David Hadwick

Chapter 6
Breaking the Fiscal Omerta: The Roadmap to Transparency in EU Tax Algorithmic Governance

Abstract: A majority of tax administrations in the Member States of the European Union (EU) are increasingly leveraging machine-learning (ML) technology to perform their fiscal prerogatives. Yet, little information about ML systems has been disclosed to taxpayers regarding the underlying input data, the risk factors learned by machines, and the overall accuracy or fairness of their outputs. The use of ML by tax administrations highlights an inherent lack of transparency regarding algorithmic-based tax risk assessments and the algorithmic selection of taxpayers. Cases such as the Dutch childcare allowance scandal or toeslagenaffaire have shown how such a lack of transparency can have dramatic consequences for taxpayers. This raises the question: to what extent is secrecy necessary for the collection of taxes and how can transparency be upheld in tax algorithmic governance? This question is addressed in two parts. Section 1 presents the state of use of ML systems by tax administrations in the EU. Section 2 delineates the criteria that compose transparency, and applies those normative criteria to the specific context of State secrecy in fiscal algorithmic governance. The analysis shows that, regardless of the reiterated importance of transparency in algorithmic governance in literature, doctrine and jurisprudence, the use of ML by tax administrations is exacerbating the level of secrecy, to the detriment of taxpayers.

6.1 Introduction

The rate at which ML systems used by tax inspectorates have proliferated is nothing short of extraordinary. In less than two decades, ML systems leveraged for fiscal governance have multiplied exponentially, from a handful of EU Member States to more than two thirds of the EU. The use of ML as a tool to perform State fiscal prerogatives has become the norm. ML-based technology is inter alia used to provide direct assistance to taxpayers, to customize default letters sent by the administration, to automatically collect data or select taxpayers for audits (Hadwick, 2022a). These technological tools have leapfrogged the digital transformation of EU tax administrations, so much so that barely any action is currently carried out without the assistance of that technology.

Most notably, with the integration of ML systems, tax administrations are able to process more data and infer more information from taxpayers' data, disrupting the fragile balance of power between the administration and the administered. Yet, little information regarding these ML systems has been publicly disclosed, primarily by virtue of the fiscal procedural rules of Member States. ML systems have been adopted without legal basis and the rights of taxpayers are systematically barred from accessing any information or details on the models leveraged by their respective administration, including during litigation. Despite the newfound importance of algorithmic transparency in literature and jurisprudence, in the context of fiscal governance, it is only a buzzword devoid of any normative purpose. In complete antithesis to the principle of transparency, fiscal algorithmic governance in the EU is characterized by a codified status quo of institutional secrecy, a fiscal omerta. Seminal cases such as SyRI, eKasa, or SS SIA demonstrate how the lack of transparency bears significant risks to taxpayers' rights. The events of the toeslagenaffaire revealed that opacity regarding ML algorithms can generate destructive consequences and poses an existential threat to taxpayers. Regardless of the risks to taxpayers, tax administrations in the EU enjoy a literal carte blanche for the development of risk-scoring models. In a context where the use of ML is proliferating at a rapid pace, the fiscal omerta is rendering some fundamental rights entirely moot and obsolete. The opacity in EU fiscal algorithmic governance raises the question: to what extent is secrecy necessary for the collection of taxes and

how can transparency be upheld in tax algorithmic governance? Section 1 demystifies the concept of machine-learning for a legal audience, the different learning techniques employed, and delineates the current state of use of ML systems by the tax administrations of the Member States. Based on a review of the literature, Section 2 presents the criteria that compose the nebulous principle of transparency, and why these criteria bear no normative consequences on tax procedures, rather characterized by a regime of institutional secrecy. In Section 2, the question of whether all of these tenets of institutional secrecy are proportionate to the aim of tax enforcement is examined, and some solutions are presented to enhance transparency in fiscal governance.

