TAX EVASION AND FINANCIAL FRAUD IN THE CURRENT DIGITAL CONTEXT

Ioana – Florina Coita, Laura – Camelia Filip, Eliza-Angelika Kicska
Finance and Accounting, Faculty of Economics, University from Oradea, Oradea, Romania
coita.iflorina@gmail.com
laura.filip99@yahoo.com
kicskaeliza3@gmail.com

Abstract: *Preventing and combating phenomenon of tax evasion is a present concern of national governments due to the magnitude this phenomenon represents and because of the increasingly sophisticated techniques used by the authors in carrying out tax frauds. Evolution of tax evasion phenomenon at international level has acquired a profound technological character due to the increasingly elaborate methods. Illegal behaviour has some specific features that could be recognized easily by artificial intelligence models. They use real data in order to derive characteristics that could be identified in due time so that tax avoidant behaviour be identified and prevented. The use of forecasting models like logistic regression, random forests or decision trees in order to model tax avoidant behaviour shows having a good predictive power. Also, the use of the neural networks allowed scientists to calculate probability of an individual taxpayer that would attempt to evade taxes or commit other types of financial frauds. Scientific literature shows an increasing interest in using neural networks to detect and predict fraudulent behaviour in the fields of tax avoidance and financial domain. Cybercrime, cryptocurrency and blockchain were created in order to facilitate payments and help owner in accumulating wealth. Current landscape of financial frauds shows a different picture. Intracommunity frauds are more and more diversified. European Union and International bodies act together to prevent and combat fraud. Could these new technologies possess a real threat to the financial security of our transactions or encourage fraudulent behaviour? This paper tries to find the answer to this question.*

Keywords: *tax evasion, financial fraud, blockchain, cryptocurrency, cybercrime.*

JEL Classification: *H26, C89.*

1. Introduction

Tax evasion is a global phenomenon that has complex implications in tax litigation as well as in any economic or social field. Seeing the legal perspective, an act or fact that aims to avoid paying taxes or to evade the payment of tax obligations is punished and so the material damage affecting state budget brings upon the legal liability of taxpayer. Tax Authority, through its coercive force, is empowered to collect public funds and in this sense, it is supported by the judicial bodies when identifying fraudulent behaviour that falls under criminal or fiscal law. Public measures entitled for preventing this type of violation of legal norms could be based on a deep and complete understanding of complex nature of human behaviour and its motivations and also of the mechanisms that underly fraud matrix in current digital context. This could help decision-makers build more efficient fiscal policies.

2. What is tax evasion?

The notion of tax evasion has multiple meanings, both legally and financially, economically or even socially. According to national criminal law, tax evasion offenses are regulated by Law no. 241 of July 15/ 2005 which aims to prevent and combat tax evasion. Tax evasion offenses are regulated at art. 9, from lit. (a) to lit. (g) from the same law. They have common

elements but also distinctive features. In economic reality, they often find themselves in competition either with each other or even with other crimes. Perhaps this is due to the fact that the tax fraudster will try to hide his intention to evade tax or even pursue it by multiple means. That is why investigating tax evasion crimes is a complex approach, which requires knowledge from various fields, both economic, financial, legal or technological.
Also, according to Tax Law no. 225/ 2007 and Tax Procedural Law no. 207/ 2005 which currently rule, tax evasion offenses have all in common same features regarding taxpayer conduct in obeying legal norms inside the specific mechanism for collecting and distributing public funds as well as their control and verification. Due to this regulation, any tax avoidant behaviour that is followed by a financial loss to the public budget revenues gets fined or punished.

