ISSN 2616-5775 Vol. 5, Issue 10: 1-5, DOI: 10.25236/AJCIS.2022.051001

# Analysis and Governance Proposal of Algorithmic Power Alienation

**Le Wang*, Jun Qian**

*Fadedongheng Law Firm, Nanjing, Jiangsu, China*
**Corresponding author: 13057629523@163.com*

***Abstract:*** *The development of Internet technology has allowed algorithms to gradually deepen their influence on our lives, and have been alienated into the power that can mobilize various factors of production, and targeted governance is imperative. This paper starts from the necessity of power alienation, analyzes the key factors, draws on mature experience, and puts forward feasible suggestions for the current situation.*

***Keywords:*** *Algorithm, Algorithmic power, Algorithmic governance*

## 1. Introduction

On August 27, 2021, the State Internet Information Office announced on the official website about the "*Internet Information Service Algorithm Recommendation Management Regulations (Draft for Comments)*" (hereinafter referred to as "*Algorithm Regulations*"), which will be targeted at the chaos of algorithm recommendation services, showing the determination of the state to govern algorithms. In fact, algorithms are profoundly affecting our lives, in the "personalized push" "big data to kill ripe" "take-out time shrinkage" and other hot topics are behind the penetration of algorithms to society, especially intelligent algorithms with autonomous decision-making capabilities, in fact, has become the deployment of social resources invisible hand, alienated into a kind of power, which makes governance urgently [1].

## 2. The Need for Governance

Unlike algorithms expressed by computers in a binary language in a general sense [2], intelligent algorithms, or algorithms as they are called in this paper, can rely on big data for autonomous learning and self-constructed decision logic to possess, process and output data after the algorithm designer designs the framework logic. What is particularly alarming is that the neutrality of intelligent algorithms is questionable, and their actual embodiment and continual development is the subjective intention of the algorithm designer [3], which inevitably produces power alienation after widespread application, as shown below.

### *2.1. Influence Users' Perceptions*

With the advantage of technology, algorithms have an impact on user perception. In mobile pushing, algorithms can use big data and cloud computing to process massive user data, analyze users' behavioral paths and ways, form "user tags", and push "thousands of people with thousands of faces", thus influencing users' perceptions and causing problems, such as "information cocoon" and "big data killing ripe". More importantly, the algorithm has been technically freed from the "tool" property, after the algorithm is artificially designed framework, its internal computer system, decision-making logic is not controlled, making the algorithm and human behavior separated, such as the search engine ranking misleading; Microsoft's artificial intelligence robot in the Twitter interactive learning, but published a sympathy for Nazi statements, etc.. The uncontrollable nature of technology and the enormous social influence are important reasons for the alienation of algorithmic power [4].

### *2.2. Control Users' Behavior*

Algorithms now form direct norms of behavior in certain Internet domains and have some coercive power to influence and control the behavior of individuals. For example, in Taobao platform, the

ISSN 2616-5775 Vol. 5, Issue 10: 1-5, DOI: 10.25236/AJCIS.2022.051001

algorithm can take the user's Alipay account to cancel the collection, funds stop payment and other coercive measures, the user needs to prove to overturn the conclusion of the algorithm and lift the coercive measures [5]; in the Didi Taxi platform, the allocation and acceptance of orders, the development of the exercise route, the payment and collection of fees, the scoring of drivers and passengers, the determination and punishment of violations are actually completed by the algorithm and automatically implemented. This coercive power to impose measures without consultation constitutes a source of power for algorithmic power in the private sphere.

### *2.3. Influence administrative decisions*

The automaticity, convenience, efficiency and accuracy of algorithms have won the favor of administrative organs. In some scenarios, public authorities rely heavily on algorithms, and even directly base their governance on algorithmic conclusions, such as automatic identification and sentencing of license plates and faces by cameras in traffic violations [7]; the algorithm used by the U.S. Federal Family Tracing Service once misidentified a citizen as a "parent who refused to pay support" and issued a $206,000 fine [8]. Thus, algorithms indirectly acquire the public power of administrative decision makers, which constitutes a source of power for algorithmic power in the public domain.

## 3. The key elements of governance

Algorithms may produce different forms of power alienation in different application scenarios, but ultimately, the root cause of algorithmic power alienation is the algorithmic technology-based, interest-driven algorithmic black box, whose specific characteristics are as follows.