6.2 Section 1: The State of Use of Machine-Learning by EU Tax Administrations

The Organization for Economic Co-operation and Development (OECD, 2019) defines AI systems as systems that, for a given set of human-defined objectives, are capable of making predictions, recommendations or decisions and are designed to operate at varying degrees of autonomy. The EU AI High-Level Expert Group (AIHLEG, 2018), the group of experts appointed by the European Commission to provide advice on the EU AI strategy, defines AI systems in a quasi-identical manner. Although the concept of machine-learning (Samuel, 1959) appeared concurrently to the term 'artificial intelligence' (McCarthy et al., 1955), it is conceptually and legally recognized as a sub-set of AI (EU AI Act Proposal, 2021).

Machine-learning can be defined as computational procedures that can autonomously, i.e. without being explicitly programmed to do so, improve performance by drawing statistical inferences from data. In essence, machine-learning is nothing more than an autonomous statistical model, or suite of models. From a computer science perspective, a machine-learning system transforms inputs into outputs without being explicitly programmed to do so by a finite set of human-designed algorithms, unlike a traditional software (Mohri et al., 2018). Similarly to any statistical model, the system assigns mathematical coefficients or 'weights'

to any individual input and adds the inputs to obtain a weighted sum (Sammut et al., 2011). The results of the weighted sum are then normalized with an activation function, which expresses results between a range of figures, for instance, as either 0 or 1 (Hill et al., 2011).[1] The particularity of a ML system, what distinguishes it from a traditional statistical model and makes it capable of autonomous learning, is the process of 'error backpropagation'. As illustrated in Figure 1, error back-propagation consists of using previous erroneous outputs as new inputs to the system. At each cycle of backpropagation, when the errors are fed back as new inputs, the system adjusts the weights thus increasing or decreasing the coefficients associated with specific inputs. By adjusting the weights, the system autonomously isolates the most important inputs to improve its performance. The machine-learning algorithm then learns to generate a statistical model, of either a static or dynamic nature. Typically, a ML system is composed of several units, so-called perceptrons, to produce finer-grained results. Together, these perceptrons form a 'neural network' and multiple layers form a 'deep neural network' (Nigrin, 1993). Figure 1 below is a schematic representation of a perceptron.

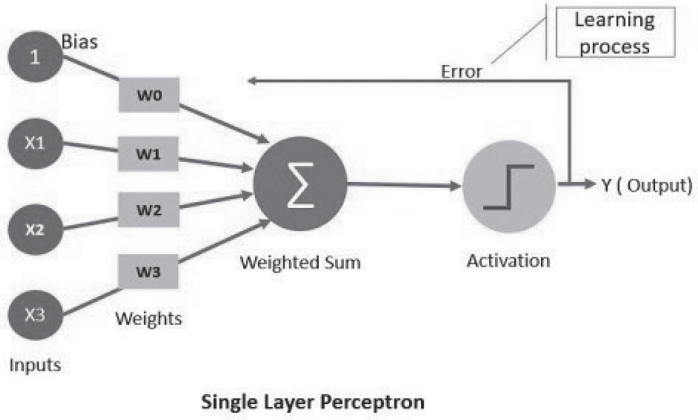

Figure 1[2]

[1] Hence, in essence the activation function decides whether the neuronal unit is activated or not.

[2] Image retrieved from : http://sumanthrb.com/ml/perceptron/ – last retrieved December 2022.

It is interesting to note that ML is often referred to as a novel 'disruptive' technology, yet in fact it is more than half a century old. Originally created in 1957, the ML system of Rosenblatt was designed to ascertain whether the picture presented was a triangle. The system was fully analogous, i.e. not a digital computer, with visual sensors that would analyze pictures of 16 by 16 pixels (Rosenblatt, 1958; Rosenblatt, 1960; Olazaran, 1993). The simple recognition and binary classification of a shape may seem like a trivial exercise. However, classifying the most straightforward shape is a multifactorial exercise involving the processing of lines, corners, reverberation of lights and shadows, etc. (Chan et al., 2002). Whether by a human or by a machine, such classification is by no means an easy cognitive feat. Through the analysis of vast amounts of pictures, the ML system was capable of inferring statistical correlations, creating a statistical model that could be applied to future inputted pictures.

