Singapore Journal of Legal Studies
[2024] 276–305

REGULATION OF ALGORITHMIC DECISION-MAKING IN CHINA: DEVELOPMENT, PROBLEMS AND IMPLICATIONS

Wang Menglu*

In China, algorithms have been increasingly used in many different sectors to facilitate analysis of massive data and optimise the decision-making process. While this approach brings significant benefits, the complex design of algorithmic models and the large scale of data involved pose serious challenges to the existing regulations. In response, China has gradually established a regulatory regime covering many areas of law, such as rules governing personal information protection and algorithm recommendation services, to oversee the development and use of algorithmic decision-making. However, China's regulatory regime is not without its limitations. Drawing on the regulatory experience of overseas jurisdictions, including the EU, the US, the UK and Singapore, this paper makes some suggestions for improving Chinese regulations. It is worth considering formulating specific requirements for data used in algorithmic decision-making and complementing the existing regulatory regime with algorithmic audit mechanisms. China is also advised to strengthen private and public enforcement and incorporate the code of ethics into the governance structure of algorithmic decision-making.

I. Introduction

Given advances in computing power and data aggregation, algorithms have been increasingly involved in decision-making systems over the past few years. This innovative decision-making approach has significant impacts on different aspects of life, such as access to financial services, online advertising, employment and judicial decisions. In China, the development of algorithmic decision-making is largely driven by private-sector technology firms with strong analytical capabilities and troves of data. Taking conventional credit assessment as an example, the heavy reliance on manual review and the lack of financial data lead to difficulties in evaluating potential risks and the repayment capability of small businesses.[1] The use of algorithms facilitates the analysis of customer data from diverse sources and provides better risk management tools, thus improving the credit assessment process. In the public sector, Chinese courts have initiated pilot projects to integrate algorithms into the judicial system, introducing intelligent models to review relevant evidence,

[*] Post-doctoral Fellow in Digital Finance and Sustainable Development, Faculty of Law, The University of Hong Kong. I thank the Hong Kong Research Grants Council Senior Research Fellowship Scheme (Project Code: SRF2021-7H01) for financial support.

[1] Hong Kong, Hong Kong Monetary Authority, *Alternative Credit Scoring of Micro-, Small and Medium-sized Enterprises* (2 November 2020) at 15–17.

offer suggestions on how to try a case, and check the consistency of judgments.[2] Algorithms have revolutionised the way that different players in the private and public sectors make their decisions and present great opportunities for innovation in many areas.

While algorithms bring important benefits to the decision-making process, there is growing concern about algorithmic bias, opacity and errors. Given the complex design of algorithmic models and the scale of data involved, the existing regulatory regime that is primarily developed to oversee human decision-making is inadequate to mitigate potential risks associated with the use of algorithms. In effect, the accountability mechanisms and legal standards designed for the decision-making process have not kept pace with technological changes in the market.[3] The fundamental problem is how to ensure that algorithms can perform tasks as expected while protecting the rights and interests of customers in the automated decision-making process. In China, the Personal Information Protection Law issued in 2021 stipulates key principles and personal rights in relation to information processing, and introduces specific requirements for automated decision-making and its impacts on individuals.[4] There is also a set of rules governing the provision of algorithm recommendation services.[5] These laws incorporate different measures to regulate the development and use of algorithms, and require service providers to ensure transparency, fairness and security in the decision-making process. However, China's regulatory regime is not without its problems, such as the limitations of data protection rules, inadequacies of the algorithmic transparency principle and challenges in safeguarding the rights of individuals affected by algorithms. It is thus important to assess these regulatory responses in China and make some suggestions for improvement.

The remainder of the paper proceeds as follows. Part II will discuss the basic concepts and workings of algorithmic decision-making, and identify several problems associated with the process. As finance is one of the most digitalised industries and is heavily influenced by algorithms, this part will take the finance industry as an example to explain related issues in detail. Part III will focus on the development of China's regulatory regime for data-related issues and algorithmic decision-making. Part IV will critically examine the strengths and weaknesses of these regulatory responses by comparison with the experiences of some overseas jurisdictions. Part V will put forward suggestions for improvement of the regulatory regime. The last part will conclude.

[2] Rachel E Stern, Benjamin L Liebman, Margaret E Roberts & Alice Z Wang, "Automating Fairness? Artificial Intelligence in the Chinese Court" (2021) 59 Colum J Transnat'l L 515.

[3] Joshua A Kroll, Joanna Huey, Solon Barocas, Edward W Felten, Joel R Reidenberg, David G Robinson & Harlan Yu, "Accountable Algorithms" (2017) 165(3) U Pa L Rev 633 at 636 [Kroll, "Accountable Algorithms"].

[4] Personal Information Protection Law of the People's Republic of China 2021 [Personal Information Protection Law 2021].

[5] Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services 2021 (People's Republic of China) [Provisions on Algorithm-generated Recommendations 2021].

II. Algorithmic Decision-making and its Problems

With strong analytical capabilities and large customer datasets, algorithms are widely used in various areas to optimise the decision-making process, and show great potential in improving service efficiency and promoting business innovation. Despite these benefits, the complex design of algorithmic models and data-related issues have also raised growing concerns. Thus, this part will first analyse the basic concepts and workings of algorithmic decision-making and then map out some problems with their application in practice, setting the stage for a later discussion of regulatory responses.

A. *Basic Concepts and Workings of Algorithmic Decision-making*

In general, an algorithm is described as a set of rules to be followed when performing calculations or solving specific problems, which involves transforming inputs into outputs through a sequence of computational steps.[6] It is not just a method to process data, but a way of using machines to make decisions that would otherwise be made by humans.[7] Algorithmic models can filter data and select features that are considered highly relevant to decision-making, thus providing solutions in response to different needs.[8] They are designed to control increasingly advanced machines and replace humans at some junctures in complex decision-making processes. Given the widespread availability of data and improvements in computing power, algorithms have been used in a variety of industries and applications, such as controlling self-driving cars and assessing credit risks.

There are several major steps in designing an algorithm, including specifying a target variable, collecting and processing data, and developing a model through exposure to training data and feature selection.[9] Specifically, an algorithm designer first needs to clarify the purpose of the algorithm design and define a problem to be solved. In the area of credit assessment, the outcome predicted by an algorithmic model is customers' creditworthiness, which is treated as the target variable. The next step is to collect troves of customer data for training the algorithmic model in a certain way. Given the explosive growth in the volume and variety of data, algorithms are able to analyse various facets of borrower behaviour and thus make better-informed loan decisions.[10] After the training data is collected, inputs relevant to the target variable will be identified and assigned appropriate weights through

[6] Robert Sedgewick & Kevin Wayne, *Algorithms*, 4th ed (Boston: Addison-Wesley, 2011).

[7] Woodrow Barfield & Jessica Barfield, "An Introduction to Law and Algorithms" in Woodrow Barfield, ed, *The Cambridge Handbook of the Law of Algorithms* (Cambridge: Cambridge University Press, 2020) at 3 [Barfield, "Law and Algorithms"].

[8] Deven R Desai & Joshua A Kroll, "Trust but Verify: A Guide to Algorithms and the Law" (2017) 31(1) Harv J L & Tech 1 at 6.

[9] Mikella Hurley & Julius Adebayo, "Credit Scoring in the Era of Big Data" (2016) 18(1) Yale J L & Tech 148 at 168 [Hurley, "Credit Scoring"].

[10] David Restrepo Amariles, "Algorithmic Decision Systems: Automation and Machine Learning in the Public Administration" in Woodrow Barfield ed, *The Cambridge Handbook of the Law of Algorithms* (Cambridge: Cambridge University Press, 2020) at 273.

a process called feature selection.[11] In this way, significant input variables can be selected to assess creditworthiness of customers. It is also important to continuously improve the algorithm by feeding new datasets into the system. This description of algorithm development is a simplified one which shows the workings of algorithmic decision-making at the basic level; in practice, algorithmic decision-making is a more complex and iterative process involving considerable efforts and various techniques.

B. *Problems of Algorithmic Decision-making*

1. *Problems with data*

What an algorithmic model can learn depends on the examples to which it is exposed, and thus the bias in training data is very likely to cause systematic errors in decision-making. For example, in the area of credit assessment, algorithms are designed to harness large amounts of customer data from e-commerce transactions, social networks and other related online activities. The problem is that unrepresentative or incomplete training datasets can bias the automated decision-making system to treat similarly situated borrowers in different ways. Specifically, if the training data used for an algorithmic model is more representative of certain groups of borrowers, the credit decisions will systematically disadvantage borrowers who are underrepresented in the database.[12] There is also growing concern about dark zones in data collection, that is, the systemic omission of people on the margins of big data, which can cause them to be overlooked or misrepresented.[13] This marginalisation can lead to disproportionate representation in the training data and further affect the accuracy of algorithms. The Chinese tech giant, Ant Group, has developed algorithmic decision-making systems by analysing a massive amount of data about Internet-savvy users.[14] However, the company may undervalue the preferences and behaviour of customers who are less involved in online activities and unable to produce sufficient data.

In addition, the efficacy of algorithmic decision-making is primarily determined by the quality of input data in the model. An important computing principle, "garbage in, garbage out", is that low-quality data may skew the results produced by algorithms and amplify the impact of bias in training datasets.[15] If customer data used for decision-making is of poor quality, the algorithmic models will be ineffective or flawed. In the first quarter of 2022, 21 Chinese banking institutions were fined RMB 87.6 million for data governance and reporting issues, such as providing

[11] Hurley, "Credit Scoring", *supra* note 9 at 180.

[12] Solon Barocas & Andrew D Selbst, "Big Data's Disparate Impact" (2016) 104(3) Cal L Rev 671 at 681 [Barocas, "Big Data"].