### *3.1. Opaque technology*

Intelligent algorithms are derived from “deep learning” models, which use a neuron-like design with a hidden layer between the input and output layers, commonly known as a “black box”. In the black box, algorithms automatically carry out feature extraction, data training, and autonomous learning, breaking the linear relationship between input and output and blocking the cause-effect connection, which conceals the profit-driven nature of algorithmic power[9]: algorithm designers and controllers are driven by profit, unable to be objective and accurate in algorithm model design and input, while the black box further strengthens the subjective color, aggravates bias and interest orientation, and ultimately outputs “bad results”[10]. However, when the algorithm makes a wrong decision or infringes on the legal rights of the relator, the culprit is able to escape responsibility by claiming "technology neutrality".

### *3.2. No obligation to disclose*

As a technical secret, the holder of an algorithm is granted by law the right not to disclose it. However, unlike technical secrets in the usual legal sense, the subjective overtones of the algorithm itself give this type of protection the potential to act as an accomplice to the tiger. A typical case is Wisconsin v. Eric-Loomis, in which the state Supreme Court denied Loomis' appeal and did not require the vendor to disclose the algorithm or explain it [11]. A non-profit organization had conducted a statistical analysis of the extensive results of the COMPAS algorithm provided in the above case, Northpointe's Trade Secrets, which showed that black defendants were twice as likely to score higher than whites [12]. It follows that the protection of algorithms as technical secrets is likely to harbor the use of algorithms to commit commercial fraud and deceive the public for profit.

At the same time, when algorithmic decisions in administration lead to undue infringement of the public, it is difficult for the public to request government agencies to disclose the algorithm and explain the legality of the algorithm's design and the fairness of the operation results, and to prove the liability of algorithmic infringement, which makes the civil rights infringed without effective remedies [13]. This situation leads to the loss of government credibility, while causing the designers and deployers of the algorithm to use the "algorithm black box" to complete regulatory escapades.

Moreover, when users use the software and accept the user agreement, the algorithmic power already uses the format clause to make users voluntarily surrender control of their personal information, agree to the algorithm's limitation of their rights, and specify the remedy in favor of the algorithmic power. The use of technology neutrality and user consent as a barrier to evade accountability puts the attribution of responsibility to algorithmic power in a difficult position [14].

ISSN 2616-5775 Vol. 5, Issue 10: 1-5, DOI: 10.25236/AJCIS.2022.051001

## 4. Governance Experience

The phenomenon of alienation of algorithmic power has aroused widespread concern in the international community, and developed countries and regions such as the United States and the European Union have developed a number of algorithmic governance experiences that can be drawn on after years of exploration and combined with their own cultural backgrounds.

### *4.1. Algorithmic accountabilit regulatory model in the United States*

As a pioneer of the Internet, the United States responded to the systemic risks of algorithms earlier. The American Computer Society released "*The Statement on Algorithmic Transparency and Responsibility*" in 2017, which proposed seven principles to promote algorithmic transparency and enhance algorithmic reliability, among which is the establishment of a regulatory system. In the same year, the New York City Council passed the first AI regulation bill, the "*Automated Governmental Decision Systems Act*," which requires the establishment of a system of oversight and remedy regarding the fairness, accountability and transparency of algorithms. In 2019, members of the U.S. House and Senate introduced the "*Algorithmic Accountability Act (2019)*", which would require algorithm holders to self-censor the "accuracy, fairness, bias, discrimination, privacy, and security" of their algorithms and would propose granting regulatory authority to the Federal Trade Commission. This shows that the U.S. governance system is centered on "algorithmic accountability" and an external control model that emphasizes checks and balances of power and avoids direct government intervention as much as possible.

### *4.2. The EU's "Enriched User Rights" control model*

Unlike the compartmentalized and specialized governance of the United States, the EU has embedded algorithmic governance within its data protection framework. As early as 1995, the EU enacted the "*Data Protection Directive*" to establish a basic framework for data protection. In 2015, to further break down digital barriers in member states, the EU introduced the "*Digital Single Market Strategy*", which calls for a comprehensive evaluation of online platforms as well as Internet intermediary service providers to develop a subsequent regulatory framework. The EU immediately adopted the "*Robot Civil Liability Act*" and the "*General Data Protection Regulation*" in 2017 and 2018, to clarify the legal responsibilities of relevant subjects and systematically establish an accountability mechanism centered on the responsibilities and obligations of data controllers and processors. With the gradual establishment of a strict, standardized and systematic data protection system, the EU has also constructed a governance system for algorithms, which has evolved along with the development of the data protection framework, with the core of gaining the rights of data subjects and continuously strengthening the external supervision system for the standardized application of algorithms from the legal system level.

