Co-funded by the
Erasmus+ Programme
of the European Union

Jean Monnet Network on EU Law Enforcement
Working Paper Series

Slipping through the cracks: The carve-outs for AI tax enforcement systems in the EU AI Act

David Hadwick*

Abstract

The proliferation of artificial intelligence in society has been nothing short of outstanding. While the technology can be a catalyst of societal development, AI also bears significant risks to citizens' rights. Growing awareness over these issues triggered the Commission to submit the proposal for the EU AI Act as a regulatory response to control these externalities.

Yet, confusion remains around the treatment of AI systems leveraged by tax administrations. On the one hand, Recital 37 of the Preamble prescribes that systems used to determine entitlement to public benefits should be regarded as high-risk systems. Tax benefits *sensu lato* can be regarded as a public benefit but EU law remains unclear on the subject. On the other hand, Recital 38 stipulates that models used for administrative purposes by tax administrations should not be regarded as high-risks systems used for law enforcement purposes. However, in practice the vast majority of AI models of tax administrations are regarded as models used for law enforcement under other EU law instruments such as the Law Enforcement Directive. These models are used on all taxpayers to detect fraud prior to any determination of criminal suspicion, hence the dichotomy between administrative or law enforcement nature is most definitely ambiguous. This confusion in the proposal is worrisome as tax administrations are among State organs who use most AI systems. Additionally, such systems have already led to major scandals, such as the Dutch *toeslagenaffaire* where the tax administration discriminated and profiled taxpayers on the basis of their ethnicity, causing irreparable harms. By all means, risks to citizens' rights have already materialized in the context of algorithmic tax enforcement which should warrant specific considerations under the Regulation.

This uncertainty in the current version of the proposal raises the following question: *"under a teleological interpretation of the draft proposal for the EU AI Act, should AI systems used by tax administrations be regarded as high-risk systems?"* This question is addressed in two parts. Section 1 presents the state of use of AI systems by tax administrations and the typology of functions performed by these systems, focusing in particular on whether these carry out tasks of administrative or law enforcement nature. Section 2 examines whether, under the current text of the proposal for the EU AI Act and the different positions of EU institutions, these systems should be regarded as high-risk systems. Findings show that despite the risks of AI tax systems and the fact that obligations imposed on high-risk systems could mitigate these risks, tax enforcement is neglected in the Regulation.

* David Hadwick is a researcher at the DigiTax Centre of Excellence of the University of Antwerp, and Fellow at the Fonds voor Wetenschappelijk Onderzoek (FWO)/Research Foundation for Flanders (Grant N°: 11J1522N).

Hadwick, D.[1] – "Slipping through the cracks: The carve-outs for AI tax enforcement systems in the EU AI Act"

Table of Contents

Introduction

The proliferation of artificial intelligence (AI) in society has been nothing short of outstanding. In a little over a decade, AI and in particular machine-learning (ML) models have spread to every corner of society. From meteorology, medical science, physics, to entertainment, art, and even scientific writing with 'ChatGPT'[2], not a day goes by where citizens are not confronted to ML.[3] This phenomenon has not spared tax enforcement for which tax administrations leverage ML daily. The integration of AI algorithms in tax audit processes has enabled a drastic expansion of tax enforcement capabilities, increasing the number of taxpayers audited even in sectors and areas initially out of the reach of traditional audit methods.[4] While the technology can be a catalyst of societal development, AI also bears significant risks to citizens' rights. Studies have shown how the dissemination of AI technology increases the risks of conflict with fundamental rights, such as privacy, data protection, non-discrimination, and the right to a fair

[1] David Hadwick is a researcher at the DigiTax Centre of Excellence of the University of Antwerp, and Fellow at the Fonds voor Wetenschappelijk Onderzoek (FWO)/Research Foundation for Flanders (Grant N°: 11J1522N).

[2] ChatGPT is a language model developed by OpenAI, which can be used as a virtual conversational assistant to answer queries, see: https://openai.com/blog/chatgpt/ - last retrieved January 2023. It was recently heavily criticized for enabling automated academic writing.

[3] OECD, *Artificial Intelligence in Society* (OECD, 2019), 19-22.

[4] For instance, web-scraping in France enabled the DGFiP to detect undeclared swimming pools and house extensions, approx.. 20,000 per year, in remote areas that could hardly be audited prior to AI, see: <https://www.euronews.com/my-europe/2022/08/30/france-uses-artificial-intelligence-to-detect-more-than-20000-undeclared-swimming-pools> accessed April 2023.

trial.[5] This is particularly true in the context of public governance where the target population is so large and so heterogenous. Growing awareness over these issues triggered the Commission to submit the proposal for the European Union Artificial Intelligence Regulation ('EU AI Act') as a regulatory response to control these externalities.