[13] Jonas Lerman, "Big Data and Its Exclusions" (2013) 66 Stan L Rev Online 55 at 57.

[14] Ant Group Co Ltd, H Share IPO Prospectus (27 October 2020) at 192, <https://www1.hkexnews.hk/listedco/listconews/sehk/2020/1026/2020102600165.pdf>.

[15] European Union Agency for Fundamental Rights, *Data Quality and Artificial Intelligence — Mitigating Bias and Error to Protect Fundamental Rights* (11 June 2019) at 2, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf>.

inaccurate or incomplete data to financial regulators, a significant increase from previous years.[16] This demonstrates that there are still many problems with data governance even in the strictly regulated financial sector, and these data governance issues would likely be even more acute in more innovative industries. Given the increasingly important role of data in algorithmic decision-making, the practical difficulty lies in how to ensure the accuracy, completeness and consistency of data pools to improve the quality of analytical results. Moreover, the use of irrelevant data in algorithmic decision-making is very likely to raise the risk of false predictions.[17] The lack of causality between decisions and the data on which they are based can adversely affect the performance and reliability of algorithmic models.

2. *Problems with algorithmic models*

It is a challenging task to properly define an unstructured problem that may have multiple correct answers based on input data and variables.[18] Taking credit assessments as an example, there is no single algorithmic solution to this problem, since the willingness and ability of customers to repay their loans depend on a myriad of factors in practice. Data from social networks, e-commerce transactions and other online activities can be used as variables to assess credit risk of customers, and different weights are assigned to each of these inputs to calculate their final score. These uncertainties in the input data and the underlying calculation process are likely to affect credit assessment in different ways, and thus the result may vary depending on the variables available to algorithmic decision-making.

More importantly, the complex design of algorithmic models has raised some concern about how to accurately select features related to the target variable to produce effective results. Algorithms facilitate the automated discovery of patterns in massive datasets and then predict possible outcomes in different situations.[19] However, the selection of features that fail to cover a representative sample for algorithmic decision-making may result in less accurate classification of target groups. Meanwhile, potentially adverse outcomes produced by algorithms may be artefacts of statistical reasoning rather than biases in decision-making processes, in which cases certain individuals are likely to be victimised by statistically sound but factually unfair inferences.[20] It is practically difficult to develop an algorithmic model that can capture the precise distinction of each individual and make reliable predictions accordingly. In addition, algorithmic decision-making depends mainly

[16] Tang Yaohua, "Financial institutions fined a total of RMB 2.7 billion in 2022, penalties for financial consumer protection increased significantly", *21st Century Business Herald* (People's Republic of China) (13 January 2023), <http://www.21jingji.com/article/20230113/herald/9790739c408cbb6d34069144ff830bab.html>.

[17] Dirk A Zetsche, Ross P Buckley, Douglas W Arner, & Janos N Barberis, "From FinTech to TechFin: The Regulatory Challenges of Data-driven Finance" (2018) 14(2) NYU J L & Bus 393 at 422.

[18] Hurley, "Credit Scoring", *supra* note 9 at 159–160.

[19] Domingos Pedro, "A Few Useful Things to Know About Machine Learning" (2012) 55(10) Communications of the Association for Computing Machinery 78 at 78–80.

[20] Barocas, "Big Data", *supra* note 12 at 688.

on attributes that an individual shares with others in the same risk category rather than the individual's own merit, which is likely to entrench biases.[21]

Further, algorithmic models can systematise and conceal biases, making it more difficult to predict the potential impact of decisions.[22] They may be used to intentionally skew data and select features that produce less or more favourable results for certain groups of people, and then mask such erroneous results through the automated decision-making process. For example, loan facilitation service providers can manipulate the algorithmic system to falsely improve creditworthiness of their customers and thereby attract more borrowing.[23] This could pose serious challenges to ensuring the accuracy, integrity and reliability of algorithmic decision-making.

III. The Regulatory Regime in China: Recent Developments

While algorithms can replace humans at some junctures in the decision-making process, they are also susceptible to bias, unfairness and opacity. The use of algorithmic models has raised many problems in practice, which challenges existing regulations designed primarily for human decision-making.[24] The major concern is how to regulate algorithmic decision-making in a way that does not stifle such innovation while protecting the rights and interests of customers. Given the complexity of algorithms and their significant impact on individuals, China has gradually established a regulatory framework for increasingly intelligent decision-making.

A. *Overview*

In China, relevant rules for information protection and automated decision-making are scattered within an array of laws and regulations. As algorithmic models involve the collection, processing and use of massive customer data, the primary focus of China's existing regulatory regime is data governance. The Cybersecurity Law, promulgated in 2016, requires network operators to comply with relevant regulations and standards when collecting and using personal information.[25] The Data Security Law, enacted in June 2021, stipulates a set of requirements to ensure data security while encouraging its effective use,[26] and the introduction of the Personal Information Protection Law in August 2021 clarifies the legal basis for personal information processing and strengthens the processor's responsibilities.[27]

[21] Hurley, "Credit Scoring", *supra* note 9 at 183.

[22] Kroll, "Accountable Algorithms", *supra* note 3 at 680.

[23] Zhang Xiaohui, Former Assistant Governor, People's Bank of China, "Digital Economy and Fintech: Efficiency, Stability and Fairness", plenary keynote speech at Bund Summit 2021 (28 October 2021). Zhang pointed out that intelligent algorithms can easily conceal the complexity of financial risks, thus leading to over-indebtedness.

[24] Barfield, "Law and Algorithms", *supra* note 7.

[25] Cybersecurity Law of the People's Republic of China 2016 [Cybersecurity Law 2016].

[26] Data Security Law of the People's Republic of China 2021 [Data Security Law 2021].

[27] Personal Information Protection Law 2021.

The rapid development and widespread use of algorithms have raised growing regulatory concerns due to their significant impact on decision-making processes that are largely controlled by humans. In response, the Chinese government has been exploring ways to effectively regulate algorithms with the aim of striking a balance between technological innovation and customer protection. It announced a three-year plan to gradually strengthen comprehensive governance of algorithm security, including the establishment of sound regulatory mechanisms and a standardised algorithm ecosystem.[28] On 31 December 2021, the Cyberspace Administration of China ("CAC") and three other government departments jointly issued the Provisions on the Administration of Algorithm-generated Recommendations for Internet Information Services ("2021 Provisions on Algorithm Recommendations").[29] This filled a gap in algorithm regulation and imposed controls on the provision of algorithm recommendation services. More recently, the CAC released interim measures to regulate generative artificial intelligence services.[30] These interim measures mainly target technologies that generate different types of content based on algorithms, models and rules. These interim regulations can serve as a reference for market participants to determine compliance with relevant requirements, as well as indicate the direction of future legislation.

In addition to the laws and regulations, there are nationally recommended industry standards to facilitate best practices in developing and applying algorithms. On 21 October 2020, the People's Bank of China ("PBOC") issued the General Specifications for Fintech Innovation Security ("2020 General Specifications") to set out security requirements for the design and use of algorithmic models.[31] Several months later, the introduction of the Evaluation Specifications for Artificial Intelligence Algorithms in Financial Applications ("2021 Evaluation Specifications") laid down methods and criteria to evaluate the security, explainability and accuracy of algorithms in financial applications.[32] Further, on 25 September 2021, the professional committee under the Ministry of Science and Technology introduced the Code of Ethics for New Generation Artificial Intelligence ("2021 Code of Ethics").[33] It aims to integrate ethics into the entire life cycle of artificial intelligence, promote fairness and safety in various aspects of society, and prevent problems such as bias and information leakage. While such industry standards are not legally binding, they provide guidelines on how to develop accountable algorithms and ensure reliability of intelligent decision-making.

[28] Notice by the Cyberspace Administration of China, the Publicity Department of the CPC Central Committee, and the Ministry of Education of Issuing the Guiding Opinions on Strengthening the Comprehensive Governance of Network Information Service Algorithms 2021 (People's Republic of China), part 1 art 3 [Guiding Opinions on Network Information Service Algorithms 2021].

[29] Provisions on Algorithm-generated Recommendations 2021.

[30] Interim Measures for the Administration of Generative Artificial Intelligence Services 2023 (People's Republic of China) [Interim Measures for Generative AI Services 2023].

[31] People's Bank of China, *General Specification for Fintech Innovation and Security* (2020) [*General Specification for Fintech Innovation and Security*].

[32] People's Bank of China, *Evaluation Specification of Artificial Intelligence Algorithm in Financial Application* (2021) [*Evaluation Specification of AI in Financial Application*].

[33] Ministry of Science and Technology of the People's Republic of China, "Code of Ethics for New-Generation Artificial Intelligence" (2021) <https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html> [MOST, "Code of Ethics for New-Generation AI"].

B. *Data-related Regulatory Requirements*

As a key element of algorithmic decision-making, data has become the focus of Chinese regulators. While the main purpose of the Cybersecurity Law is to reduce the risk of cyberattacks and protect national security, it articulates a set of basic requirements for the collection and use of personal information and specifies some rights of data subjects. Specifically, network operators are required to follow the principles of legality, propriety, and necessity, disclose the rules, purposes, methods, and scope of information collection and use, and obtain consent from data subjects.[34] Data subjects have the right to request that network operators correct errors in personal information, and delete any personal information collected and used in violation of the agreement between the two parties.[35]

Furthermore, the Data Security Law provides a comprehensive regulatory framework to oversee data processing activities and ensure the legitimate use and effective protection of data. It requires the establishment of a category-based data protection system in line with the importance of data in economic and social development,[36] and imposes certain obligations on data processors, such as improving the data security management system and enhancing risk monitoring and assessment.[37] Moreover, data processing activities and research on new data technologies are required to conform to social morality and ethics.[38] Data processors that develop and use relevant advanced technologies are also subject to ethical requirements. This law treats data as an essential factor of production in the digital economy and sets a baseline level of security for data collection, use, transfer and other processing activities.

