

Research on the legal path of protecting citizens' privacy from the perspective of anti-money laundering law

Yan Lu

Department of Civil and Commercial Economic Law, China University of Political Science and Law,
Beijing, China

Abstract: Anti-money laundering laws and regulations play an important role in cracking down on crimes and stabilizing finance. The 2021 Anti-Money Laundering (Revised Draft) in China strengthened its system value. However, things always have two sides, and the legal system also has certain risks, especially the lack of protection of citizens' basic rights. Citizens' basic rights and anti-money laundering are not contradictory but complementary. Only by protecting citizens' basic rights can citizens' information be established and anti-money laundering work be better promoted. This paper analyzes the risks from the perspective of privacy (including "the right to keep privacy secret" and "the right to maintain privacy from illegal infringement"), and puts forward solutions to provide ideas for further improving the series of laws and regulations of the Anti-Money Laundering Law.

Keywords: Anti-money laundering law, Protection of citizens' right to privacy, Anti-money laundering and privacy protection

1. Introduction

"money laundering" is to convert illegal gains into legal ownership by certain means, which integrates the proceeds of crime into the legal economy, enables criminals to enjoy the fruits of criminal activities, and hides the evidence of illegal and illegal sources of funds. Studies have shown that the purpose of anti-money laundering work is to identify and confiscate the proceeds of basic crimes. However, the Anti-Money Laundering Law itself has a tendency to sacrifice personal interests to a certain extent for public interests, such as the possibility of excessive infringement of citizens' privacy rights. Therefore, the objective of the current study is that the public needs to realize that there is no contradiction between combating money laundering and protecting citizens' privacy from the perspective of anti-money laundering. In the long run, only by protecting citizens' privacy can they increase their trust and cooperate with their anti-money laundering tasks when dealing with financial institutions or non-financial institutions. Therefore, it is necessary to study how to seek a balanced path between combating money laundering and protecting human rights.

2. Theoretical basis of dual protection of citizens' privacy in anti-money laundering

China's anti-money laundering authority [*In this paper, it refers to the administrative department authorized by law. Article 19 of China's Anti-Money Laundering Law (Revised Draft) stipulates: "The administrative department in charge of anti-money laundering in the State Council shall carry out or cooperate with relevant organs, departments and institutions in the State Council to carry out money laundering risk assessment of the state, industries, financial institutions and specific non-financial institutions."*] will not neglect the protection of citizens' privacy in its anti-money laundering work, but the author of this paper thinks that different standards should be adopted for privacy protection in the two different processes of collecting information and using information. That is to say, when the anti-money laundering obligation agency [*In this paper, it refers to financial institutions, non-financial institutions and other voluntary organizations that impose anti-money laundering responsibilities by law.*] obtains citizens' transaction information, it uses different logic to make judgments in order to seek a balanced path between anti-money laundering work and privacy protection. There is logical support for this division: first, in the information collection stage, citizens'

transactions not only involve basic personal information such as name and occupation, but also sensitive information such as counterparties to the transaction and transaction amounts. Compared with ordinary information, the legal protection requirements for financial sensitive information are higher. Therefore, the extent to which anti-money laundering obligations agencies collect information, the scope of collected information, and the requirements for the credibility of information sources, etc., require further refinement of legal regulations. This is so called the "privacy right" in this paper. Secondly, in the stage of information anti-money laundering, laws and regulations need to clearly specify the extent to which sensitive information can meet the privacy protection requirements, anti-money laundering obligation agencies must adopt information protection technical means, the time limit for their retention of citizen information, and so on, all of which need to be further refined to meet the purpose of protecting citizens' privacy. This is so called "the privacy protection right" in this paper.