Systems used for tax risk assessments work in a very similar manner. These systems are presented with previous known examples of taxpayers that have and have not committed fraud or were compliant and non-compliant. By analyzing these examples, the systems draw statistical correlations and deduce what variables can be regarded as indicating a risk of fraud. Together, these risk indicators form a statistical model used to predict the risk of tax fraud/non-compliance for future taxpayers and transactions. This technique is referred to as supervised learning, because the correct output, i.e. who is a fraudster and who is not, is supposedly already known by the tax administration (Hoogendoorn et al., 2017).

The tax administration also makes use of unsupervised learning techniques where the data is unlabeled, i.e. the correct output is not known (Hadwick, 2022b). Clustering is an example of an unsupervised learning technique used by tax administrations (OECD, 2016). Clustering is the act of organizing groups ('clusters') whereby the objects or datapoints in one cluster are similar, and dissimilar to objects belonging to other clusters (Aggarwal, 2018). Figure 2 below is a schematic representation of a clustering algorithm.

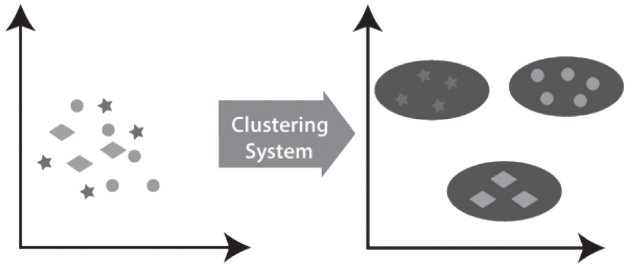

Figure 2[3]

Clustering can be regarded as the most important category of unsupervised learning techniques, as it serves as the basis for many unsupervised learning algorithms (Arroyo et al., 2016). Via clustering many functions can be performed such as classification and outlier detection. For the tax administration, clustering is used to classify similar and dissimilar taxpayers to predict tax evasion. Clustering is also used to detect abnormal behavior and outliers, such as under-reported income, by calculating the distance of points within a cluster. Points at the very edge of a cluster are likely to be outliers, indicative of potential tax evasion.

Even as a fiscal governance tool, ML-based technology is certainly not a new phenomenon. ML was already used in 2004 with, for instance, XENON, a 'spider' system designed by tax administrations in the Netherlands, Denmark and Sweden to automatically collect taxpayer data online (European Commission, 2006). Nowadays, at least 18 out of the 27 Member States' tax administrations use ML systems on a regular basis (Hadwick, 2022b). Additionally, Eurofisc members developed Transaction Network Analysis (TNA), a ML data-matching system specifically designed to detect and prevent carousel fraud (OECD, 2021). Hence, in some areas of taxation, ML systems are already used consistently throughout the EU. ML systems perform several functions for tax administrations: taxpayers assistance through the use of chatbots (OECD, 2019; Vero Skatt, 2021); automated data collection with 'spiders' or 'web-scraping' algorithms (CIAT, 2017; Loi n°2019-1479);

[3] Image retrieved from: https://laptrinhx.com/machine-learning-clustering-algorithm-2431293740/ – last retrieved December 2022.

the detection of risks through clustering or network analysis (Juhasz, 2021); the selection cases for audits via risk management systems (RMS) (OECD, 2016; Revenue Authorities, 2014; Federal Ministry of Austria, 2018); or nudging, by adapting the language used on communications sent to taxpayers (van Hout, 2018; van Luts et al., 2019). By far the most prevalent function for which ML systems are used by tax administrations are RMS tools to select taxpayers for audits.[4] All 18 Member States' tax administrations that use ML exploit one or more of such risk-scoring systems (Hadwick, 2022b). Moreover, the Commission points out that even in Member States where ML is not used for the algorithmic-based selection of taxpayers for audit, their tax administrations use traditional statistical approaches and data analytics to determine which taxpayers should be audited (European Commission, 2022). Hence, the use of statistical risk indicators for tax enforcement is a constant throughout the EU.