In addition, the introduction of the Personal Information Protection Law consolidated relevant provisions on personal information protection and further systematised the legal framework. The processing of personal information is required to comply with some fundamental principles, including but not limited to the principles of legality, necessity, propriety, fairness, transparency, purpose limitation and data minimisation.[39] It grants data subjects a number of rights to ensure protection at all stages of information processing, and also greatly increase the responsibilities placed on personal information processors by imposing more specific regulatory requirements on their activities. In response to the rapid development of the platform economy, this law places additional obligations on information processors that provide important internet platform services and have a large number of users and complex business types.[40] As a result, internet platforms that process massive amounts of customer information and offer technical solutions such as algorithm design may be subject to more stringent regulations.

[34] Cybersecurity Law 2016, art 41.

[35] Cybersecurity Law 2016, art 43.

[36] Data Security Law 2021, art 21.

[37] Data Security Law 2021, arts 27, 29–30.

[38] Data Security Law 2021, art 28.

[39] Personal Information Protection Law 2021, arts 5–7.

[40] Personal Information Protection Law 2021, art 58.

More importantly, there are specific rules governing automated decision-making in the Personal Information Protection Law. It defines automated decision-making as the activity of automatically analysing and evaluating an individual's behaviour, habits, or economic, health, and credit status through computer programs and making decisions.[41] When using personal information for automated decision-making, information processors are required to ensure the transparency of the decision-making process and the fairness of the results, and must not provide unreasonable differential treatment to individuals in terms of trading prices or other trading conditions; where information push or commercial marketing to individuals is conducted by means of automated decision-making, options not specific to individuals' characteristics must be provided simultaneously, or convenient ways to opt out must be provided for individuals; when a decision having a significant impact on an individual's rights and interests is made by means of automated decision-making, the individual shall have the right to request that the information processor explain the decision and the individual may object to a decision made solely by means of automated decision-making.[42] The Personal Information Protection Law lays down basic principles for applying automated decision-making to different services and establishes a clear baseline for subsequent algorithm regulation in China.

C. *Regulatory Mechanisms for Algorithms*

In response to the widespread use of automated decision-making, the Chinese government has established a comprehensive governance structure for algorithms. The Guiding Opinions on Strengthening the Comprehensive Governance of Internet Information Service Algorithms ("2021 Guiding Opinions on Algorithms") laid down some key principles to develop and apply algorithms, such as the principles of security, transparency, fairness and explainability.[43] The regulatory objective is to maximise the benefits of algorithmic decision-making while controlling the risks involved in such technological innovation. Later, four government departments jointly enacted the 2021 Provisions on Algorithm Recommendations, which stipulated the detailed requirements for algorithm recommendation services.

1. *Ex ante mechanisms*

Ex ante regulatory mechanisms are primarily designed to prevent the use of algorithmic models that may pose significant risks to customer protection. In China, the authorities have established a security management system for algorithms covering different categories and levels, which is based on the characteristics of public opinions, the capacity for social mobilisation, the type of service content, the number of users, the importance of data processing, and the degree of intervention in user

[41] Personal Information Protection Law 2021, art 73(3).

[42] Personal Information Protection Law 2021, art 24.

[43] Guiding Opinions on Network Information Service Algorithms 2021, part 1, arts 2-3.

behaviour.[44] An algorithm recommendation service provider that has public opinion properties or social mobilisation capacities[45] shall submit its name, service form, field of application, type of algorithm, algorithm self-assessment report, content to be displayed and other information through the filing system,[46] and conduct security assessments in line with relevant regulations.[47] This enables regulators to determine the risk level of different algorithms prior to their application in recommendation services and take appropriate regulatory measures based on their potential impacts.

More recently, the Interim Measures for the Administration of Generative Artificial Intelligence Services ("2023 Measures for Artificial Intelligence") reiterated the requirements for algorithm filings and security assessments. It stipulated that service providers should report to the CAC for security assessments and complete the formalities of algorithm filing before using generative artificial intelligence to carry out related business.[48] These regulations contribute to a better understanding of the performance of algorithmic models and the identification of vulnerabilities in the decision-making process, thus mitigating potential risks in the initial stage.

2. *Ongoing oversight*

In addition to *ex ante* mechanisms, it is essential to monitor the use of algorithms on a continuous basis. While the Personal Information Protection Law stipulates that information processors should ensure the transparency of automated decision-making, it primarily focuses on the protection of individuals' rights in a general sense, rather than the compliance of algorithm service providers. The 2021 Guiding Opinions on Algorithms sets out more specific rules, requiring enterprises to improve algorithm security management, strengthen risk prevention and take responsibility for the results of algorithm applications.[49]

A major goal of algorithm regulation is to help market participants understand how systems automatically make decisions. The lack of transparency in algorithmic decision-making has raised growing concerns since it could pose a challenge to regulatory scrutiny. In this regard, the 2021 Provisions on Algorithm Recommendations requires service providers to disclose relevant rules for searching, sorting, selection and push of algorithm recommendation services to avoid disputes with users.[50] Service providers must also inform users of the algorithm recommendation services provided in a conspicuous manner and display the algorithm's basic principles, goals

[44] Provisions on Algorithm-generated Recommendations 2021, art 23.

[45] Factors determining whether service providers have public opinion properties or social mobilisation capacities include the type of service provided and the scale of service users. Provisions on the Security Assessment for Internet Information Services with Characteristics of Public Opinions or Capable of Social Mobilization 2018 (People's Republic of China), arts 2-3 [Provisions on Security Assessment 2018].

[46] Provisions on Security Assessment 2018, art 24.

[47] Provisions on Security Assessment 2018, art 27.

[48] Interim Measures for Generative AI Services 2023, art 17.

[49] Guiding Opinions on Network Information Service Algorithms 2021, part 2 art 4.

[50] Provisions on Algorithm-generated Recommendations 2021, arts 7, 12.

and operating mechanisms in an appropriate manner.[51] Moreover, algorithms without a clear explanation of the information and rationale behind the decision-making process are opaque to users, making it difficult to find errors or bias in the system. According to relevant regulations, the provider of algorithm recommendation services is required to make an explanation and assume corresponding responsibilities when the application of algorithms has a significant impact on the users' rights and interests.[52] In the area of generative artificial intelligence, the provider must clarify and disclose the target groups, application scenarios and purposes of its services, and take appropriate measures to prevent users from excessively relying on or indulging in the services.[53]

Furthermore, it is important to ensure fairness of the automated decision-making process, that is, algorithms cannot be designed and used in a way that systematically disadvantages or even discriminates against similarly situated individuals and businesses. In accordance with the principle of fairness, the provider of algorithm recommendation services must offer users options which are not targeted at their personal characteristics, or the option to stop receiving relevant services, and the function of selecting or deleting user labels.[54] When selling goods or services, the provider shall also protect customers' right to fair transactions and cannot use algorithms to offer unreasonable differential treatment in terms of transaction prices or other transaction conditions based on consumers' preferences, habits and other characteristics.[55] In the process of algorithm design, training data selection, and model generation and optimisation, service providers that use generative artificial intelligence must take measures against discrimination based on race, gender, age, occupation, *etc*.[56]

In addition, security is a key principle to protect algorithms from malicious attacks that could threaten their integrity or disrupt their services, thus enhancing public trust in automated decision-making. The providers of algorithm recommendation services are required to implement appropriate management systems and technical measures, such as reviews of technology ethics and algorithm mechanisms, security assessment and monitoring, data protection and incident response, and the employment of professionals and technical support staff commensurate with the scale of services provided.[57] They are also required to keep log files for security assessment and inspection by relevant authorities and provide necessary technical and data support.[58] Indeed, periodic evaluation of operating mechanisms, models, data and outcomes is important to ensure the security of algorithm recommendation services. As a general principle, the security of algorithms and data resources is essential to the development of generative artificial intelligence. The Chinese government supports the innovation of artificial intelligence algorithms and frameworks and other underlying technologies, and prioritises the use of secure and

[51] Provisions on Algorithm-generated Recommendations 2021, art 16.

[52] Provisions on Algorithm-generated Recommendations 2021, art 17.

[53] Interim Measures for Generative AI Services 2023, art 10.

[54] Provisions on Algorithm-generated Recommendations 2021, art 17.

[55] Provisions on Algorithm-generated Recommendations 2021, art 21.

[56] Interim Measures for Generative AI Services 2023, art 4(2).

[57] Provisions on Algorithm-generated Recommendations 2021, art 7.

[58] Provisions on Algorithm-generated Recommendations 2021, art 28.

reliable computing power and tools.[59] There are also requirements to provide users with safe, stable and continuous services during the life cycle of the generative artificial intelligence.[60]

3. *Ex post mechanisms*

Ex post mechanisms are routes for aggrieved parties to seek relief after the occurrence of damage caused by algorithmic decision-making, which essentially includes public and private enforcements. The principle of algorithmic accountability is designed to promote the responsible development and use of automated decision-making models and deter illegal and unethical business practices. In terms of public enforcement, the 2021 Provisions on Algorithm Recommendations impose different types of penalties on algorithm recommendation service providers, depending on the extent of their illegal acts. Specifically, if a service provider violates the regulations on algorithmic transparency, fairness and security, the competent authorities can issue a letter of warning, circulate a notice of criticism, or order it to make corrections; if the service provider refuses to correct their errors or if the offence is serious, it can be ordered to suspend information updates and fined between RMB 10,000 and RMB 100,000.[61] There are similar penalty mechanisms for providers of generative artificial intelligence services.[62] In addition, a provider of algorithm recommendation services that fails to comply with requirements governing cybersecurity, data security and personal information protection may also be punished accordingly. For example, in line with the Personal Information Protection Law, the relevant authority can impose penalties, such as fines, confiscation of illegal income, suspension of business activities and revocation of licenses, on algorithm recommendation service providers that fail to meet their obligations when processing personal information.[63] The law also allows regulators to fine information processors up to RMB 50 million or 5 per cent of their previous year's turnover, whichever is higher, for serious violations.