Like the traditional right to privacy in civil law, the protection of privacy in anti-money laundering is still to protect the interests of personality, that is, to protect citizens' personality rights. Citizen's "information right" in anti-money laundering is an extension of personal information right in the field of anti-money laundering, which exists to protect public interests. China's Civil Code classifies citizens' right to personal information protection as "personality right", and juxtaposes "personal information" and "privacy right", which shows that they are not included, but two independent personality rights to protect different personality legal interests. This division has a historical background. The awareness of privacy protection was awakened in the United States in the 1880s. It originated from the concern for personal interests and focused on the protection of the tranquility of private life. It is the part that individuals are unwilling to let others know except for the public interest part. It is the right of an individual to independently manage personal information without interference from a third party. The protection of personal information is a product of the era of the third industrial revolution, emphasizing whether individuals can make their own decisions.

The author believes that the similar principle is also applicable to the Anti-Money Laundering Law, that is, the legal interests protected in the anti-money laundering information collection stage are biased towards the "privacy right" protection here, that is, "the right to keep privacy secret"; The protection of information anti-money laundering processing stage is biased towards the protection of "personal information" here, that is, "the right to maintain privacy from illegal infringement".[*Guodan, Legal definition of financial consumers, Academic exchange, 2010, 8(2): 54-57: The right to financial privacy is included in the civil rights system of participating in transactions, and it is further subdivided into the right to keep financial privacy secret and the right to maintain financial privacy from illegal infringement, which this paper can learn from.*]

In this article, the so-called "the right to keep privacy secret" refers to the right of citizens to reserve personal information irrelevant to the public interest of anti money laundering when the anti money laundering obligation authority conducts transactions, and the right not to be peeped by others. It is a kind of Personality rights that reserves information other than specific information from illegal intrusion, knowledge, collection, use and disclosure by others under special circumstances. The so-called "the right to maintain privacy from illegal infringement" refers to the right of citizens to demand that anti money laundering obligations institutions not infringe upon personal information collected during the exercise of their powers, except for the public interest of anti money laundering as stipulated by law. If violated, citizens have the right to seek relief from public authorities or take private remedies permitted by law.

3. Risk analysis of citizens' privacy rights being violated in anti money laundering

Although the draft of Anti-money laundering issued by China in 2021 greatly makes up for the previous shortcomings and is conducive to promoting international cooperation, it is problematic to expand the public power of anti-money laundering without detailed regulation in time, and it may

even damage the privacy of citizens, for example, in order to better curb money laundering activities, increase the enthusiasm of the whole people to combat money laundering. To improve the efficiency of anti-money laundering, anti-money laundering voluntary agencies need to extensively collect and retain personal data of citizens and disclose it to anti-money laundering authorities. During this period, there may be a risk of infringing upon citizens' personal data due to illegal collection and use.

3.1 Risk of infringement of citizens' "the right to keep privacy secret"

The draft of China's Anti Money Laundering Law has expanded the obligation subject of anti money laundering, that is, individual citizens also have anti money laundering obligations, and their way of fulfilling obligations is through the active cooperation of obligation institutions in due diligence and other work. [Article 35 states, *"Any unit or individual shall have the obligation to conduct due diligence in the process of establishing and maintaining business relationships with financial institutions and specific non-financial institutions... to truthfully provide information related to the purpose and nature of establishing business relationships or transactions, as well as the source and purpose of funds."*] In addition, Article 36 of the Anti Money Laundering Law (Draft) also stipulates the obligation to independently report transactions with significant amounts in cash that are not conducted through financial institutions. These additional provisions expand the possibility of protecting the public interest by expanding the subject of obligations, but due to the lack of specific and detailed regulatory documents, and personal information has huge convertible value. For example, big data's preference design is based on the collection of citizen information, and anti-money laundering obligation agencies are for profit, so they naturally have a tendency to expand the scope of collecting citizen information. This poses a potential risk to the privacy of citizens. In practice, it is not uncommon for anti-money laundering voluntary agencies to collect citizen information beyond the scope. For example, the China Consumer Association has tested and evaluated the personal information collection and privacy infringement of 100 mobile phone applications. It is found that more than 90% of the applications are overcollected, of which the financial institutions, as one of the anti-money laundering obligations, are the most serious. [XUE Qiu. *"Suspected of collecting personal privacy beyond the scope, many banks have completed rectification"*. Arrival at: <https://xueqiu.com/2904895572/138959113>.(last accessed: 13/05/2023).] Therefore, once the authorities concerned do not legally regulate the scope and methods of information collection of anti-money laundering agencies, but blindly emphasize the individual's responsibility for anti-money laundering and cooperate with the responsibility of collecting due diligence information, it is very permissible for voluntary agencies to abuse their power and infringe upon the right of citizens to keep personal information confidential which has nothing to do with the public interest.