6.3 Section 2: Algorithmic Transparency as the New Buzzword

In recent years, algorithmic transparency has been hailed as the new keyword, to quell citizens' fears of AI. Eminent scholars on AI and data protection (Hildebrandt, 2012; Pasquale, 2011; Pasquale, 2015; Pasquale et al., 2014; Wachter et al., 2019), have stressed the importance of transparency to combat the risks of algorithmic governance. The OECD and the EU, through the Commission (2021; EU AI Act, 2021), the AI HLEG (AIHLEG, 2019) or AI Watch (Misuraca et al., 2020; Manzoni et al., 2022) have highlighted the paramount necessity of transparency as a pre-condition for citizens' trust in an open and democratic society. The significance of transparency as a principle of law is also codified in Article 11 of the Treaty on the European Union (TEU, 2012). Even in the niche isolated world of taxation, reference to the importance of transparency have been made on several occasions. In the case of Systeem

[4] Out of the 60 ML systems identified, 32 could be qualified as risk-scoring algorithms or risk-management systems, see Hadwick, 2022.

Risico Indicatie (SyRI, 2020; SUWI Wet, 2020), a ML risk-scoring system used by the Dutch tax administration to select taxpayers for audit, the Court of the Hague halted the use of the system by virtue of the lack of transparency of the legislation governing the system. The Court ruled that, having regard to the risks discrimination of SyRI, transparency was primordial to verify whether these risks are sufficiently neutralized. In eKasa (eKasa, 2021), the Constitutional Court of Slovakia ordered to temporarily end the use of the eKasa system, finding that the ML system had not been authorized through the prior adoption of a legislative measure. The system was meant to act as an electronic cash register system and Enterprise Resource Planning (ERP) system, automatically transferring a wide array of data on both buyers and sellers to the Slovak tax administration for the detection of VAT fraud. The data transferred was subsequently processed by an ML system to detect risks and devise risk indicators for the selection of taxpayers for audit. The Constitutional Court found a grave breach of the principle of legality, but also advised the legislature to adopt specific safeguards, all of which related to transparency (eKasa, 2021, § 112 et seq.). A very similar reasoning can be observed in CJEU SS SIA (SS SIA, 2022), where the Court found that a request by the Latvian tax administration for the transfer of large bulks of data, to be processed by automated and non-automated means, violated the GDPR. In particular, the CJEU asserted that the request for information was contrary to Article 5(1) of the GDPR, namely the principles of fairness, lawfulness and transparency, by virtue of the lack of legislative measure authorizing the transfer. In each of these cases, transparency is viewed as an important safeguards against the risks of algorithmic governance. The lack thereof is systematically invoked as the ratio decidendi to rule against the integration of ML systems.

Despite the multiple iterance of the importance of transparency for data protection, algorithmic governance and even democracy, the concept is hardly ever defined in a comprehensive manner in legislation. Although being a fixture of EU constitutionalism, and an even older pillar of Western philosophy (Kant, 1795; Hobbes, 1651; Mill, Bentham, Montesquieu, de Tocqueville as cited in Gosseries, 2005), the concept of transparency is undeniably nebulous. Cynically, one could say that perhaps because of this elusive meaning, it is so heavily brandished as a pillar

of digital governance. Upon analysis of the literature, three normative axes can be inferred from the principle of transparency:

Firstly, subjects must be sufficiently informed about an official activity – a decision, measure, norm, law, etc. – both prior to the activity, throughout the process, and after its adoption or conclusion ('publicity').

Secondly, the information should be easily accessible and provided in a clear, concise and intelligible manner ('accessibility').

Thirdly, prior to the official activity, procedures should be established to ensure that the governing body is properly regulated, supervised or monitored, that the governing body can be held liable in case of 'torts'[5] and that subjects can obtain reparations ('accountability').

For the purpose of this paper, the focus will be specifically on publicity, the axis most concerned with tax secrecy. Prima facie, there are three channels for taxpayers to obtain information on the ML models used by tax administrations: through the law, upon exercise of their data subject rights to information and access, and before the courts through disclosure requests. All of which are lacunary in the specific context of fiscal algorithmic governance.

First, regarding the transparency of legislative norms, upon comparative legal review of the 18 Member States whose tax administrations make use of ML systems, only 4 have a law which mentions some of the ML systems used (Hadwick, 2022b). Most Member States do not even prescribe in their tax codes that the tax administration is empowered to make use of such technological tools. No Member States have published a complete inventory of the models used by their respective tax administrations, or at least an inventory of the models that exhibit a risk of conflict with taxpayers' rights (Hadwick, 2022a). In theory, the principle of legality prescribes that a measure that generates a risk to the exercise of natural rights should be regulated through legislative norms, and thus should be communicated to the public (Venice Commission, 2016). Currently, respect of the principle of legality is far from being the norm.