Moreover, aggrieved parties involved in the algorithmic decision-making process can initiate private enforcement in the form of civil litigation to seek compensation. In general, a person who infringes upon the civil rights and interests of others and causes damage shall bear tortious liability.[64] Internet service providers shall also be liable for infringement through the use of information networks.[65] In this regard, customers will have a cause of action in tort against a provider of algorithm recommendation services or generative artificial intelligence services if their rights and interests are harmed. They can further claim compensation if the service provider's

[59] Interim Measures for Generative AI Services 2023, art 6.

[60] Interim Measures for Generative AI Services 2023, art 13.

[61] Provisions on Algorithm-generated Recommendations 2021, art 31.

[62] Interim Measures for Generative AI Services 2023, art 21.

[63] Personal Information Protection Law 2021, art 66.

[64] Civil Code of the People's Republic of China 2020, arts 1165–1166 [Civil Code 2020].

[65] Civil Code 2020, art 1194.

violations cause financial loss or serious mental harm.[66] Where it is difficult to determine the financial loss or the benefits obtained by the infringer, the court may award damages of up to RMB 500,000 depending on the particular circumstances of each case.[67]

IV. Evaluating the Chinese Experience: Strengths and Weaknesses

As discussed above, China has made great efforts to address problems with algorithmic decision-making by introducing an array of laws and regulations. The regulatory objective is to promote the development and application of innovative algorithms while, at the same time, safeguarding the rights and interests of customers. In the international arena, some jurisdictions, such as the European Union (EU), the United States (US), Singapore and the United Kingdom (UK), are also reforming their regulatory frameworks in response to the widespread use of algorithmic decision-making. By comparing the experience of these overseas jurisdictions, this part will critically examine the strengths and weaknesses of China's regulatory regime.

A. *Strengths of the Chinese Regulations*

China has formulated specific regulations on algorithm recommendation services, which are applicable to different types of widely used algorithmic techniques, including generation and synthesis, personalised push, sorting and selection, search and filtering, and scheduling decision-making.[68] The 2021 Provisions on Algorithm Recommendation delineates the responsibilities of algorithm recommendation service providers to ensure security of internet information content, maintain market order, and protect individuals' rights and interests. It imposes additional requirements on the provision of algorithm recommendation services to minors, seniors, labourers and consumers.[69] Such groups of individuals are susceptible to increasingly intelligent decision-making, which may lead to differential treatment or even significant financial loss. Hence, the providers of algorithm recommendation services are required to strengthen protection for these vulnerable groups. These special protection measures indicate that Chinese regulators are aware of the potential harm caused by biased or even malicious algorithms, thus ensuring accountability and high ethical standards in the decision-making process.

In addition, the 2021 Provisions on Algorithm Recommendation establishes a series of governance mechanisms covering the whole process of algorithm recommendation services, such as data use, operating principles, models, and outcomes.

[66] Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Civil Disputes over Infringements upon Personal Rights and Interests through Information Networks (2020 Amendment), art 11 [Provisions on Civil Disputes 2020].

[67] Provisions on Civil Disputes 2020, art 12.

[68] Provisions on Algorithm-generated Recommendations 2021, art 2.

[69] Provisions on Algorithm-generated Recommendations 2021, arts 18-21.

The service providers need to monitor the performance of algorithms on a continuous basis and fulfil their responsibility for algorithm security, fairness and transparency. More importantly, China is one of the pioneers in adopting an algorithm filing system, which requires algorithm recommendation service providers with public opinion properties or social mobilisation capacity to disclose relevant information.[70] In this way, regulators can have a basic understanding of the algorithms used by internet service providers and assess the algorithms' potential impacts on the public. The algorithm filing system is also useful for future reference, that is, it includes information about the internet service providers' ability to evaluate and control risks involved in algorithms and thus determine the degree of their responsibility. The requirements for timely changes of filing information further demonstrate regulatory flexibility and agility. It would in turn facilitate the establishment of a category-based management system to set out differentiated rules for algorithms accordingly.

In China, the legal consequences of non-compliance with relevant regulations allow for both private and public enforcement. The aggrieved parties are entitled to seek relief by initiating a civil lawsuit against algorithm recommendation service providers.[71] Given the novelty and complexity of algorithmic decision-making, public enforcement by the CAC, with its professional resources and technical means, can be more efficient in implementing regulatory measures than private enforcement by individuals to deter violators. There is a range of administrative penalties, such as a letter of warning, a notice of criticism, corrections and fines, and even criminal liability,[72] which help protect the legitimate rights and interests of customers. These *ex post* mechanisms play an essential role in ensuring regulatory compliance and quality of algorithm development and application.

B. *Weaknesses in the Chinese Regulations*

1. *Limitations of data protection in algorithmic decision-making*

While the Personal Information Protection Law does not prohibit the processing of sensitive personal information in automated decision-making, it imposes higher requirements on information processors, such as having specific purpose and necessity, taking strict protection measures, obtaining a separate consent of individuals, and conducting *ex ante* impact assessments.[73] From a regulatory perspective, it can dampen the effect of bias by placing a restriction on the types and amounts of data

[70] Provisions on Algorithm-generated Recommendations 2021, art 24.

[71] See, *eg*, *Beijing iQIYI Science & Technology Co Ltd v Beijing ByteDance Technology Co Ltd* [2018] Beijing Haidian District People's Court Civ 49421, which is the first infringement case regarding a short video platform's recommendation algorithm. The court held that the short video platform provides information storage space and information stream recommendation technology, and therefore has a higher duty of care for users' infringements. This judgment offers guidance on the duty of care of network service providers in relation to algorithm recommendation.

[72] Provisions on Algorithm-generated Recommendations 2021, art 31.

[73] Personal Information Protection Law 2021, arts 28-29, 55.

that an algorithmic model can collect and use.[74] However, there may be a trade-off between the removal of some sensitive data and the performance of algorithms. In other words, the constraint on data processing may lead to a potential loss of useful information with great relevance to decision-making and thus adversely affect the accuracy of algorithms.[75] Algorithmic models also have the ability to analyse the relationship between different pieces of information that is not directly related to special categories of personal data, such as data concerning race, gender and health, and then generalise personal characteristics of customers to make decisions without accessing information that falls into these sensitive categories.[76] Hence, stringent requirements for the collection and processing of sensitive personal information may not necessarily solve data-related problems in algorithmic decision-making.

In addition, there are specific rules for automated decision-making in the Personal Information Protection Law, which requires information processors to ensure the transparency of decision-making and the fairness of outcomes. An individual has the right to request from the information processor an explanation of a decision, and to object to a decision that is based solely on automated decision-making and has a significant impact on the individual's rights.[77] The EU's General Data Protection Regulation (GDPR) sets an important precedent for the processing and use of personal data and the requirements for automated decision-making. According to Article 22 of the GDPR, the data subject has the right not to be subject to a decision based solely on automated processing, which produces legal effects concerning the person or similarly significantly affects the person.[78] The data controller shall implement suitable measures to safeguard the data subject's legitimate rights and interests, at least the right to obtain human intervention, to express the point of view and to contest the decision.[79] Furthermore, the decision shall not be based on special categories of personal data unless the processing of data obtains explicit consent from the data subject or is necessary for substantial public interest, and suitable protection measures are in place.[80] Recital 71 further states that a decision may include automatic refusal of an online credit application or e-recruiting practices without any human intervention, and the automated processing of personal data evaluating the data subject's aspects shall also give an explanation of the decision reached; the data controller shall take appropriate procedures and technical measures to ensure the correction of inaccuracies in personal data, the minimisation of the risk of errors, and to prevent discriminatory effects on natural persons.[81]

[74] Scott R Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Tex L Rev 85 at 149.

[75] Bryce W Goodman, "A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection", paper presented at the 29th Conference on Neural Information Processing Systems (2016).

[76] *Ibid*.

[77] Personal Information Protection Law 2021, art 24.

[78] Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 96/46/EC (General Data Protection Regulation), EU Council Regulation (EU) 2016/679 [2016] OJ L 119/1, art 22(1) [General Data Protection Regulation (EU)].

[79] General Data Protection Regulation (EU), art 22(3).

[80] General Data Protection Regulation (EU), art 22(4).

[81] General Data Protection Regulation (EU), Recital 71.

By comparison, the prohibition on automated individual decision-making in the GDPR does not apply to decisions that are necessary for entering into or performance of a contract, authorised by law, or based on explicit consent from the data subject.[82] In these cases, the GDPR requires the data controller to implement suitable measures to protect rights and interests of the data subject. However, there are no such exceptions in the Personal Information Protection Law. Under China's existing regulatory framework, information processors cannot use contractual necessity, legal authorisation or individuals' consent as justification for automated decision-making if the decision is based solely on automated decision-making and has a significant impact on personal rights and interests. This may place a heavy compliance burden on information processors and lead to unnecessary uncertainty in automated decision-making.