3.2 Risk of infringement of citizens'"the right to maintain privacy from illegal infringement"

If there are no relevant laws and regulations for regulation in the processing, submission and storage of anti-money laundering citizen information collected by anti-money laundering obligation agencies, it is easy to lower the standard of information protection, and even abuse the collected information for profit, infringing upon the right of citizens' information to be protected from illegal use.

Firstly, if the anti-money laundering system does not have the technical conditions to match its responsibilities, and the citizens' information processing and storage institutions lack the technical means to keep pace with the times, the citizens'"the right to maintain privacy from illegal infringement" will be exposed and tampered with. The information collected by anti-money laundering agencies is stored in their respective information storage centers. on the one hand, the information is separated, and China's anti-money laundering monitoring center can not well identify money laundering, because money laundering itself is a series of acts, separation may not be money laundering, comprehensive evaluation is money laundering, but because the anti-money laundering monitoring center does not have enough technology of comprehensive information processing, it will lead to regulatory loopholes. On the other hand, with the continuous development and utilization of Artificial Intelligence, Block Chain, Cloud Computing, Internet of Things and other technologies, if

the data storage system of anti-money laundering agencies cannot be updated in time, there is a great risk of information being tampered with and leaked. In practice, anti-money laundering obligation agencies will outsource information storage and processing to third-party organizations, which will increase the risk coefficient of data tampering and disclosure. In addition, the fourth chapter of China's Cyber Security Law clearly emphasizes the responsibility of data users to prevent data from being tampered with and leaked; The Guidelines for Data Governance of Banking Financial Institutions require business institutions to use mobile phone data according to laws and regulations, protect customer privacy and improve technology. Therefore, it is necessary to upgrade the institutional technology.

Secondly, if the collected citizens' information does not have relevant supporting implementation rules to support the classified and targeted protection of information, there is a risk of infringing citizens' right to know and consent. In the information collection of citizens by anti-money laundering obligation agencies, once citizens provide personal information, they lose control over it. In order for citizens to monitor that their information is not abused by the anti-money laundering obligation organs and can be deleted and desensitized in time, citizens should have the right to ask the anti-money laundering obligation organs to inform them of the scope, methods and purposes of information processing and the policy basis. However, in practice, anti-money laundering agencies usually use lengthy privacy format agreements to make citizens reach an agreement without fully understanding it. What's more, if they don't meet the relevant agreements, they can't conduct relevant transactions. In addition, there is a risk of infringing citizens' right to consent to the second use of the collected information beyond the original purpose. If the anti-money laundering obligation agency processes personal data beyond the scope of public interest, it must obtain the consent of individual. Due to the lack of perfect supervision and restriction, in practice, there are a large number of behaviors that anti-money laundering obligation agencies transfer the collected citizen information beyond the authorized scope for profit. In the name of improving transaction efficiency and stabilizing the trading market, the act of processing information without citizens' authorization will infringe on citizens' basic rights.

4. Suggestions on possible ways to protect citizens' privacy rights under the Anti-Money Laundering Law

Even though governments of all countries recognize anti-money laundering as a priority of government regulation at all levels, the purpose of government regulation is to maintain financial stability and for every individual citizen. It is not advisable to overemphasize macro public interests while ignoring the protection of micro individual interests. Therefore, it is necessary to strike a balance between the anti-money laundering duty agency and the protection of citizens' right to privacy.