Yet, confusion remains around the treatment of AI systems leveraged by tax administrations in the proposed AI Act. Without a category of their own, it is unclear whether AI systems used by tax administrations qualify as high-risk systems or not. The confusion in the proposal is worrisome as tax administrations are among State organs who use AI systems the most. Additionally, such systems have already led to scandals and seminal jurisprudence such as *SyRI*[6], *eKasa*[7] or *SS SIA*[8]. The most striking example is the Dutch *toeslagenaffaire* where using an AI model, the tax administration discriminated and profiled taxpayers on the basis of their ethnicity, causing irreparable harms.[9] By all means, risks to taxpayers' rights have already materialized in the context of algorithmic tax enforcement which should warrant specific considerations, not carve-outs, under the proposed Regulation.

This uncertainty in the current version of the proposal raises the following question: *"based on a teleological interpretation of the draft proposal for the EU AI Act, should AI systems used by tax administrations be regarded as high-risk systems?"* This question is addressed in two parts. Section 1 presents the state of use of AI systems by tax administrations and the typology of functions performed by these systems, focusing in particular on whether these carry out tasks of administrative or law enforcement nature. Section 2 examines whether, under the current text of the proposal for the EU AI Act and the different positions of European Union ('EU') institutions, these systems should be regarded as high-risk systems.

[5] See *inter alia*, Frederik Zuiderveen Borgesius, *Discrimination, artificial intelligence, and algorithmic decision-making* (Council of Europe, 2018); Marta Papis-Almansa, 'The use of new technologies in VAT and taxpayers' rights' (2022) available at SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4034858> accessed April 2023; Yvan Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2018), 31 Harv. J.L. & Tech. 890; L. Scarcella, 'Tax compliance and privacy rights in profiling and automated decision-making' (2019) 8 Internet Policy Review.
[6] Rechtbank Den Haag, 5 Februari 2020 (*SyRI* case), ECLI:NL:RBDHA:2020:1878.
[7] 492 Constitutional Court of the Slovak Republic PL. ÚS 25 / 2019-117 (*eKasa* case).
[8] CJEU, Case C-175/20 *'SS' SIA v Valsts ieņēmumu dienests*, ECLI:EU:C:2022:124.
[9] For a breakdown of the *toeslagenaffaire*, see David Hadwick & Shimeng Lan, 'Lessons to be learned from the Dutch Childcare Allowance Scandal: A Comparative Review of Algorithmic Governance by Tax Administrations in the Netherlands, France and Germany' (2021) 13 World Tax Journal 609; Tweede Kamer Der-Staten Generaal, *'Ongekend Onrecht'* (The Hague, 17 December 2020); Autoriteit Persoonsgegevens (Dutch Data Protection Authority), *Belastingdienst/Toeslagen - De verwerking van de nationaliteit van aanvragers van kinderopvantoeslag* (20), Rapport N° z2018-22445.

Section 1 – The state of use of AI tax enforcement algorithms in the EU

A. The use of AI fiscal governance tools in context

Studies show that tax administrations regularly make use of ML prior and throughout the tax audit process.[10] Based on a synthetized literature review of official policy documents of the European Union (EU), the Organisation for Economic Co-operation and Development (OECD), the Intra-European Organisation of Tax Administrations (IOTA) and the Inter-American Centre of Tax Administrations (CIAT), at least 18 EU Member States' tax administrations have integrated ML to operate their fiscal prerogatives.[11] Hence, two thirds of tax administrations in EU Member States are leveraging ML-based technology to perform their missions. Tax administrations constitute one of the State organs that leverages AI the most, for a wide array of purposes, and since the longest period. Reports indicate that EU tax administrations were already beginning to make use of ML, as early as 2004.[12] Thus several years prior to predictive policing, facial recognition and other heavily debated algorithmic law enforcement methods, tax administrations were already frontrunners in the use of AI.

Three key drivers can explain the popularity of ML algorithms for public fiscal governance: first, the ever-increasing documentary burden to be processed by tax officials; second, the reduction of human resources of tax administrations; third, the necessity to strengthen e-forensics methods for e-commerce and against specific types of fast-paced fraudulent schemes. Firstly, since the financial sub-prime crisis and revelations such as the Panama and Pandora Papers, a number of regulations have been adopted to more heavily police taxpayers, in particular in the global financial sector.[13] These events led to the creation of the Base Erosion and Profit Shifting ('BEPS') project[14] and propelled policy-makers such as the EU and the OECD to revive international regulatory initiatives on the financial sector, the likes of the Common Reporting Standards ('CRS'), the Foreign Account Tax Compliance Act ('FATCA')

---

[10] See *inter alia* Marcin Rojszczak. 'Compliance of Automatic Tax Fraud Detection Systems with the Right to Privacy Standards Based on the Polish Experience of the STIR System' (2021), 49 Intertax 39; M. Papis-Almansa, 'The Polish Clearing House System: A 'Stir'ring Example of the Use of New Technologies in Ensuring VAT Compliance in Poland and Selected Challenges' (2019) 28 EC Tax Review 43; Sonia Sanchez, ''Virtual Assistant' for VAT' in OECD, *Tax Administration Series 2019 Comparative Information on OECD and other Advanced and Emerging Economies*, 176; Ignacio Gonzalez Garcia, 'Analytics and Big Data – The New Frontier: Cases of Use at AEAT' (2018) in CIAT, Tax Administration Review 44, 35-49; Diana van Hout, 'Gedragsbeïnvloeding in het belastingrecht: Are you 'nudge' (2018) 549 Tijdschrift voor Fiscaal Recht 928; Maarten van Luts & Marc van Roy, 'Nudging in the context of taxation' (IOTA Publishing, 2019); OECD, *Advanced Analytics for Better Tax Administration* (2016), 23 & 39.