Further, Article 24 of the Personal Information Protection Law does not provide individuals with the right to obtain human intervention, to express their point of view and to contest a decision that significantly affects the individual. It may be inadequate to protect data subjects with suitable measures and ensure the legitimacy of automated decision-making.[83] Data subjects should be entitled to challenge a decision and express their view. It is also important to allow the persons with the capacity and authority to change the decision to review the automated decision-making process. Moreover, Chinese law does not specify the extent and manner in which automated decisions shall be explained to individuals, nor does it set out criteria for assessing the significant of impacts. By comparison, the EU's Article 29 Data Protection Working Party issued guidelines to clarify relevant requirements for automated decision-making.[84] Specifically, it states that legal effects require a decision to affect individuals' legal rights or their legal status under a contract, and describes the threshold for significance of a decision.[85] The guidelines can provide some practice recommendations for data controllers when making solely automated decisions and facilitate their compliance with the GDPR requirements.

2. *Inadequacy of the algorithmic transparency principle*

The principle of algorithmic transparency is essential to inform customers about how a decision-making model operates and facilitate the identification of risks arising from automated processing.[86] Algorithmic transparency is also a major regulatory tool to ensure accountability of internet service providers. The 2021 Provisions on Algorithm Recommendation places great emphasis on improving the transparency of the basic principles, goals and operating mechanisms of algorithms. However,

[82] General Data Protection Regulation (EU), art 22(2).

[83] Wang Ying, "Categorisation of Algorithmic Infringements and Legal Responses — A Regulation Framework Based on the Personal Information Protection Law" [2021] 6 *Law and Social Development* 133 at 147 [Wang, "Algorithmic Infringements"].

[84] European Union Data Protection Working Party, *Guidelines on Automated Individual Decision-making and Profiling for the Purpose of Regulation 2016/679* (revised 6 February 2018).

[85] *Ibid* at 21–22.

[86] Danielle Keats Citron & Frank Pasquale, "The Scored Society: Due Process for Automated Predictions" (2014) 89(1) Wash L Rev 1 at 24–25.

the problem is that algorithmic transparency prescribes principle-based standards, without detailed implementing rules. This may undermine the effectiveness of the transparency principle in the context of algorithmic decision-making.

By comparison, in April 2019, the European Parliamentary Research Service released a governance framework for algorithms, stating that it is more feasible to improve transparency of the behaviour of computing systems rather than transparency in the way outcomes are reached given the complexity of algorithmic processing and the scale of data involved in computations.[87] The report proposes to establish a tiered regulatory regime based on the degree of risk associated with algorithms. A specialised regulatory body can be tasked to develop a risk assessment matrix for classifying algorithmic applications and determining the level of regulatory oversight, and to cooperate with industry associations to set relevant standards and best-practices procedures.[88] This allows regulators to access necessary technical and other information for a robust impact assessment. Under the governance framework, high-risk uses of algorithmic decision-making should be subject to stricter transparency requirements, and to more severe penalties for violation of relevant rules.

In May 2024, the Council of the EU approved the Artificial Intelligence Act, which is the world's first comprehensive law on artificial intelligence.[89] It follows a proportionate risk-based approach and places a set of obligations on providers of artificial intelligence systems depending on the level of risk. Specifically, high-risk artificial intelligence systems shall ensure that their operations are sufficiently transparent and provide users with relevant information, such as the characteristics, capabilities and limitations of the system's performance, the human oversight measures, and necessary maintenance measures.[90] There are also transparency obligations for certain artificial intelligence systems, including systems intended to interact with natural persons, emotion recognition or biometric categorisation systems, and systems that generate or manipulate image, audio and video content.[91] Importantly, the provider of high-risk artificial intelligence systems shall register with the EU database set up by regulators, which contains information about the systems and is accessible to the public.[92] Moreover, the GDPR requires data controllers to provide specific information about automated decision-making to fulfil their transparency obligations, including the existence of automated decision-making, meaningful information about the logic involved and the significance and the envisaged consequences of the processing.[93]

[87] European Parliamentary Research Service, *A Governance Framework for Algorithmic Accountability and Transparency* (2019) at 35 [European Parliamentary Research Service].

[88] *Ibid* at 72–74.

[89] Regulation Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2016/1828 (Artificial Intelligence Act), EU Council Regulation (EU) 2024/1689 [12 July 2024] OJ L [Artificial Intelligence Act (EU)].

[90] *Ibid* at art 13.

[91] *Ibid* at art 50.

[92] *Ibid* at arts 49, 71 and Annex III.

[93] General Data Protection Regulation (EU), arts 13(2)(f), 14(2)(g).

In the US, the White House published the Blueprint for an AI Bill of Rights in October 2022, which lays out a set of principles and associated practices to guide the design, deployment, and governance of automated systems.[94] For example, impact assessments and reporting are necessary to protect individuals from ineffective or unsafe systems, algorithmic discrimination, and abusive data practices, as well as provide notice, explanation, and access to human consideration and fallback.[95] Moreover, the Algorithmic Accountability Act of 2023 was introduced in the House of Representatives, which requires covered entities to perform impact assessments of their automated decision systems and ensure transparency of critical decisions that have a significant effect on consumers.[96] Specifically, covered entities shall submit a summary report of their automated decision systems, containing information about the category of decisions, the intended purpose of systems, the testing and evaluation of systems, limitation on certain uses or applications of systems, input datasets, transparency or explainability measures, and likely material negative impact on consumers.[97] This enables regulators to better understand how automated decision systems operate and provides them with effective tools to mitigate algorithmic harm. It also proposes to develop a publicly accessible repository designed to inform consumers about the use of automated decision systems and ensure regulatory compliance.[98] The Federal Trade Commission is empowered to provide guidance and technical assistance on how to meet the requirements of impact assessment and transparency.[99] As automated decision systems have materially affected every aspect of a consumer's life, such as the availability of education, employment and financial services, there is a need for a high degree of transparency and accountability in the process. In addition to the proposed legislation, there are industry standards established by the National Institute of Standards and Technology ("NIST") to help organisations mitigate risks posed by artificial intelligence systems and promote responsible development and use of the systems.[100] It clarifies that transparency and accountability are characteristics of trustworthy artificial intelligence systems, and the scope of transparency spans from training data to the model design, the intended use cases, and how and when decisions are made.[101] The NIST's framework provides guidance on how to implement those standards and what practical actions can be taken to improve functionality and trustworthiness of artificial intelligence systems.

Moreover, in November 2018, the Monetary Authority of Singapore ("MAS") issued guidelines containing a set of principles for the use of artificial intelligence

[94] The White House Office of Science and Technology Policy, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (2022).

[95] *Ibid* at 5–7.

[96] Algorithmic Accountability Act of 2023, H.R. 5628, 118th Cong. (USA).

[97] *Ibid* at § 5.

[98] *Ibid* at § 6(b).

[99] *Ibid* at § 7(a).

[100] National Institute of Standards and Technology (USA), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (2023).

[101] *Ibid* at 15–16.

and data analytics ("AIDA") in the financial sector.[102] Unlike general guidance on the algorithm development in other jurisdictions, the MAS's guidelines are specific for firms using AIDA in decision-making to provide financial products and services. It contains a set of principles to promote fairness, ethics, accountability of transparency of AIDA-driven decisions. In terms of the transparency principle, disclosure of the use of AIDA can increase public confidence, and clear explanations about decision-making can facilitate data subjects' understanding about how data affects the decision and what consequences it may have.[103] The guidelines further illustrate that a firm can consider the materiality of decisions when determining the appropriate level of transparency, since excessive transparency may provide individuals with unintended opportunities to manipulate algorithmic models.[104] It is necessary for firms to balance such considerations while increasing transparency in the use of AIDA. More recently, MAS released a number of white papers detailing assessment methodologies for the principles to guide the responsible use of artificial intelligence by financial services institutions. Specifically, it provides a methodology to evaluate the need for external transparency and recommends a set of internal capabilities to underpin such transparency.[105] Financial services institutions should ensure an appropriate level of transparency in the overall decision-making process, the reasons behind specific decisions, the impact of AIDA systems, and available redress options.[106] The proposed methodology takes the form of checklist questions mapped to each stage of an AIDA lifecycle, such as setting transparency standards, preparing input data, and validating and monitoring the system.[107] Importantly, MAS encourages financial services institutions to integrate transparency with their existing risk management practices and implement transparent requirements in a scalable manner, not just in individual AIDA use cases.[108] These white papers provide practical and detailed guidance on how to assess AIDA systems used in the financial sector.

In the UK, the Central Digital and Data Office launched the Algorithmic Transparency Recording Standard to help public sector organisations provide clear information about their use of algorithmic tools in decision-making.[109] The standard recommends that public sector bodies should be subject to mandatory transparency obligations. It uses the algorithmic transparency template to guide organisations in disclosing relevant information, and then publishes these disclosures for public review. There are tier 1 and tier 2 information in the template, covering information

[102] Monetary Authority of Singapore, *Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector* (2018).

[103] *Ibid* at 12.

[104] *Ibid*.

[105] Monetary Authority of Singapore, *Veritas Document 3C — FEAT Transparency Principles Assessment Methodology* (2022).

[106] *Ibid* at 12–13.

[107] *Ibid* at ch 3.

[108] *Ibid* at ch 4.