Second, access to information on ML systems will also be denied to taxpayers who make a specific request for it. Indeed, because ML

[5] For the purpose of this paper, torts simply means 'wrongdoing', not necessarily a civil law torts, but also including criminal wrongdoing and violation of taxpayer fundamental rights.

systems are used to assess tax risks and thus also to detect and predict risks of fraud, these systems are used to investigate crimes. Accordingly, tax procedural rules of Member States foresee that access to data on ML systems used by tax administrations, for example, statistical risk indicators, is barred from taxpayers with the argument that it could potentially prejudice the investigation of a crime. This limitation to the right of access is explicitly foreseen by the GDPR in Article 23(1), sub-paragraph (e) and (h), and Article 15(1) of the Law Enforcement Directive (LED). In the context of the prevention of crime, a limitation on the right of data subjects to be informed of data processing operated with their personal data is also prescribed in Article 13 (3)(b) LED. Consequently, taxpayers can lawfully be barred from being informed that they were subjected to data processing by ML systems and denied their right to access any information regarding these systems. In addition to these EU secondary law instruments, limitations to the right of access and right to information are also prescribed in Member States' tax procedural codes. In Member States such as Belgium (Loi du 5 Septembre 2018), France (Arrêté CFVR, 2021) and Poland (STIR, 2017), the limitations of habeas data rights are prescribed in the norms which regulate the use of data and the use of ML systems by the administration. In other Member States such as Germany, these limitations are prescribed directly in tax codes (AO, 2022). In both situations, the reasoning is the same: disclosing details on ML systems, in particular risk indicators, would jeopardize the investigation or prevention of a crime, hence access to such data is excluded. Since systems for tax risk assessments are used on all taxpayers, whether suspected of fraud or not, taxpayers are systematically deprived of their rights as data subjects.

Third, even in the case of an administrative recourse against a tax administration or in the context of a trial, taxpayers are barred from accessing details on the ML systems used by their tax administration. This limitation in the context of judicial proceedings, is explicitly provided in, for instance, Section 88(5) (4) of the German Tax Code.[6] As a result,

[6] Abgabenordnung, Sec. 88(5) (4): "*Einzelheiten der Risikomanagementsysteme dürfen nicht veröffentlicht werden, soweit dies die Gleichmäßigkeit und Gesetzmäßigkeit der Besteuerung gefährden könnte*" – *'risk-indicators should never be made public'* – this includes the context of judicial proceedings.

taxpayers who hold legitimate grievances over an ML system used by tax administrations, for instance, a taxpayer who believes to be the subject of discrimination, cannot exercise disclosure rights. As legitimate as it may be, this request will automatically be denied by virtue of State secrecy. Effectively, the obligation of disclosure and the equality of arms in a potential trial are completely turned on their head, to the extent that the rights to data protection, to non-discrimination and to a fair trial become moot. Conclusively, in the context of taxation, publicity is a normative 'market failure'. Taxpayers are not afforded any points of reference to understand what data is processed, with what sort of technological tools it is processed and what the outcome of the processing is. Taxpayers cannot know what types of ML systems are used by their respective administration, whether in the law, as data subjects or as defendants in a trial.

This opacity is based on an illegitimate fear that transparency would enable some taxpayers to circumvent fiscal risk assessments. Yet, the consequences of a lack of transparency are very real and seriously erode taxpayers' rights. This opacity generates a strong power asymmetry in favor of the tax administration. It disrupts the balance of power between the administration and the administered in the constitutional order. In fact, the risks of such opacity have already manifested in the Dutch childcare allowance scandal, or toeslagenaffaire (Hadwick et al., 2021). In this case, taxpayers showed reliable evidence of being the victims of unlawful ethnic profiling by a tax risk assessment tool of the Dutch tax administration. Yet, for more than eight years their grievances fell on deaf ears by virtue of the impossibility for them to access information on the ML systems used by the administration. Ultimately, the lack of publicity in the toeslagenaffaire led to the resignation of the entire Dutch cabinet, and the discrimination of 35,000 taxpayers caused irreparable harm, led to forced separation of children from their families and costs of half a billion euros in public funds for compensation (DutchNews, 2021). If the judiciary or the DPA had been informed that the Dutch tax administration was using discriminatory risk indicators, such as ethnicity, this scandal could have been avoided outright.