4.1 Common Suggestions on the Protection of "Two Privacy Rights"

When the personal interests of privacy conflict with public interests, it is necessary to follow the principle of equivalence when formulating legal rules. Whether it is the "right to keep privacy confidential" or the "right to maintain privacy from illegal infringement", the principle of equivalence needs to be followed in the process of collecting and processing personal financial information. In other words, if there are policy purposes other than combating money-laundering and terrorist financing, which do not seem to have appropriate interests to support the processing of citizen data collected for anti-money-laundering, then this violates the protection principle of proportionality restrictions.

In the personal Information Protection Law of China, Article 6 clearly points out that personal information processing must have a clear and reasonable purpose and a way that has the least impact on personal rights and interests. In the legal practice of various countries, in order to better achieve the goal of anti-money laundering, EU Directive 2015/849 requires EU member state to establish a beneficial ownership register (RBO), which contains the personal data of the owners of each legal

entity in the member state, such as their names, nationalities and ownership interests, and makes the RBO available to a series of financial entities such as banks. [Article 30(1), Directive 2015/849 of the European Parliament and the Council of 20 May 2015 on preventing the use of the financial system for money laundering or the financing of terrorism (EU). It amends Regulation (EU) No. 648/2012 of the European Parliament and of the Council and repeals Directive 2005/60/EC of the European Parliament and of the Council and Council Directive 2006/70/EC] Directive 2018/843 is an extension of the directive in 2015, allowing any ordinary member of the public to access RBO, regardless of whether they can prove their legitimate interests. [Article 1, Directive (EU) 2018/843 of the European Parliament and the Council of 30 May 2018, amending Directive (EU) 2015/849 on preventing the use of the financial system to launder money or finance terrorism, and amending Directives 2009/138/EC and 2013/36/EU.] In 2022, the European Court of Justice made judgments in joint cases C-37/20 and C-601/20, arguing that the provisions of the EU anti-money laundering directive on the publication of the beneficial ownership register were inconsistent with the EU Charter of Fundamental Rights. The court held that although preventing money laundering is an effective goal, providing data to the public is neither a necessary nor an appropriate way to achieve this goal, thus violating the EU Charter of Fundamental Rights. [Court of Justice of European Union. "Judgment of the Court in Joined Cases C-37/20 | Luxembourg Business Registers and C-601/20". Arrival at: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188en.pdf>. (Last accessed: 04/05/2023)] This judgment has also promoted the improvement of the EU anti-washing regulations. Then, in 2021, the European Commission proposed the establishment of anti-money laundering regulations 2021/0240 [Proposal of the European Parliament and the Council on the establishment of the Anti-Money Laundering and Combating the Financing of Terrorism Authority and the amendment of Regulations (EU) 1093/2010, (EU) 1094/2010 and (EU) 1095/2010.] and 2021/0239 [Proposal for a regulation of the European Parliament and the Council on preventing the use of the financial system to launder money or finance terrorism.] to the European Anti-money Laundering Administration, which provided a reference template for the balance between regulating financial crimes and privacy protection.

When determining the degree of "equivalence", we can take public safety as one of the criteria, that is, when the anti-money laundering authorities need to obtain citizen information in the process of anti-money laundering, they need to use it as a reference indicator. If they can achieve their goals through other alternative information, they don't need to obtain citizen information. If they only need to obtain a low proportion of citizen data information to achieve their goals, they can't obtain a high proportion of data. For example, since regulators should also pay attention to strengthening anti-money laundering information and intelligence exchange, and adopt regular or irregular information consultation, clue research and special discussion to find out the characteristic problems in time to promote the safe and efficient sharing of data and information among departments under the strict implementation of confidentiality discipline, it is unnecessary to retrieve the same information repeatedly if it is not necessary.