3. Tax evasion in the digital context

Current digital context created a favourable environment for tax fraudsters into using technologies for collecting and manipulating information present in the virtual environment in order to develop increasingly complex systems for tax fraud mechanisms. Using artificial intelligence for detecting fraudulent behaviour together with robotization of tax audits and evaluating taxpayers' risk could increase the rate of discovering tax frauds (Faúndez-Ugalde et al., 2020). In the same time, using various forms of artificial intelligence like the blockchain technology could offer a potential leverage to Tax Authority in preventing and combating non-complaint behaviour. This in turn could shape the role of State and its institutions in dealing with tax evasion or avoidance, building a powerful architecture based on public needs and values (Ølnes et al., 2017).
Forecasting tax behaviour is a complex process taking into account the non-linear nature existing in real data. Tax avoidance as a social phenomenon is being evaluated and measured based on existing network characteristics in order to be able to build a decision model (Lismont J. et al., (2018). On the other hand, neuronal models have the capacity to analyse and process large quantities of data better than humans do (Roung-Shiunn Wu et al., (2012). MLP model proves higher accuracy in prediction regarding financial or behavioural data (Pérez López C. et al., 2019). One study showed that individuals' behaviour regarding paying taxes is influenced by external and internal factors like audits, penalties, risk aversion by using multi-agent systems and Markov reinforced learning networks (Fayçal and Mohamed, 2018), (Goumagias et al., 2018).
There are studies that reveal the need to adapting neuronal models used according to the type of fraud being analysed so a hybrid intelligent model was tested on tax returns and other financial variables to detect corporate tax evasion by combining MLP, SVM, logistic regression, concluding that MLP outperformed other techniques in the field of tax fraud (Rahimikia et al., 2017), (Zakaryazad and Duman, 2016), (Sharma, 2012), (Ryman-Tubb et al., 2018). In this sense, recent research shows similar results by testing MLP models versus other AI algorithms (Bishop, 2006). In another study, using hybrid machine learning tools for fraud detection, authors make a comprehensive comparison on various detection tools in the literature analysed having found that each specific type of fraud, either financial or any kind, is better identified with a specific type of tool (Hosaka T., 2019).

4. Blockchain and tax evasion in current virtual environment

4.1. What is blockchain?

Blockchain is an algorithm that divides information into several segments called blocks, which it links in a chain, more specifically, is a distributed database. Each block has the cryptographic key of the previous block in its composition, with the exception of the first block

in the chain. Unlike IoT, which uses a centralized approach, blockchain records and stores transactions on a decentralised peer-to-peer network.

4.2. Cryptocurrency trading mechanism

Cryptocurrencies are generated with the signal that a payer shall send a transaction to a beneficiary. This transaction consists of the amount in cryptocurrencies that you want to be transferred and a smart-contracts (Xu, 2016). Smart contracts are algorithms that run when the "contractual clauses" are met, so that the process is as automated and time efficient as possible (Xu, 2016). Smart-contracts is distributed and analysed by all devices on the blockchain network (Xu, 2016). If the "clauses" are met, the devices on the network authorize the transaction and the smart-contract will be saved in a block (Xu, 2016). The devices in the blockchain will distribute the smart-contract, and the amount in cryptocurrencies will be transferred to the recipient (Luke Conway, 2020: Blockchain explained). In conclusion, the blockchain is distributed between all the network devices, updated by them, but it cannot be controlled by anyone.

4.3. Blockchain uses in detecting fraudulent behaviour

The integration of blockchain technology brings many challenges, but also benefits, both to the public and private systems. Blockchain technology can provide currently untapped benefits in the area of e-governance. The main public processes in which blockchain technology could bring significant advantages are: health, evidence of state assets, voting, retention of final judgments handed down by courts, criminal records (tax, judicial), property rights but especially in the efficiency of processes carried out by tax administrations (Ølnes et al., 2017). However, it should be noted that governments need to test on a smaller scale the transformation of processes through blockchain, in order to avoid serious and costly errors and to understand in depth the phenomena that have arisen and to be perfected (Ølnes et al., 2017). Currently, blockchain technology is intended to be integrated into several areas of activity, and in the economic field, this technology will be able to make a significant contribution. At the moment, companies want an evolution, a refinement of blockchain technology and evaluate the benefits of using blockchain in the future, including: lower data storage costs, more accurate records and facilitating the long-term control process (Hima, no date).