[109] Central Digital and Data Office (UK), "Algorithmic Transparency Recording Standard — Guidance for Public Sector Bodies" (2023) <https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard/algorithmic-transparency-recording-standard-guidance-for-public-sector-bodies [Central Digital and Data Office (UK)].

about how and why the algorithmic tool is used, who owns and has responsibility for the tool, what the tool is designed for, how the tool affects decision-making, the data used to train and run the tool, impact assessments of the tool, common risks of the tool and actions taken to mitigate the risks.[110] Due to better visibility of the algorithmic decision-making process, the implementation of this standard enhances meaningful transparency and promotes the development of trustworthy algorithms. In October 2022, the UK Information Commissioner's Office issued guidance to provide organisations with practical advice on explaining the processes, services and decisions made or assisted by artificial intelligence.[111] Unlike a statutory code of practice, this guidance sets out a number of overarching principles and checklists. An important principle to ensure the explainability of decisions is transparency, which requires making the use of artificial intelligence for decision-making obvious and appropriately explain the decisions in a meaningful way.[112] Specifically, the organisations may need to disclose information about the technical logic behind the artificial intelligence model, the input features, parameters and correlations, the application of the statistical results, the types and sources of training data, and the assessments of data quality.[113]

From a comparative perspective, China can learn from the regulatory experiences of these overseas jurisdictions to lay down detailed rules on algorithmic transparency. However, the transparency principle has its inherent limitations. The elements of a decision strategy, the algorithmic systems for executing decisions, and the key inputs and outcomes may need to be kept confidential, as they are closely related to competitive advantages of companies using algorithms.[114] In this regard, the disclosure of technical details such as the source code may enable competitors to copy the algorithmic models or users to game the decision-making system to their advantage. For example, the credit providers generally use a set of proxy variables, including credit history, payment records and income statements, and then assign different weights to these inputs in algorithmic models to assess the default risk of a borrower. If full disclosure of the credit assessment algorithm is required, loan applicants who are familiar with the decision-making process can potentially influence the outcomes by controlling the input of relevant information.[115] It is important for companies to protect their innovative algorithms and trade secrets, which in practice may be incompatible with transparency requirements.

In addition, the principle of algorithmic transparency may raise concerns about the excessive disclosure of personal data used to train or deploy the model, thus posing a challenge to privacy protection. It also compromises the security of automated decision-making systems, which can be easily hacked due to the disclosure of technical details and data. By using system vulnerabilities, wrongdoers are likely to crack the algorithms, steal customer information and manipulate the outcome

[110] *Ibid*.

[111] Information Commissioner's Office (UK) and The Alan Turing Institute, *Explaining Decision Made with AI* (2022).

[112] *Ibid* at 41.

[113] *Ibid* at 45

[114] Kroll, "Accountable Algorithms", *supra* note 3 at 658.

[115] *Ibid*.

of decisions.[116] The problem is how to ensure that algorithms are subject to regulatory scrutiny, while safeguarding data subjects. More importantly, algorithmic decision-making involves a vast amount of data and complex computer programming with codes. Despite transparency requirements for algorithms, affected parties who do not specialise in related fields or do not possess technical skills may be unable to fully understand the design details and figure out the decision-making process.[117] As the development of an algorithm is a dynamic process, its transparency does not necessarily mean that it would be knowable at every stage. China needs to take these limitations into account when developing regulatory mechanisms for algorithmic transparency.

3. *Difficulties in implementing ex post mechanisms*

Given the potential harm caused by errors or bias in algorithms, *ex post* mechanisms are important to ensure accountability and to provide relief to aggrieved parties. While victims of algorithmic decision-making can initiate civil litigation in tort, there may be some challenges in seeking compensation. Firstly, information asymmetry between users and internet service providers makes it difficult to find evidence and prove the tort. For example, algorithms designed for credit assessment may be applied in a way that does not obviously disadvantage individuals.[118] Unlike price discrimination where consumers pay different prices for the same product, credit risk faced by each loan applicant is different and thus needs precise distinction when determining the lending rate. However, algorithms based on shared characteristics of a group of prospective borrowers may victimise part of them through inferences that are statistically sound but not fair.[119] In this regard, it would be difficult for an individual to prove possible bias or error in creditworthiness assessment compared to other similarly situated borrowers.

Moreover, as algorithms can be designed to intentionally conceal errors and bias in the decision-making system, it is a challenging task for aggrieved parties to hold the internet service provider accountable.[120] A crucial factor in the successful claim in a tort case is establishing a causal relationship between the problem of algorithmic decision-making and the damage. Due to the complex programming and a massive amount of data involved, customers cannot fully understand technical details in the algorithm to defend their rights and interests.[121] The automated decision-making

[116] Zhang Xiaoshan, "Legal Regulations on Algorithmic Discrimination: Euro-American Experience and Chinese Approach" [2019] 6 Journal of East China University of Science and Technology 63 at 68.

[117] Shen Weiwei, "The Myth of Algorithmic Transparency — A Critique of Algorithm Regulation Principles" [2019] 6 Global Law Review 20 at 28–31.

[118] Christian Sandvig, Kevin Hamilton, Karrie Karahalios & Cedric Langbort, "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms", paper presented at a pre-conference of the 64th Annual Meeting of the International Communication Association (2014) [Sandvig, "Auditing Algorithms"].

[119] For a more detailed discussion, see Part II.B.2 above.

[120] Zhan Hao, *Research on Algorithm Discrimination of Data Mining in the Age of Big Data* (2020) (unpublished MPhil thesis, Hunan Normal University).

[121] Li Cheng, "Legal Governance of Artificial Intelligence Discrimination" [2021] 2 China Legal Science 127 at 137–139.

process makes the casual relationship more obscure. It was found that 34 per cent of plaintiffs failed in civil litigation regarding employment discrimination, since they could not prove the causal relationship between their identity attributes and unfair treatment by the employers, which was the primary reason for losing the cases.[122] This problem may be particularly acute in complex and opaque algorithmic decision-making.

Secondly, it is difficult to prove concrete harm suffered by the aggrieved parties in cases involving algorithms on the ground that risks are accumulated throughout the decision-making process, including the data collection, feature selection and predicted results. Internet service providers can generate great economic benefits through the effective use of algorithms to make commercial decisions, and on the other hand, their compensation liability can be relatively insignificant. In this regard, the deterrent effect of private enforcement may be limited. Further, small amounts of damages awarded to the aggrieved parties are very likely to discourage them from bringing civil actions, given the time and effort spent on litigating the tort.

In addition to private enforcement, the relevant authorities can also initiate public enforcement against noncompliant internet service providers. They have the power to investigate and impose different types of penalties on any organisation, such as fines, confiscation of illegal income and suspension of business activities.[123] Chinese regulators can penalise internet service providers for violating relevant requirements when processing personal information for automated decision-making under the Personal Information Protection Law. However, it is practically difficult to calculate illegal gains from algorithmic decision-making. For example, information processors may collect and use personal data without consent to train algorithmic models but reasonably incorporate them into the decision-making process. The problem is whether the gains derived from these algorithmic decisions are illegal. Furthermore, the current level of fines imposed by the 2021 Provisions on Algorithm Recommendations is inadequate to act as a deterrent to internet service providers, especially to those that generate huge revenue from algorithm recommendation services. In cases of gross violations of relevant regulations, the providers of algorithm recommendation services are subject to a fine of not less than RMB 10,000 but not more than RMB 100,000.[124] These regulatory mechanisms could be strengthened to effectively deter misconduct in algorithmic decision-making.

V. The Way Forward: Improvement Suggestions for China

Algorithms are playing an increasingly important role in the decision-making process. While it can bring many benefits to different aspects of life, there are some problems related to data and algorithmic models. China has responded to these problems by strengthening regulations on personal information and algorithm recommendation services. These regulatory rules can serve as a reference for regulators

[122] *Ibid* at 138.

[123] Administrative Penalty Law of the People's Republic of China 1996 (2021 Revision), art 9.

[124] Provisions on Algorithm-generated Recommendations 2021, arts 31, 33.

and also reflect the direction of future regulation. As discussed before, China's existing regulatory regime has its limitations and needs to be improved.

A. *Improving Regulatory Requirements for Algorithmic Decision-making*

Under the current regulatory framework, China attaches great importance to information protection and has granted individuals different data-related rights by introducing a series of laws and regulations. Given that data is an essential element in automated decision-making, relevant rules governing cybersecurity, data security and personal information protection can provide the basis for regulation of algorithms. In addition to these general provisions, it is worth considering formulating specific requirements for training and testing data used in algorithms. For example, under the EU's AI legislation, datasets used to train, validate and test high-risk artificial intelligence systems must meet certain quality criteria and be subject to appropriate management practices, such as the relevant design choices, data collection and processing, the examination of possible biases and the identification of possible data gaps or shortcomings.[125] Importantly, training, validation and testing datasets must be relevant, representative, free of errors and complete, and must also take into account the characteristics or elements that are particular to the specific setting within which the high-risk artificial intelligence system is intended to be used.[126] There are also detailed rules for the use of data to develop, test, maintain or update the automated decision system in the Algorithmic Accountability Act of 2023. It requires covered entities to provide information about sources of input data, including the type and collection methods of data and customers' informed consent for the inclusion and further use of data, reasons for using data, and other information, such as the representativeness and quality of datasets.[127] Based on these international experiences, China could complement existing regulations with specific requirements for the use of training and testing data in algorithmic decision-making. Given that data used to develop and test algorithms may be unrepresentative or of low quality, decisions made through the automated system can easily lead to unfavourable treatment of similarly situated individuals. Hence, the formulation of clear rules for input data can effectively mitigate the risk of algorithmic decision-making at source and also help customers safeguard their data-related rights.

Furthermore, the algorithmic decision-making process is not a straight linear path from data input to output, but an iterative process consisting of complex workflows such as problem definition, data collection and cleaning, feature selection, and model training and deployment.[128] The existing regulations that focus primarily on the underlying data or personal information used in algorithmic decision-making may not be adequate to address problems related to the logic involved and correct

[125] Artificial Intelligence Act (EU), *supra* note 89 at art 10(2).

[126] *Ibid* at art 10(3)-(4).

[127] Algorithmic Accountability Act of 2023 (USA) at § 4(a)(7).