## 5. Current Status and Recommendations

Compared with the United States and the European Union, China's mobile Internet is developing rapidly and there are various forms of algorithmic power alienation, but China has a late start on algorithmic governance and there is no unified legislation yet. Relevant regulations are scattered in the laws and regulations on personal information protection, information security, platform monopoly, industry access, regional governance, etc., such as the "*Personal Information Protection Law*", the "*Anti-Monopoly Guidelines on the Platform Economy*", the "*Interim Regulations on the Management of Online Tourism Business Services*", and the "*Data Regulations of Shenzhen Special Economic Zone*".

(a) "*Algorithm Regulations*" Article 7, Article 14 are mentioned algorithm recommendation service providers on algorithm recommendation related service rules, basic principles, purpose intent, operation mechanism for public disclosure, but did not clarify the scope of public disclosure, public disclosure mode, disclosure degree, the actual operation of enterprises have difficulties. As a necessary means to ensure the transparency of algorithms, algorithm information disclosure should balance the user's right to know with the interests of algorithm holders, and should be chosen in an appropriate way. Therefore, we can try to fully disclose the algorithm operation rules and the creation verification process, and follow the example of setting up an "audit trail" to ensure that the algorithm design and operation can be traced and understood by general users [15]. At the same time, there should not be mandatory full disclosure of the algorithm, and the data uploading and filing can be done in the way of key item concealment for the part involving enterprise trade secrets to control the scope of disclosure.

ISSN 2616-5775 Vol. 5, Issue 10: 1-5, DOI: 10.25236/AJCIS.2022.051001

(b) "*Algorithm regulations*" Article 7, Article 8 mentioned the audit and verification of the mechanism of the algorithm, from the system compliance, the maintenance of public order and morality to make it clear as the main responsibility of the algorithm recommendation service providers, but did not specify the implementation details and definition of standards, the actual supervision of the relevant departments is extremely difficult. With reference to the mature experience of EU, the supervision of algorithms can be combined with internal audit and external administrative supervision of enterprises.

In the area of private rights, we can follow the example of the EU in setting up a data protection officer (DPO) system. The EU's "*General Data Protection Regulation*", Article 37(5) and Article 39(1), mandates the establishment of DPOs, which require independent and professionally educated data protection officers to supervise data processing activities within the enterprise, including auditing data security, monitoring the operational status and results of algorithms, and providing audit recommendations to the enterprise. Some Chinese companies have already introduced the system for internal auditing of algorithms, such as China Eastern Airlines, which established a DPO position in June 2018, becoming the first company in China to establish a "data protection officer", and Huawei, which has appointed a European Union DPO in its official response to the issue.

In the area of public power, the relevant administrative departments should construct an audit supervision system. Unlike the aforementioned DPO internal audit system, the audit oversight system is a reflection of the administrative function, and it is a gap-checking system for the DPO internal audit system. A special audit of the algorithm holder's data processing policy and behavior may be conducted by an independent auditor, which may be conducted on an annual basis to maintain the transparency of the algorithm's operation, and the specific audit shall include but not be limited to the legality, fairness, effectiveness, and transparency of the algorithm's design. This audit system is covered in India's "*Personal Data Protection Act 2019*", as well as in our "*Information Security Technology - Personal Information Security Code*", which was enacted on October 1, 2020, but is not yet a mandatory norm in China.

(c) The "*Algorithm Regulation*" is a useful attempt for algorithm governance in China, and if it is adopted, its final implementation effect will determine the legislative thinking of the higher law. The current "*Algorithm Regulations*" emphasize administrative supervision, the object of which is limited to algorithm recommendation service providers, showing the tendency of focusing on supervision and not suppressing applications, but thus leading to the lack of both the scope of recourse and the intensity of supervision. In order to effectively curb the possibility of alienation of algorithmic power and prevent the social risks caused by algorithmic infringement, we should first clarify the subject of algorithmic responsibility. In the absence of relevant provisions in the current law, the principle of "piercing the corporate veil" can be referred to corporate law, and algorithms can be subject to penetrating regulation and liability, i.e. the designer, deployer and owner of the algorithm should be held liable for infringement [16-17]. Second, clarify the rules of tort liability. In algorithmic infringement, the infringer is in a disadvantageous position while the controller of the algorithm is in a strong position. Therefore, the controller of the algorithm should have a higher duty of care, and in order to balance the difference between the two parties, the burden of proof should be in favor of the infringer. Finally, the exclusion of liability needs to be carefully limited. The algorithm has the data characteristics of "algorithmic black box" and the exemption barrier of "informed consent" of users, which can easily avoid tort liability, and the loose exemption is not conducive to the protection of users' rights and interests.