4.2 Suggestions on the Protection of Citizens' "Right to Keep Privacy Confidential"

Firstly, the law defines the principles of citizen information collection of anti-money laundering obligation institutions through detailed rules, including the principles of relevance, completeness, accuracy and timeliness. First of all, the data collected by anti-money laundering agencies must be relevant to the purpose and must not exceed the limited scope to avoid excessive infringement of citizens' right to keep privacy confidential. Then, the citizen data collected by anti-money laundering agencies must be complete and without omitted, comprehensive and without any subjectivity. Finally, the citizen information collected by anti-money laundering agencies should be updated in a timely manner, that is, due diligence on citizens in transactions does not end over just once. Once it is subjective and not updated in time, it is extremely easy for the anti-money laundering obligation agency to make mistake when reporting large transactions to the China Anti-money Laundering Monitoring and Analysis Center, and mistakenly include ordinary citizens in the list monitoring system [For example, it is necessary to implement restrictive trading measures on the targets listed

on the United Nations sanctions list, and strengthen due diligence measures on politically exposed persons (PEPs).], then the anti-money laundering authority will have a greater chance to investigate the information of citizens outside the scope of ordinary investigation, which will infringe on the privacy of innocent ordinary citizens. In this regard, it can be learned from China's "Information Security Technology Personal Information Security Standard", and give detailed and clear guidance on the collection, use and sharing of personal information by enterprises.

Secondly, Improve the relevant system of restrictions on financial institutions or non-financial institutions when conducting due diligence. Specifically, some unnecessary due diligence can be filtered through laws and regulations that clearly specify the amount of transactions that need to collect information. Both the United States and the European Union have adopted this approach. Directive(EU) 2015/849 of the European Parliament and of the council (The EU Anti-Money Laundering Directive IV) requires obligatory entities to carry out detailed investigation initiation limits for customer due diligence when entering into a business relationship or executing a temporary transaction, i.e. under Article 13, regardless of whether the transaction involves a single operation or multiple operations that appear to be linked, as long as it reaches €15,000 or more; Or, in the case of physical transactions, in the case of cash transactions, the amount reached 10,000 euros or more; Or for providers of gambling services, when conducting transactions totaling €2,000 or more (while collecting winnings, placing bets or both), if there is a suspicion of money laundering or terrorist financing, or if there is doubt about the authenticity of previous due diligence, the obliging entity must carry out additional customer due diligence. The United States requires that cash transactions above \$10,000 be reported to the anti-money laundering monitoring agency, but there is no limit to the amount of information reported for non-cash transactions [IRS. "Form 8300 and Reporting Cash Payments of Over \$10,000, 2023". arrival at: <https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000>, (last accessed: 05/06/2023)], which is related to the historical background of more emphasis on civil liberties than the European Union.

In China, only general regulations require anti-money laundering agencies to report natural person customers' cash payment transactions of more than 50,000 yuan or domestic transfer transactions of more than 500,000 yuan. [Article 5, Measures for the Administration of large transactions and suspicious transaction reports of Financial institutions in China] For example, the due diligence of depositing or withdrawing 50,000 yuan in remote areas for a series of transaction purposes and sources of funds is highly enforceable. For economic development areas, on the one hand, this amount is less enforceable; on the other hand, when too many people in the area reach this limit, the privacy of citizens and the protection of legal interests violate the principle of equivalence. Therefore, this quota can consider the feasibility of various provinces and autonomous regions to formulate their own, and consider raising this normative document to laws and regulations on the basis of perfection.

Suggestions on the Protection of Citizens' Right to Maintain Privacy from illegal Infringement

Firstly, the authorities can formulate relevant rules to encourage anti-money laundering obligation agencies to improve their information processing and storage technologies. First of all, citizens provide personal information in transactions with anti-money laundering agencies, including information of citizens themselves, information of counterparties and information of financial institutions. Compared to ordinary information, it involves higher sensitivity and is more likely to be attacked by criminals, so it is necessary to improve technical capabilities in storage and encryption methods. In order to increase the enthusiasm of anti-money laundering obligatory institutions, a unified evaluation system for citizens' information security protection should be established through normative documents, including evaluation subjects, evaluation timeliness, evaluation standards, etc. Besides, through regular operational training, the operational capacity of staff of anti-money laundering voluntary agencies can be improved in order to improve staff efficiency as well as their risk response capacity. Finally, the implementation of the personal responsibility system, refined to personal responsibility, which can be achieved through the macro normative document requirements, the details of regulation can be set up by each department. For example, in practice, the Bank of China

has established a "customer information traceability mechanism" to accept customer complaints and follow up. Once the information is leaked, it can be blamed to the specific responsible person in time.