[128] David Lehr & Paul Ohm, "Playing with the Data: What Legal Scholars Should Learn About Machine Learning" (2017) 51(2) U C Davis L Rev 653 at 655.

errors in other steps of automated processing.[129] In this regard, Chinese regulators may consider formulating specific algorithm regulations. For example, the PBOC issued the 2020 General Specification and the 2021 Evaluation Specification to facilitate best practices in applying algorithms in the financial sector. The 2020 General Specification establishes security requirements concerning the algorithm design, explainability, traceability and defence against attacks,[130] and the 2021 Evaluation Specification lays down basic rules, evaluation methods and judging criteria for algorithm applications in different stages.[131] While these recommended industry standards are not legally binding, they can provide a baseline for the subsequent regulation of algorithms, and the relevant principles contained therein can be integrated into the regulatory regime.

In addition, the 2021 Provisions on Algorithm Recommendations requires internet service providers to ensure transparency and explainability of algorithms. The problem is that the effectiveness of these regulatory requirements may be undermined, which is largely due to the lack of detailed implementation rules. Inspired by the UK's regulatory experience, it is worth considering using an algorithmic transparency template to guide the disclosure of relevant information, including the purpose, datasets and logic involved, the significance, envisaged consequences of algorithms and persons responsible for their operation.[132] This approach could allow regulators to gain a comprehensive understanding of the automated decision-making process and offer clear guidance to regulated entities on how to better comply with transparency requirements. In terms of the right to explanation, it does not mean that all information about an algorithm should be provided, especially to consumers without relevant expertise and technical skills.[133] Hence, there is a need to clarify whether the subject being explained should be the algorithmic processes and/or the particular decision, and then determine the standards and methods of explanation according to different algorithm application scenarios.[134]

B. *Strengthening Oversight through Algorithmic Auditing*

As discussed before, the principle of algorithmic transparency has some limitations.[135] In addition to transparency requirements, algorithmic auditing can act as an essential regulatory tool in verifying the fairness and accuracy of the automated decision-making process. This regulatory approach has a long history in the financial markets. For example, public companies must issue audited annual financial reports to provide information about their activities and performance throughout the preceding year. The Institute of Electrical and Electronics Engineers defines

[129] Wang, "Algorithmic Infringements", *supra* note 83 at 149.

[130] *General Specification for Fintech Innovation and Security, supra* note 31 at s 8.

[131] *Evaluation Specification for AI in Financial Application, supra* note 32.

[132] Central Digital and Data Office (UK), *supra* note 105. For a more detailed discussion, see Part IV.B.2 above.

[133] Margot E Kaminski, "The Right to Explanation, Explained" (2019) 34(1) BTLJ 189 at 214.

[134] Zhang Xin, "The Right to Explanation of Algorithmic Decisions and Algorithmic Governance" (2019) 31(6) Peking University Law Journal 1425 at 1439–1442.

[135] For a more detailed discussion, see Part IV.B.2 above.

an audit as "an independent examination of a software product, software process, or set of software processes performed by a third party to assess compliance with specifications, standards, contractual agreement, or other criteria."[136] In this regard, audits are also useful for identifying non-compliance in the increasingly intelligent decision-making process. While the input and output of an algorithm are knowable, its internal workings are essentially a black box to the majority of individuals affected by the automated decisions.[137] It is thus a major challenge to effectively evaluate and mitigate potential risks in the internal workings of algorithms. Given the complexity of algorithmic models, it is unreasonable to assume that each affected party has technical skills, resources and sufficient time to conduct an audit, which thus requires the assistance of qualified auditors. Algorithmic auditing mechanisms allow external experts to assess whether there are systemic errors or biases in the internal workings and to monitor the decision-making process independently.[138] Drawing on the EU's practice, collaboration with market participants such as algorithm designers, users and professional third-party auditors may merit consideration by Chinese regulators to develop appropriate audit standards and procedures and disclose relevant findings for public scrutiny.[139]

On 16 November 2022, the EU's Digital Services Act entered into force and laid down a set of rules governing gatekeeper online platforms in digital markets.[140] Under this regulatory framework, independent auditing is an important mechanism to ensure the effective implementation of obligations and to help the providers of digital services identify risks in relation to the underlying data and design of algorithms. It requires providers of very large online platforms and very large online search engines to grant access to all relevant data and premises for independent audits to assess their compliance with regulations and codes of conduct.[141] Auditors should have the necessary expertise in risk management and technical competence and capabilities to audit algorithms, and ensure the confidentiality, security and integrity of information obtained when performing their tasks.[142] They may also request explanations of the digital services provider's algorithmic systems and data processing. Moreover, an audit report must be established to express an opinion about whether the provider of very large online platforms and very large online search engines complies with the obligations and make operational recommendations on specific measures to achieve compliance.[143] The European Commission is empowered to adopt the necessary rules on the procedural steps, auditing methodologies and reporting templates for the audits.[144]

[136] Institute of Electrical and Electronics Engineers, "IEEE Standard for Software Reviews and Audits" in *IEEE Std 1028-2008* (2008) at 5.

[137] Bennie Mols, "In Black Box Algorithms We Trust (or Do We?)", *Communications of the ACM* (16 March 2017) <https://cacm.acm.org/news/214618-in-black-box-algorithms-we-trust-or-do-we/fulltext>.

[138] Sandvig, "Auditing Algorithms", *supra* note 118.

[139] European Parliamentary Research Service, *supra* note 87 at 59.

[140] Regulation on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act), EU Council Regulation (EU) 2022/2065 [2022] OJ L 277/1 [Digital Services Act (EU)].

[141] Digital Services Act (EU), art 37(1).

[142] Digital Services Act (EU), arts 37(2)–37(3).

[143] Digital Services Act (EU), art 37(4).

[144] Digital Services Act (EU), art 37(7).

In terms of audit procedures, it is essential to address problems regarding the frequency, focus and function of algorithmic auditing.[145] Specifically, auditors can conduct an impact assessment of algorithms prior to their implementation and review the quality of input data through a series of tests, thus minimising potential discriminatory effects in the decision-making process.[146] Algorithm developers may frequently modify their models as new sets of customer information are collected and analysed. In this regard, periodic auditing is needed to evaluate the performance of algorithmic models on a continuous basis to reduce the likelihood and severity of algorithm bias after they are deployed at scale.[147] The focus and function of auditing is largely dependent on the risk level of algorithm bias and the corresponding magnitude of harm on customers. External auditing of some algorithmic models may only require information about inputs and outputs, without access to the underlying source code.[148] Hence, there is a need for appropriate auditing standards and procedures to identify and mitigate risks of algorithmic decision-making in different circumstances.

In August 2023, the CAC released the draft rules for personal information protection compliance audits.[149] It requires personal information processors to conduct regular compliance audits, either by the processor's internal department or by an entrusted third party.[150] The CAC is responsible for establishing a recommended directory of professional audit institutions and providing a list of key audit matters. Where algorithms are used to process personal information, the compliance audit should focus on assessing the transparency of automated decision-making and the fairness of results.[151] For example, personal information processors need to carry out security assessments and ethical reviews of algorithmic models prior to implementation, and take measures to prevent possible adverse effects of automated decision-making. This proposed regulation could provide guidance for algorithmic auditing.

Inspired by these experiences, China can formulate regulations regarding the use of algorithms in different scenarios and determine the level of oversight for different automated decision-making systems based on the risk assessment. For high-risk algorithmic systems, there is a need for more stringent transparency requirements to provide regulators and users with sufficient information about the data collection and processing, the design choices, the characteristics and limitations of algorithms, and other information related to their performance. If core technical details such as source codes are not suitable for full disclosure given the protection of trade secrets and personal privacy, algorithm developers can entrust a third-party auditor

[145] Bryce Goodman, "Discrimination, Data Sanitization and Auditing in the European Union's General Data Protection Regulation" (2016) 2(4) EDPL 493 at 503–506.

[146] *Ibid* at 503.

[147] *Ibid* at 504.

[148] European Parliamentary Research Service, *supra* note 87 at 71.

[149] Notice by the Cyberspace Administration of China of Request for Public Comments on the Measures for the Administration of Personal Information Protection Compliance Audits (Exposure Draft) 2023 (People's Republic of China) [Notice for Public Comments on Personal Information Protection Compliance Audits 2023]

[150] Notice for Public Comments on Personal Information Protection Compliance Audits 2023, arts 4-5.

[151] Notice for Public Comments on Personal Information Protection Compliance Audits 2023, Annex art 9.

recognised by relevant regulators to conduct independent examination and issue compliance reports. In addition, it may be useful to establish a certification system for algorithms, thus promoting customers' trust in automated decision-making.[152] This mechanism could be an important complement to existing regulations. External auditors with expertise in risk management and technical competence should be granted access to the training and testing data used for high-risk algorithms to assess their conformity with regulatory requirements. In order to ensure the proper functioning of the algorithm on a continuous basis, any material changes to the decision-making system that could affect its regulatory compliance or intended purposes should also be examined by the auditors prior to the application. After the examination, the provider of the algorithmic system can obtain a certificate to demonstrate its compliance with relevant regulations. For other algorithmic systems with limited risks, regulators can set up a registration system for relevant information disclosure to increase public transparency and strengthen oversight of their application.