4.3.1. Blockchain and tax evasion

The resources of the public budget are made up of taxes, taxes and contributions, hence the financing of public expenditure (public lighting, works, investments). In order for the state to obtain a higher level of public resources, tax increases may occur, leading to increased tax pressure on the population and thus attempts at tax fraud (Faccia and Mosteanu, 2019b). A main task of the tax administration is to identify fraudulent behaviour, but also to provide advice and assistance to the taxpayer in such a way as to reduce and prevent the risk of non-payment of taxes to the public budget. Triple-entry acounting isn't as far as we'd ever imagine. Accounting principles and rules can be integrated into smart-contract, with transactions verified and validated by all devices on the blockchain network, thus enabling errors to be avoided, such as duplicate payments (Faccia and Mosteanu, 2019a). Today, financial and accounting data of the companies are stored both in the company and at the fiscal administration, which implies a waste of resources. In order to achieve greater transparency and to facilitate the access of the tax administration to carry out control procedures, it is necessary to customise the blockchain algorithm so as to allow permanent and unrestricted access by the tax administration and other public institutions in the investigation and sanctioning of tax fraud and criminal offences arising from such fraud (Hima, no date).

The blockchain mechanism can protect economic operators from the serious effects of tax fraud committed by mistake, providing a high degree of security through data encryption and transparency to tax administrations. The tax authorities will also be able to give more confidence to fiscal declarations as they will only be entered into the blockchain after they are verified and validated by all devices in the system, and if a declaration is to be amended, the modified block will need to be revalidated including all the blocks after the modified one (Hima, no date). Integration must be achieved gradually, first through smart-contracts, which could take the place of physical contracts, the processing of clauses and terms and conditions so that their verification and validation is as quickly as possible, but we must not lose sight of the fact that, until a fully functioning blockchain system is in line with the fiscal and economic-financial requirements, some possible high costs will have to be borne (Hima, no date).

Tax administrations collect large sets of high-speed information and an equally large variety, which is called Big Data. Big Data analysis includes data processing, information extraction, analysis of data whith neural models and networks (Faúndez-Ugalde et al., 2020). The OECD supports and urges the tax administrations of the world's states to cooperate at a higher level by facilitating access to information exchange in order to increase tax compliance, overall transparency and reduce tax fraud (Faúndez-Ugalde et al., 2020). The challenge of the authorities will, in fact, be not to integrate blockchain technology, but to harmonise the new technology between the involved structures of the state and economic agents and to protect the confidential data of each economic operator from any other foreign interaction that could endanger the data (Hima, no date). This is cost-effective for the state because human error is eliminated by automating processes, and transparency can live high levels, thus helping to fight tax evasion and fraud (Hima, no date).

4.4. Blockchain and money laundering

The crime of money laundering is part of economic crime, which is a complex and cumbersome process. Money laundering is regulated in Romania by Law no. 219/ 2019 on preventing and combating money laundering and financing terrorism and is framed as a criminal offence, punishable by imprisonment. Money laundering consists of converting money resulting from illegalities through different channels in order to lose illicit origin or any information that might highlight origin. Usually, this money ends up in the global economy, thus affecting its performance, but this step of the money laundering circuit is the most complicated because from here the money can be tracked (Albrecht et al., 2019).

Directive 2005/60/EC of the European Parliament and of the Council indicates the facts to be considered as money laundering offences. Although the European Union urges the recognition of money laundering as a criminal offence, some Member States are postponing the change in legislation to this effect (Leția, 2014).

Criminal groups manage to survive on money from illicit activities. These activities include: thefts, murders, prostitution, drug sales, organ trafficking, protection fees. Currently, moving cash or through banks is a rather difficult process, involving many risks. For this reason, cryptocurrencies are an easier way to trade for criminal groups.

Many criminal and criminal groups use cryptocurrencies on the black market because some are very difficult to track and others almost impossible. Cryptocurrencies are of major importance in the money laundering process due to the anonymity enjoyed by users. Criminals will make the most of all the benefits of cryptocurrencies, especially as they will be able to easily by pass investigations by the authorities.