## 6. Conclusion

The development of technology has unwittingly brought mankind into the "age of power" of algorithms. People cannot deny the existence of the digital era, nor can they stop the digital era from moving forward, just like human beings cannot fight against the power of nature. In the face of the alienation of algorithmic power, the best approach is to trace the root cause, prescribe the right medicine, outline the boundaries of its power by law, and prevent the abuse of power.

## References

*[1] B.H. Raven: Power and Social Influence, Ivan Dale Steiner& Martin Fishbein(eds.), Current Studies in Social Psychology, Holt, Rinehart and Winston, 1968, pp.127—145*
*[2] [US] Christopher Steiner, "Algorithmic Empire", translated by Li Shiaoying, People's Post and Telecommunications Publishing House, 2014, p. 132.*

ISSN 2616-5775 Vol. 5, Issue 10: 1-5, DOI: 10.25236/AJCIS.2022.051001

*[3] Peng, Lan. Survival, cognition, and relationships: how algorithms will change us[J]. Journalism, 2021(03): 45-53.*
*[4] Sandra Barman, Change of State: Information, Policy, and Power, The MIT Press, 2006, p.11—12.*
*[5] Article 6.1 of the Taobao Platform Service Agreement (effective date 08/19/2019). https://terms. alicdn.com/legal-agreement/terms/TD/TD201609301342_19559.html, 2021-09-11.*
*[6] Zheng Yushuang. Cracking the technology neutrality conundrum-Jurisprudence of the relationship between law and technology rethought[J]. Journal of East China University of Political Science and Law, 2018, 21(01): 85-97.*
*[7] Empowering big data to build a smart transportation ecosystem, http://www.rmjtxw.com/news/ dsj/40968.html, 2021-09-11.*
*[8] [US] Luke Dormer, The Age of Algorithms: New Engines for the New Economy, translated by Hu Xiaorui and Zhong Yi, CITIC Publishing Group, 2016, p. 56.*
*[9] Tan Jiusheng, Fan Xiaoyun. The causes, risks and governance of algorithmic "black boxes" [J]. Journal of Hunan University of Science and Technology (Social Science Edition), 2020, 23(06): 92-99.*
*[10] Zhang Shuling, Cracking the black box: Algorithmic power regulation and transparent realization mechanism in the era of smart media [J]. China Publishing, 2018(07): 49-53.*
*[11] In Wisconsin v. Eric Loomis, the sentencing phase court adopted the COMPAS recidivism evaluation, prompting Loomis to appeal on the grounds that the court's reliance on COMPAS violated his due process rights and his right to equality. The state Supreme Court ultimately upheld the initial sentence. 2020.*
*[12] Jeff Larson, eta, How We Analyzed the COMPAS recidivism Algorithm. https://www.propublica.org /article/how we analyzed the compas recidivism algorithm. 2021-09-11*
*[13] Zhang Linghan, The conflict and reconciliation between algorithmic automated decision-making and administrative due process system [J]. Eastern Jurisprudence, 2020(06): 4-17.*
*[14] Ning Yuan, The adherence and amendment of the rule of informed consent in personal information protection [J]. Journal of Jiangxi University of Finance and Economics, 2020(02): 115-127.*
*[15] Zhang Linghan: A study of algorithmic interpretation power of business automated decision making [J]. Legal Science (Journal of Northwestern University of Political Science and Law), 2018, 36(03): 65-74.*
*[16] Wang Qinghua, The path of legal regulation of artificial intelligence: A framework discussion [J]. Modern Jurisprudence, 2019, 41(02): 54-63.*
*[17] [US] Nicholas Negroponte, Digital Survival, translated by Hu Yong and Fan Haiyan, Beijing: Electronic Industry Press, 2017, p. 299.*