C. *Enhancing the Private and Public Enforcement*

While aggrieved parties in algorithmic decision-making can initiate civil litigation to seek compensation, they are likely to encounter some problems with proof of infringement and concrete harm. The neutrality of technology may be used as a strong argument to evade responsibility.[153] If the designer and operator of algorithmic systems are different, it will also be difficult to determine who should be liable for the damage. Traditionally, the manufacturer or operator of a machine is responsible for the consequences. However, the use of algorithms has challenged the responsibility ascription in situations where the designer or operator may not be able to control the decision-making process or predict the machine behaviour.[154] The damage caused by algorithmic decision-making can be attributed to a combination of factors, such as low-quality data and flawed models, and in practice, the designer or operator possesses more information about such technical details and limitations. Due to the massive asymmetry of information, the burden of identifying and disputing inaccuracies in algorithmic systems should not fall on the customers.[155] According to the Personal Information Protection Law, if an information processor cannot prove that it is not at fault, it shall bear tortious liabilities, including damages.[156] This mechanism provides reference for determining responsibility of relevant parties involved in algorithmic decision-making. It is worth considering placing the burden of proof on the designer or operator of algorithmic systems.

[152] Lilian Edwards & Michael Veale, "Enslaving the Algorithms: From a "Right to an Explanation" to a "Right to Better Decisions"?" (2018) 16(3) IEEE Security & Privacy 46 at 51–52 [Edwards, "Enslaving the Algorithms"].

[153] Zhang Linghan, "Algorithm Accountability Systems for Internet Platform Supervision" [2021] 3 Oriental Law 22 at 24.

[154] Andreas Matthias, "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata" (2004) 6 Ethics & Information Technology 175 at 175–176.

[155] Hurley, "Credit Scoring", *supra* note 9 at 198.

[156] Personal Information Protection Law 2021, art 69.

In addition, a possible solution to avoid burdening customers with the responsibility of understanding technical details and address the evidential difficulties in a civil action while ensuring effective protection of their rights is to set up a representative body.[157] There is a similar mechanism stipulated in the GDPR, that is, data subjects can mandate a not-for-profit body to lodge a complaint, exercise the right to an effective judicial remedy and receive compensation on their behalf.[158] After data subjects notice a breach of their rights, they can reach out to a third party who has the capability to analyse technical problems and then enlist its help. This regulatory approach could be adopted to strengthen private enforcement in algorithmic decision-making. In China, the Personal Information Protection Law also prescribes where an information processor violates relevant rules and infringes upon rights and interests of numerous persons, the People's Procuratorate, the consumer organisations specified by law and other organisations designated by the CAC may file a lawsuit.[159] As errors and bias in algorithmic decision-making are very likely to cause damage to a large group of similarly situated customers, a representative body with its industry knowledge and expertise would be in a better position to initiate civil litigation than individual aggrieved parties. In this regard, a nonprofit consumer protection organisation can be established and empowered to help victims of algorithmic decision-making assert their rights and obtain judicial remedies.

In terms of public enforcement, there is a great need to clarify the calculation of unlawful gains and increase the current level of penalties. For example, the GDPR lists several key factors that can be taken into account when deciding whether to impose an administrative fine and deciding on the amount of such fine in each case, including the nature, gravity, and duration of infringement, the intentional or negligent character, relevant previous infringements, any actions taken to mitigate the damage, the degree of cooperation with the regulatory body, *etc*.[160] Similarly, Chinese regulators can determine the level of penalties by reference to the risks to which algorithmic decision-making systems are exposed and the extent to which customers are harmed by the illegal practices. Furthermore, administrative fines serve to deter further infringements and have a higher disciplinary function than other types of penalties.[161] Under China's existing regulatory framework, the level of fines imposed on providers of algorithm recommendation services for their misconduct is inadequate to act as a deterrent.[162] It is therefore essential to introduce substantial fines to enforce compliance with rules concerning the development and application of algorithmic decision-making systems.

[157] Edwards, "Enslaving the Algorithms", *supra* note 152 at 52–53.

[158] General Data Protection Regulation (EU), art 80.

[159] Personal Information Protection Law 2021, art 70.

[160] General Data Protection Regulation (EU), art 83.

[161] Paul Nemitz, "Fines under the GDPR" in Ronald Leenes *et al* (eds), *Data Protection and Privacy: The Internet of Bodies* (London: Bloomsbury Publishing, 2019) at 231–248.

[162] For a detailed discussion, see above Part IV.B.3 above.

D. *Developing the Code of Ethics for Algorithms*

In addition to reforming the regulatory framework, ethics is playing an increasingly important role in the governance of algorithmic decision-making. The code of ethics is not legally binding, but it can serve as quasi-legal instruments to guide the design and application of algorithms. Despite the fact that both public and private sectors rely heavily on algorithmic decision-making, these intelligent systems are not morally neutral and bring significant ethical risks in practice.[163] Through continuous optimisation of algorithms, it is likely to make more accurate and efficient decisions; however, there is growing concern about whether such decisions owe an ethical obligation to demonstrate responsibility and care for individuals. For example, a Beijing-based social organisation specialising in legal aid for migrant workers conducted research on the relationship between delivery riders and online service platforms, finding that algorithm-based decisions placed unreasonable demands on the riders.[164] These platforms used algorithms to choose the shortest delivery time as a benchmark for the riders' performance, rather than allowing a reasonable amount of time to complete their delivery work.[165] Such unethical practices in algorithmic decision-making have placed a heavy workload on vulnerable riders. While laws and regulations can set the threshold needed to protect individual rights, they do not always keep pace with the development of algorithms and may not be appropriate to address certain ethical issues. In this regard, non-legal norms can be incorporated in the governance structure to encourage ethical behaviour in algorithmic decision-making and facilitate consensus building within the industry.[166]

On 8 April 2019, the European Commission published the *Ethics Guidelines for Trustworthy AI* to foster and secure ethical and robust artificial intelligence.[167] It states that artificial intelligence systems can equally contribute to the enhancement and deterioration of social skills, thus affecting human and societal well-being.[168] More importantly, artificial intelligence needs to treat individuals as moral subjects rather than as objects to be sifted, sorted, scored or manipulated, and needs to be developed in a way that respects human dignity.[169] In China, the introduction of the 2021 Code of Ethics aims to promote responsible artificial intelligence and provide ethical principles for individuals and organisations engaged in its management, development, supply and use.[170] Given increasingly intelligent decision-making

[163] Andreas Tsamados, Nikita Aggarwal, Josh Cowls, Jessica Morley, Huw Roberts, Marlarosaria Taddeo & Luciano Floridi, "The Ethics of Algorithms: Key Problems and Solutions" (2022) 37(1) AI & Society 215.

[164] Zhicheng Public Interest Lawyers, "The Riders' Dilemma: The Law on Delivery Platform Employment" (13 September 2021), <https://zgnmg.org/%e9%aa%91%e6%89%8b%e8%b0%9c%e4%ba%91%ef%bc%9a%e6%b3%95%e5%be%8b%e5%a6%82%e4%bd%95%e6%89%93%e5%bc%80%e5%a4%96%e5%8d%96%e5%b9%b3%e5%8f%b0%e7%94%a8%e5%b7%a5%e7%9a%84%e3%80%8c%e5%b1%80%e3%80%8d%ef%bc%9f/>.

[165] *Ibid*.

[166] Lee Jyh-An, "Algorithmic Bias and the New Chicago School" (2022) 14(1) Law, Innovation and Technology 95 at 107.

[167] High-Level Expert Group on Artificial Intelligence (EU), *Ethics Guidelines for Trustworthy AI* (2019).

[168] *Ibid* at 19.

[169] *Ibid* at 10.

[170] MOST, "Code of Ethics for New-Generation AI", *supra* note 33 at art 3.

systems and the complexity of application scenarios, it calls for collaboration among different market participants, such as regulators, self-regulatory organisations, regulated institutions and customers, to establish appropriate industry standards and improve ethical performance of algorithms. In line with the general code of ethics, Chinese regulators responsible for different industries can further develop implementation details to adapt to the specific market circumstances, such as the evaluation specification for algorithm applications in the finance sector.

VI. Conclusion

Over the past few years, algorithms have been increasingly used in many different sectors, such as finance, employment and criminal justice, to optimise decision-making processes. This intelligent approach can improve efficiency in data analytics and present great opportunities for innovation. In China, the development of algorithmic decision-making is largely driven by private-sector technology companies with strong analytical capabilities and large amounts of customer data. While algorithms bring significant benefits to different aspects of life, the complex design of decision-making models and the scale of data involved in the process pose serious challenges to the existing regulatory regime. The fundamental problem is how to regulate algorithmic decision-making in a way that does not hinder innovation while ensuring adequate protection of individuals' rights.

In response to the growing concern about the development and use of algorithms, China has gradually established a regulatory framework covering many areas of law. For example, the Personal Information Protection Law lays down specific requirements for automated decision-making and its impacts on individuals. There is also a set of rules governing the provision of algorithm recommendation services and generative artificial intelligence. In addition to mandatory regulations, China has also introduced industry standards and codes of ethics to provide guidance on developing a comprehensive governance structure for algorithms. However, China's regulatory regime is not without its limitations, such as problems related to data requirements, algorithmic transparency and *ex post* mechanisms. Drawing on the regulatory experience of some overseas jurisdictions, including the EU, the US, the UK and Singapore, this paper makes some suggestions for improvement. While relevant rules governing cybersecurity, data security and personal information can provide the basis for the regulation of algorithms, it is worth considering formulating specific requirements for datasets used to develop, test and maintain the automated decision-making systems. China is also advised to strengthen the regulation of algorithms and lay down relevant requirements at different stages of the decision-making process. Furthermore, algorithmic auditing enables professional third parties with risk management expertise and technical competence to assess the performance of decision-making systems and ensure the effective implementation of obligations. In terms of customer protection, China could adopt a series of mechanisms to enhance both private and public enforcement, such as establishing a representative body in civil litigation and introducing substantial fines. Last but not least, a code of ethics should be incorporated in the governance structure of algorithmic decision-making to encourage more ethical business practices.