Bitcoin can be used in money laundering and financing terrorism because it has three key features: the user is not obliged to publish his real identity because he owns a wallet with a pseudo-identity, it is a peer-to-peer platform (excludes banking intermediary and legislative regulations) and transactions are instantaneous and fee-free (Fletcher et al., 2021). The wallet (virtual wallet) is, in fact, the correspondent of the beneficiary's bank account through

which it can trade cryptocurrencies. Unlike fiat currencies (government-issued currencies, but no gold coverage, like dollar, euro (Chen, J. and Anderson, S., 2021: Fiat Money), cryptocurrencies are very easy to transfer from one jurisdiction to another, and for this process only an internet connection is needed (Albrecht et al., 2019).
We can include in cybercrime facts like: hacking and malware attacks, credit card fraud (Tiwari et al., 2020). Turner and Irwin (2018) have been trying to uncover the people behind the bitcoin transactions. Although they were able to track the transaction throughout the blockchain, they were stuck to the fictitious identity of the wallets used in the transaction (Tiwari et al., 2020).
Limitations of blockchain use are found on several levels: environmental impact through the rapid wear and end of video cards and processors that are wasted with a different collection treatment, high electricity consumption (Hima, no date). Also, other risks to which we are subjected through blockchain are: the 51% attack, system hacking, identity theft (Xu, 2016). The 51% attack involves intervention with a higher computing power in the calculations for cryptocurrency mining, so all the benefit resulting from the calculations will be charged by a single user. (Xu, 2016). System hacking involves intervening and taking control of the blockchain system (Xu, 2016). Identity theft can be achieved even by stealing some equipment that makes up the blockchain system.

5. Financial frauds in European Union

Fraudulent intelligence is a dangerous weapon in society. European Union's activity is hampered by the occurrence of fraudulent behaviour, which refers to the violation of the provisions of national Tax Law under Directive 2006/112/EC. The main reasons behind fraudulent behaviour are highlighted in the Triangle of Fraud namely: opportunity, justification, financial pressure or motivation (Cendrowski et al., 2007). The intra-community offender pursues illegal acts in order to obtaining sums of money from the national or European budget (Voicu et al., 2015). In this fraud matrix another element is Triangle of Trust by Dupont and Karpoff (2020) and indicates a perspective of disciplining inappropriate behavior and stimulates creation of trust in economic transactions. The last element is the Leffler and Klein Model on ways to detecting fraud (Klein and Leffler, 1981).
The mechanism of intra-Community fraud is emphasized on modalities of total or partial evasion of payment of some obligations from state budget or their illegal reimbursement. Understanding criminal behaviour of tax evasion in EU and VAT fraud consists in analysing the mechanism of tax fraud. A short typology of frauds at EU level is MTIC followed by illegal VAT deduction or cross-invoicing, fictitious intra-Community delivery, cash and carry fraud and imports using customs procedure (Fisher, 2011).
Fraudulent behaviour also makes its presence felt at the European funding level, committed by obtaining or using European funds and or national public funds for unjustified purposes of a project (UE, 2017). Semeta and Kessler (2011) agree that a main fraudulent thinking of an individual is to influence the procedure of purchasing goods. The fraudulent mechanism based on public funds is related to corruption and this is considered an abuse of power for personal gain (ECA, 2019a). Main frauds regarding financing of European funds are: falsification of the financing request, over-invoicing of project costs, filling in with false data of the non-reimbursable financing applications and others. The financing of a European project can be done by falsifying specific documents, such as: the value indicated in the request for reimbursement is higher than the real value of the good, the eligibility of payment through a forged document or invoice and the allocation of funds and their use for other purposes that have nothing to do with the reason for their allocation (Smolej, 2015). During the 2007-2013 programming period, Member States' cohesion fund fraud was reported in percentages and the highest were in Slovakia 2.13%, Romania 1.10% and Czech Republic

0.88% and the lowest in France, Belgium and Luxembourg below 0.05% (ECA, 2019b). Recovery rate of amounts resulting from financial fraud in 2018 were found in: Slovenia 100%, Sweden 97%, Czech Republic 95%, Finland 93%, Hungary 91%, France 89% and Austria 84%. (UE, 2019). OLAF as an EU representative of combating fraud has entered into a cooperation agreement with the World Bank's Integration Department and with the authorities of the Member States to control, monitor, audit, investigate financial crime and the use of funds received (Vlogaert, 2006).