In addition, the technology of information exchange and coordination among anti-money-laundering obligation agencies should be improved. Improving technical capability is not only an effective means to implement the confidentiality of citizens' information, but also an effective tool to improve the efficient and comprehensive anti-money laundering management of anti-money laundering authorities. Under the current legal framework, suspicious transaction reports and large-value transaction reports cannot be shared among anti-money laundering obligatory agencies, and there is a lack of mutual information governance coordination and linkage, which cannot achieve a good overall protection. In 2020, the research group of the Anti-Money Laundering Bureau of the People's Bank of China proposed "building a blockchain platform to realize the sharing of anti-money laundering information among different financial institutions", focusing on the advantages of blockchain technology, and deeply exploring the construction ideas and methods of building blockchain in different scopes such as single, multiple and national financial institutions. But this is a technical idea without institutional support. Citizens' information collected by anti-money laundering obligation agencies may be exposed when it is transferred to the authority or within the anti-money laundering obligation agency system. Therefore, it is necessary to use normative documents to require anti-money laundering obligation agencies to determine appropriate protection technologies through normative documents and build a dynamic and on-demand systematic technical protection system. It is conceivable that with the continuous maturity of big data and artificial intelligence technology, the collection and processing of citizen information in doing business with anti-money laundering agencies in the future is likely to become a "machine" execution. Therefore, the anti-money laundering law needs to regulate how to use technical means through rules. Engineering-based calculation can ensure that there is no third-party intervention from source data to results, and the calculation process can be documented through blockchain and other technologies, so that problems can be dealt with in time when found. The formulation of standards depends on the different policy positions of the national authorities of various countries. When the anti-money laundering authority needs to obtain citizens' data, it will not let the anti-money laundering business personnel of a single financial institution or non-financial institution make these decisions about where to set boundaries, how deep to protect the data, for whom to protect the data, and under what terms to protect data, etc.. Article 7 of the personal Information Protection Law of China points out that personal information processors must disclose the rules of processing, and clearly state the purpose, method and scope of processing. Article 21 points out that "where a personal information processor entrusts a third party to deal with personal information, he shall agree with the trustee on a series of means for entrusted processing, and supervise the personal information processing activities of the trustee". In Denmark, when applying high-tech financial anti-money laundering monitoring technology, the Danish Anti-money laundering working Group stressed that sharing IT systems is an important means of improving the efficiency of anti-money laundering control, while also posing "regulatory challenges". Too strict enforcement of EU data protection rules may hinder banks' ability to effectively combat money laundering, said Linda Nielsen, chair of the working group. However, Kaiser said that banks also deal with data that are "not strictly required by legal obligations" in their efforts to monitor money laundering, and in this case, it is not clear to what extent the EU data Protection regulations allow. He called for "inclusive and pragmatic guidance on how to interpret GDPR in the context of anti-money laundering", which he said should be developed in conjunction with the European Banking Authority, which is responsible for ensuring the consistent and effective application of EU anti-money laundering directives. [Maria Bergström, "The Many Uses of Anti-Money Laundering Regulation—Over Time and into the Future", *German Law Journal*, 2018, 5(1):1149-1167] Sanctions or measures against money laundering must be effective, proportionate and dissuasive. If EU laws do not specifically stipulate any punishment for acts violating EU laws, or refer to national laws, regulations and administrative provisions, member States are free to choose the applicable punishment, that is, administrative punishment, criminal punishment or a combination

of the two, then there will be "different punishment for the same crime", that is, the punishment generated under the EU system only needs to comply with the EU Charter of Fundamental Rights and be effective, moderate and dissuasive. However, any measure based on Article 83 (1) of the TFEU will not leave such freedom to member States, and at this point we can see the need for a uniform standard, there will be no unfairness, and there will be no differences between the EU because of different standards. Therefore, a unified standard is conducive to efficiently promoting data collection and reducing the instability caused by unbalanced treatment. However, based on the fact that China is a multi-ethnic country with a vast territory, unbalanced development between east and west, south and north, and unbalanced technology, the issue of local autonomy should also be taken into account when formulating relevant standards.

