience learned to write papers. This process recognizes the lack of knowledge reserves and writing experience, and the collection of case texts is still limited, and there are problems with insufficient depth in analysis. In the future, I hope to learn richer principles and knowledge, combine the research thinking of different disciplines, learn more practical cases and put forward useful insights and effective solutions for new problems that have evolved with the development of the times from a more professional perspective.

References

1. P. Chen, An Exploration of Data Protection Path under Automated Decision-making [J]. Internet World,2021,(10): 12–17.
2. X.D. Ding, Automated Decision Making Based on Trust: Reflection on the Principle of Algorithmic Interpretation Power and Institutional Reconstruction [J/OL]. Chinese Jurisprudence: 1–20 [2022-03-02].
3. Y.F. Jin, W. Kelly, T.H. Zhang, Legal Regulation of "Big Data Killing" from the Perspective of the Personal Information Protection Law, Journal of Zhejiang Sci-Tech University (Social Science Edition), 2021, 98–106
4. M.H. Shi, " Research on Some Legal Issues of "Big Data Killing" [J]. Cooperative Economics and Science and Technology, 2022(04): 190–192.

5. Y.C. Hu, Y.F. Feng, An Inquiry on the Protection of Consumers' Right to Fair Trade in the Killing of Big Data [J]. Journal of Shaanxi Normal University (Philosophy and Social Sciences Edition), 2022, 51(01): 161–176.
6. Y.M. Chen, J.P. Li, M. Schwartz, Competitive differential pricing [J]. The Rand Journal of Economics, 2021, 52(1):
7. M.S. Lewis, Identifying Airline Price Discrimination and the Effect of Competition[J]. International Journal of Industrial Organization, 2021 (prepublish):
8. Y.L. Liu, On the anti-monopoly regulatory system of big data "killing" behavior[D]. South China University of Technology, 2020.
9. Q. Liu, Legal Regulation of "Big Data Killing" Behavior of E-commerce Platform Operators[D]. Zhongnan University of Economics and Law, 2019.
10. N. Naeem, Manifestation of Consent in Clickwrap Agreements[J]. Faṣlnāmah-i Pizhūhish-i Huqūq-i Khuṣūṣī, 2017, 5(17):
11. H. Jason, S.C. Wirasinghe, J.D. Hunt, Bus headway optimization with consumer surplus as a measure of societal benefit [J]. International Journal of Urban Sciences, 2021, 25(1):
12. R. Steppe, (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective. Computer Law & Security Review, 33(6), 768–785.https://doi.org/10.1016/j.clsr.2017.05.008
13. B. Michael, Economics and the Theory of Games [M]. CRC Press: 2019-09-18.
14. W. Liu, S. Long, D. Xie, Y. Liang, J. Wang, (2021). How to govern the big data discriminatory pricing behavior in the platform service supply chain? An examination with a three-party evolutionary game model. International Journal of Production Economics, 231, 107910.
15. Y. Liu, Construction of personal information protection system for algorithmic consumers in digital society[J]. Guangdong Social Sciences, 2022, (01): 261–271.
16. H. Wen, Attention Measurement—of the Chinese Government's Promotion of Basic Public Services Based on Text Analysis of the Work Report of the Central Government (1954–2013) [J]. Journal of Social Sciences of Jilin University, 2014, 54(2): 20–26, 171.
17. H.Q. Yang, J.Q. Che, Extraterritorial Effects of the Personal Information Protection Law[J]. Legal Person, 2020, (12): 78–81.
18. J.D. Qiu, Y. Wang, " Data-Wisdom Decision Model: Theoretical Construction Based on Big Data [J]. China Soft Science, 2018, (12): 17–30.
19. Z.B. Xu, Z.Y. Feng, X.H. Guo, D.J. Zeng, J.Q. Chen, Frontier Issues of Big Data-Driven Management and Decision-making[J]. Management World, 2014,(11): 158–163.
20. X.H. Chen, Analysis of Technology Integration and Applied Innovation Trend in the Era of Digital Economy [J]. Journal of Central South University (Social Science Edition), 2018, 24(05): 1–8.