6. In conclusion

Current context of technological development brought increasingly sophisticated techniques that are used by fraudsters in carrying out tax frauds. Preventing and combating fraudulent tax behaviour is a present concern of national governments all across globe and this in turn could be more efficiently tackled with the help of AI algorithms. The usefulness of computational intelligence in detecting the risk of tax fraud refers to finding an empirical model that can be tested and validated to be able to predict fraudulent behaviour. Cybercrime is a form of criminal activity. Only a computer, network and human interface is needed to enable criminals to steal money. Also, governments and the investigative bodies should keep up with the technological development of tax evasion phenomenon in order to control it and prevent and combat fraud. The European Commission is responsible and makes the necessary checks on external expenditure. OLAF has set up a network that provides assistance to Member States and is called the Anti-Fraud Information System. The establishment of this institution has improved both the anti-fraud management authorities and the Member States. The European Union and the Member States have a common responsibility and both are fighting to combat fraud, irregularities, corruption, tax evasion and any other crime that does not comply with compliant legislation. Regardless of the type, nature or form of the existing fraud, it must be prevented, detected and the correct measures taken.

Notations

Abbreviations
AI - artificial intelligence
MLP – multilayer perceptron
SVM – support vector machines
IoT – Internet of Things
BC – blockchain
EU – European Union
OLAF - European Anti-Fraud Office
MTIC - Missing Trader Intra Community Fraud
OECD - Organisation for Economic Co-operation and Development

References

1. Albrecht, Chad & Duffin, Kristopher & Albrecht, Conan & Morales Rocha, Victor. (2019) *The use of cryptocurrencies in the money laundering process. Journal of Money Laundering*, Control. 22. 00-00. 10.1108/JMLC-12-2017-0074.
2. Bishop M.C. (2006) *Pattern Recognition and Machine Learning*, Library of Congress Control Number: 2006922522. (ISBN-10: 0-387-31073-8, ISBN-13: 978-0387-31073-2). 2006 Springer Science+Business Media LLC.
3. Cendrowski H. et al. (2007) *The Handbook of Fraud Deterrence*. Available online at: https://onlinelibrary.wiley.com/doi/book/10.1002/9781119202165, [15.04.2021].