It is important to note that aside from grave statistical malpractice, such as in the toeslagenaffaire, discrimination can occur fairly easily when resorting to ML models for public governance. Even with an impeccable

computational procedure, discrimination and errors can result from factors such as biased data, imbalanced classification or incorrect labels. Yet, in a governance context, where the target population is so heterogenous as the entire cohort of taxpayers, these factors will occur more often than not. For instance, ensuring that the training data is representative of the entire population to avoid a sample bias requires rigorous vigilance and extremely granular data. The same can be said of correct labeling which necessitates regular updates long after the algorithm has been properly trained to avoid longitudinal fallacies. The list of potential biases in data collection illustrates how complex it is to carry such a process without any mistakes (Mehrabi et al., 2022). Even with perfect data, the computational procedure itself may generate discriminatory features. Often these biased risk indicators will follow neutral and sound policy choices. For instance, targeting individuals with foreign bank accounts or businesses with high prevalence of physical cash. These attributes are empirically proven to be indicative of potential tax evasion. Yet, as features of a model, these attributes would generate prohibited indirect discrimination against foreign taxpayers. Transparency would enable checks and balances by other governmental organs or citizens themselves, to verify whether risks of discrimination or data protection infringements have been properly considered by the administration.

In such a context, completely barring all taxpayers from any information about the data processed or risk indicators used in ML systems, both in the law or through the exercise of their data subject rights, is manifestly disproportionate. Taxpayers even with knowledge of the data or features of the model cannot game the system. Risk indicators used in the model relate to objective characteristics of taxpayers. Taxpayers, whether natural or legal persons, cannot modify all personal characteristics and factors of production without it being detected by the administration in some shape or form. Discrepancies from one year to another, a sudden change in revenue or unusually high purchases would automatically raise red flags. For more than 95% of taxpayers, the tax administration is capable of completing their tax returns without any input from the taxpayer, simply by compiling documentation from third parties (Bøhm, 2021). Most OECD countries have dozens sometimes a hundred different typologies of risk indicators that are continuously updated (OECD, 2017). Knowledge of some statistical correlations cannot enable someone to

continuously cheat the whole system without insurmountable economic burdens. Simply put, cheating would be more costly than compliance. In addition, risk-scoring algorithms are but one kind of algorithm used by tax administrations among many. Risk indicators only relate to one specific type of algorithm, namely risk-scoring algorithms. Even if all risk indicators were disclosed, other ML algorithms would not be affected and would still be able to detect tax evasion. Accordingly, the interest of taxpayers in knowing what data is processed and how, both in the law or through specific requests, greatly outweighs those of an administration.

Moreover, even if you acknowledge the need of the administration to maintain some secrecy, barring disclosure in the context of litigations against the administration is both dangerous and nonsensical. Technological solutions exist to test the compliance of a model with the rights to non-discrimination or data protection, without opening the black box or conveying the internal logic of a model. Technical processes such as counterfactual explanations, for example, through machine-learning models such as Local Interpretable Model-Agnostic Explanations 'LIME' (Ribeiro et al., 2016; Wachter et al., 2017), enable the review of a model without accessing any sensitive details. These solutions are model-agnostic, i.e. they perform on any ML model, and provide satisfactory explanations interpretable even by laymen. Invoking tax secrecy to completely deny any access to the model, even in litigation, is by far the most intrusive solution an administration can opt for. Developing a simple API to counterfactually test some benchmarks is a costless solution that would protect taxpayers' rights while guaranteeing the same level of secrecy for the administration. In such a context, when solutions exist to enable the review of a model while maintaining a form of black box, the current omerta promulgated by the administration is manifestly disproportionate to the aim pursued.