5. Conclusion

When dealing with the problems existing in the anti-money laundering work, the anti-money laundering authority should realize that it is as important to ensure the realization of the anti-money laundering goal as not infringing on the basic rights of citizens. When considering the principle of equivalence, because of the differences of national conditions, it needs to be evaluated against the human rights catalogues of various countries. At present, there is a lack of fully unified legal norms to ensure that the responsibility of anti-money-laundering reporting is commensurate with the seriousness of the crime, the value of criminal property and the interests of anti-money-laundering law enforcement agencies. Therefore, the obligatory anti-money laundering entity must be able to prove that its policies and procedures for data collection and processing are commensurate with the risks posed by customers, and when the relevant legal system has no clear provisions on the appropriateness in the process of the game, it is necessary for the obligatory subject to weigh the interests under this principle.

If China's privacy protection in the Anti-money laundering Law does not meet the standards of international practice, it will not be conducive to cracking down on transnational money laundering. For example, the EU data Protection Directive forbids member States from transmitting personal data to countries that do not meet the EU data protection level, although it protects member States from illegal infringement to a certain extent by blocking cross-border flows, however, in the long run, it will not be conducive to the development of cross-border business. At the same time, the authority needs to realize that although most countries support the protection of the right to privacy in the Anti-money laundering Law, there are differences in legal concepts, moral standards and cultural backgrounds in different countries. This leads to differences in the scope of privacy protection, which in turn affects the use of the Anti-money laundering Law. So, when formulating rules, power organs need to refer to international practice to refine the protection of citizens' right to privacy in the normative documents of anti-money laundering in accordance with local conditions.

References

- [1] Zheng Yan, "Principles of Anti-Money Laundering Law", Research on legal regulation of personal data processing by financial institutions, 1st, Liaoning University Press, China, 2021, 15-23.
- [2] Guodan, "Legal definition of financial consumers", Academic exchange, 2010, 8(2):54-57.
- [3] XUE Qiu. "Suspected of collecting personal privacy beyond the scope, many banks have completed rectification". Arrival at: <https://xueqiu.com/2904895572/138959113>. (last accessed: 13/05/2023).
- [4] Court of Justice of European Union. "Judgment of the Court in Joined Cases C-37/20 [Luxembourg Business Registers and C-601/20". Arrival at: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188en.pdf>. (Last accessed: 04/05/2023).

- [5] IRS. "Form 8300 and Reporting Cash Payments of Over \$10,000, 2023". arrival at: <https://www.irs.gov/businesses/small-businesses-self-employed/form-8300-and-reporting-cash-payments-of-over-10000>, (last accessed: 05/06/2023).
- [6] Maria Bergström, "The Many Uses of Anti-Money Laundering Regulation—Over Time and into the Future", *German Law Journal*, 2018, 5(1):1149-1167.
- [7] Bravo, Karen E, "Follow the Money - Does the International Fight against Money Laundering Provide a Model for International Anti-Human Trafficking Efforts.", *University of St. Thomas Law Journal*, 2008, 6:138-203.
- [8] Rahn, Richard W, "Taxation, Money Laundering and Liberty.", *Journal of Financial Crime*, 2002, 9(2):341-346.
- [9] Lee, Stephen, "The Economic Dimensions of Family Separation.", *Duke Law Journal*, 2022, 9:845-906.
- [10] Dan Cooper, Kristof Van Quathem, Philipp Tamussino & Aleksander Aleksiev, "CJEU Invalidates Public Anti-Money Laundering Registers on Privacy Grounds", *EU Data Protection, Financial Privacy*, 2022, arrival at:
- [11] <https://www.insideprivacy.com/eu-data-protection/cjeu-invalidates-public-anti-money-laundering-registers-on-privacy-grounds/>,