4. Chen, J. and Anderson, S. (2021) *Fiat Money*. Available online at: https://www.investopedia.com/terms/f/fiatmoney.asp, [16.04.2021].
5. Council Directive 2006/112/EC on *the common system of value added tax*. available online at: https://eur-lex.europa.eu . [14.04.2021].
6. Conway, L. (2020) *Blockchain explained*. Available online at: https://www.investopedia.com/terms/b/blockchain.asp. [17.04.2021].
7. Directive 2005/60/EC on *preventing the use of the financial system for money laundering and terrorist financing*. Available online at: https://eur-lex.europa.eu/.
8. Dupont Q. Karpoff JM. (2020) *Triunghiul încrederii: Legi, reputație și cultură în cercetarea financiară empirică*, J. Autobuz. Etică 163.
9. European Court of Auditors - (ECA) (2019a) *Fighting fraud in EU spending: action needed.* Available online at: https://op.europa.eu, [16.04.2021].
10. European Court of Auditors - (ECA) (2019b) *Tackling fraud in EU cohesion spending: managing authorities need to strengthen detection, response and coordination.* available online at: www.eca.europa.eu, [15.04.2021].
11. European Parlament and the Council – (UE) (2019) *30th Annual Report on the Protection of the European Union's financial interests - Fight against fraud.* Available online at: https://ec.europa.eu, [16.04.2021]
12. European Union – (UE) (2017) *Nereguli și antifraudă.* Available online at: https://www.runv.ro/doc_implem_POCU/prezentare-nereguli.pdf, [17.04.2021].
13. Faccia, A. & Mosteanu, N. (2019a) *Accounting and blockchain technology: from double-entry to triple-entry.*
14. Faccia, A. & Mosteanu, N. (2019b) *Tax Evasion, Information Systems and Blockchain*, Journal of Information Systems Management. 13.
15. Faúndez-Ugalde, A., Mellado-Silva, R., Aldunate-Lizana, E. (2020) *Use of artificial intelligence by tax administrations: An analysis regarding taxpayers' rights in Latin American countries*, Computer Law & Security Review, Volume 38, 105441.
16. Fayçal Y., Mohamed T. (2018) *Partially observable Markov methods in an agent-based simulation: a tax evasion case study*, by Elsevier B.V.
17. Fisher J. (2011) *Analysis Eastenders Cash and Carry: lessons learnt*. Available online at: https://www.devereuxchambers.co.uk/, [17.04.2021].
18. Fletcher, E., Larkin, C., Corbet, S. (2021) *Countering money laundering and terrorist financing: A case for bitcoin regulation*, Research in International Business and Finance, Volume 56, 101387.
19. Goumagias N. D., Hristu-Varsakelis D., Assael Y. M. (2018) *Using deep Q-learning to understand the tax evasion behavior of risk-averse firms*, Expert Systems with Applications, Vol. 101, 2018, (pg.258-270).
20. Hima, Z. (no date) *Blockchain in Taxation*, Szechenyi Istvan University. Available online at: http://kgk.uni-obuda.hu/, [15.04.2021].
21. Hosaka T. (2019) *Bankruptcy prediction using imaged financial ratios and convolutional neural networks*, Expert Systems with Applications. Volume 117, 2019, (pages 287-299).
22. Karpoff M.J. (2020) *The future of Financial Fraud*. Available online at: https://corpgov.law.harvard.edu/, [17.04.2021].
23. Klein B. Leffer KB. (1981) *The role of market forces in assuring performance.* Polit. Econ.
24. Law 219/2019 on *Preventing and Combating money laundering and financing terrorism*. Available online at: http://legislatie.just.ro/7, [16.04.2021].
25. Leția, A. (2014) *Investigarea criminalității de afaceri*, București, Universul Juridic.
26. Lismont J. et al. (2018) *Predicting tax avoidance by means of social network analytics.* Decision Support Systems, Volume 108, 2018, Pages 13-24.
27. Ølnes S., Ubacht J., Janssen M. (2017) *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*, Government Information Quarterly, Volume 34, Issue 3, pg. 355-364.
28. Pérez López C., Jesús Delgado Rodríguez M. & de Lucas Santos M. (2019) *Tax Fraud Detection through Neural Networks: An Application Using a Sample of Personal Income Taxpayers*. Future Internet 2019, 11(4), 86. Special Issue Future Intelligent Systems and Networks 2019.
29. Rahimikia E. et al. (2017) *Detecting corporate tax evasion using a hybrid intelligent system: A case study of Iran*. International Journal of Accounting Information Systems, Vol. 25, pg. 1-17.
30. Roung-Shiunn Wu et al. (2012) *Using data mining technique to enhance tax evasion detection performance.* Expert Systems with Applications, Volume 39, Issue 10, 2012, Pages 8769-8777.

31.Ryman-Tubb N. F., Krause P., Garn W. (2018) *How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark*. Engineering Applications of Artificial Intelligence, Volume 76, 2018, Pages 130-157.
32. Sharma A. (2012) *A Review of Financial Accounting Fraud Detection based on Data Mining Techniques*. International Journal of Computer Applications (0975 – 8887), Volume 39– No.1, February 2012, Information Systems Area Indian Institute of Management, Indore, India.
33. Semeta A., Kessler G. (2011) *Compendium of Anonymised Cases Structural Actions*. available https://www.interreg-croatia-serbia2014-2020.eu/, [14.04.2021].
34. Smolej D. (2015) *Fraudulent use of the funds of the European Agricultural Fund for Rural Development.* Available online at: *https://www.policija.si/f,* [15.04.2021].
35. Tiwari, Milind & Gepp, Adrian & Kumar, Kuldeep (2020) *A review of money laundering literature: the state of research in key areas*, Pacific Accounting Review.
36. Vlogaert J. (2006) *Fighting fraud and corruption: how the European Union protects its public funds.* Available online at: https://www.unafei.or.jp/f, [17.04.2021].
37. Voicu C. Et al. (2015) *Investigarea infracțiunilor de evaziune fiscală*. Available online at: http://www.inm lex.ro/fisiere/f, [16.04.2021].
38. Xu, Jennifer J. (2016) *Are blockchains immune to all malicious attacks?* Financial Innovation, Springer, Heidelberg, Vol. 2, Iss. 25, pp. 1-9.
39. Zakaryazad A., Duman E. (2016) *A profit-driven Artificial Neural Network (ANN) with applications to fraud detection and direct marketing*. Neurocomputing, Volume 175, Part A, 2016, Pages 121-131.