6.4 Conclusions

While ML systems have been used for almost two decades, taxpayers' fundamental rights have been thoroughly neglected during all that time. Within the EU digital constitutional order, the principle of transparency perfectly illustrates this appalling neglect. The status quo is one of secrecy,

an institutional law of silence authorized by Member States' legislatures. Little information on the ML systems used by tax administrations is disclosed to taxpayers. Either in legislation, as less than a quarter of Member States have an actual legal basis that authorizes the use of ML by their respective tax administrations. Nor upon request by taxpayers, as tax procedural rules forbid taxpayers to access details on ML systems based on an illegitimate fear of administrations that it would hinder fraud investigations. Even when taxpayers hold legitimate grievances and substantiated claims, access to information is outright denied rendering their right to data protection, to non-discrimination and to a fair trial effectively moot. This opacity is not without consequences and has already led to dramatic cases such as the toeslagenaffaire. Accordingly, the digital transformation of the tax administration poses an existential threat to taxpayers' rights.

It is clear that the current policy of institutional secrecy of EU tax administrations is neither necessary nor proportionate to the aim pursued. The vast majority of taxpayers use pre-filled in tax returns and the administrations can complete the quasi-totality of tax returns without any input from the taxpayers. In such a context, additional transparency through the disclosure of some details on the ML systems used or the data processed, would not hinder tax enforcement. Moreover, technical solutions, such as counterfactual explanations, already exist and enable the review of ML systems without disclosing sensitive details or the inner workings of a model. Consequently, maintaining complete secrecy and upholding the legal black box, is unnecessary and disproportionate to the aim of not hindering tax enforcement. By no means will such secrecy render an administration better or more effective, while the harm generated by the omerta for an administration's legitimacy and for taxpayers' rights are considerable. Despite the existence of technical solutions to uphold fundamental rights, EU legislatures are opting for a regime of heightened surveillance, inquisitorial against taxpayers. In the long term, such opacity coupled with the digital surveillance regime instituted will only antagonize taxpayers, and serve as a catalyst for less compliance and less cooperation with tax inspectorates.

References

Abgabenordnung, Sec. 32c (1) 2. (2022) (AO).

Aggarwal, C.C. (2018). *Data Clustering: Algorithms and Applications*. (Aggarwal, C.C. & Reddy, C.K. Eds.) CRC Press.

Arrêté du 21 Février 2014 portant création par la DGFiP d'un traitement automatisé de lutte contre la fraude dénommé «ciblage de la fraude et valorisation des requêtes», Art. 4(1) (as amended by Arrêté du 8 mars 2021). (Arrêté CFVR).

Arroyo, A., Tricio, V., Herrero, A., Corchado, E. (2016). *International Joint Conference SOCO' 16 – CISIS'16 – ICEUTE'* (Grana, M., Lopez-Guede, J.M., Etxaniez, O., Herrero, A., Quintian, H., Corchado, E. Eds.). Springer.

Boztas, S. (2022, December 10). *The childcare benefits scandal: voices of the victims*. DutchNews. https://www.dutchnews.nl/news/2021/01/the-childcare-benefits-scandal-voices-of-the-victims/.

Chan, L.A., Der, S.Z., & Nasrabadi, N.M. (2002). *Image Recognition and Classification: Algorithms, Systems and Applications* (B. Javadi, Ed.). CRC Press

CIAT (2017). *Tax Administration Review n° 42 CIAT/AEAT/IEF*. ISSN 1684-9434.

Citron, D. & Pasquale, F. (2014). The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, 89(1), pp. 1–32.

CJEU, Case C-175/20 *'SS' SIA v Valsts ieņēmumu dienests*, ECLI:EU:C:2022:124, (2022). https://curia.europa.eu/juris/document/document.jsf;jsessionid=585975999D28585C894A285291AE718D?text=&docid=254583&pageIndex=0&doclang=FR&mode=lst&dir=&occ=-first&part=1&cid=154930.

Communication from the Commission to the EP, Council, the European Economic Social Committee and the Committee of the Regions, Building Trust in Human-Centric AI COM(2019) 168 final, (2019). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0168&from=BG.

Constitutional Court of the Slovak Republic PL. ÚS 25 / 2019-117 (December 2021) (*eKasa* case). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2021/492/20211217.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Art. 15(1). (2016) ('Law Enforcement Directive').