[11] David Hadwick, 'Behind the One-Way-Mirror: Reviewing the Legality of EU Tax Algorithmic Governance' (2022) 31 EC Tax Review 184 https://doi.org/10.54648/ecta2022019; The author has designed a website with an empirical inventory of all ML systems used by tax administrations in the EU, see: David Hadwick, 'AI TAX ADMIN EU' <https://www.uantwerpen.be/en/projects/aitax/country-reports/> accessed April 2023.

[12] European Commission, Risk Management Guide for Tax Administrations – Fiscalis Risk Analysis Project Group (February 2006), 67.

[13] Aanor Roland, 'Multiple Streams, leaked opportunities and entrepreneurship in the EU agenda against tax avoidance' (2020) 6 European Policy Analysis 77.

[14] Allison Christians and Stephen E. Shay, 'Assessing BEPS: Origins, Standards, and Responses' (2017) 102A Cahiers de Droit Fiscal International, Available at SSRN: <https://ssrn.com/abstract=2997548>; Alisson Christians & Laurens van Appeldoorn, *Tax Cooperation in an Unjust World* (OUP 2021), 4.

and Anti-Money Laundering ('AML') regulations.[15] These initiatives led to the addition and strengthening of several mechanisms of cross-border data transfer such as the Automatic Exchange of Information ('AEoI'), Country-by-Country reports ('CbCr'), and the administrative cooperation Directives ('DAC') in the EU.[16] The primary effect of the foregoing was an exponential increase in the administrative burden for tax officials, who on the receiving-end of all that data, had to process it. Given the amount of data transferred, doing so manually would be tremendously labor- and resource-intensive. Hence, automation and machine-learning became natural allies of choice.

Secondly, the financial crisis also had an effect on the human workforce and composition of the administration itself. Following the crisis, almost every States in the EU and beyond had to adopt austerity measures, which included institutional reorganizations and reduction of the workforce employed by public sector organs such as the tax administration. On average, from 2009 to 2018, tax administrations in the EU lost about 14.2% of their entire workforce as reported by the European Public Service Union ('EPSU').[17] In some jurisdictions, such as Belgium, Latvia and Lithuania, the number is close to 30%.[18] These individuals were not necessarily laid off as a result of the crisis. Rather, positions of employees who left were not renewed and part of their tasks were outsourced sometimes to the private sector, such as catering, but also to technology with the adoption of machine-learning models.

Thirdly, the enlargement of digital marketplaces and e-sharing websites, e.g., Amazon or Airbnb, and the apparition of new digital assets such as cryptocurrencies, forced the administration to expand their surveillance capabilities. The use of ML algorithms enables tax administrations to more efficiently monitor the previously dark corners of the internet, such as online gambling websites, security exchanges and trading platforms, or even the deep web.[19] With the emergence of these new ways of commerce came new forensic accounting methods, such as machine-learning web-scraping.[20] Aside from these new business models, EU tax administrations required e-forensics methods capable of flagging transactions in real-time or near real-time to combat fast-paced fraudulent schemes. This is particularly true for so-called 'carousel frauds' or Missing Trader Intra Community Fraud ('MTIC'), which continue to generate 60 billion euros in tax losses annually according to Europol.[21] These fast-paced

[15] Harriet Brown & Grahame Jackson, *A Practitioner's Guide to International Tax Information Exchange Regimes: DAC6, TIEAs, MDR, CRS and FATCA* (Spiramus Press Ltd., 2021), 13.
[16] Aanor Roland & Indra Römgens, 'Policy Change in Times of Politicization: The Case of Corporate Taxation in the European Union' (2021) 60 Journal Common Market Studies 355, https://doi.org/10.1111/jcms.13229.
[17] Lionel Fulton, 'The Impact of Austerity on Tax Collection' (2020) *European Public Service Union* Report n°3, 18.
[18] *Ibid*. Fulton (2020), 17.
[19] IOTA, *Deep Web – IOTA Report for Tax Administrations* (IOTA 2012), pp. 15-16; CIAT Technical Conference, *Prevention and Control of Tax Evasion* (Nairobi Sep. 2013); 8-10; Dirk Dierickx 'The Belgian compliance model and the methodology to obtain data from "Sharing Economy" platforms' in *Disruptive Business Models – Challenges and Opportunities for Tax Administrations* (IOTA 2017), 21-23.
[20] JB Hillman, 'Disruptive technology: Impact on compliance' in *Disruptive Business Models – Challenges and Opportunities for Tax Administrations* (IOTA 2017), 31-33.
[21] See EU Parliament Press Release (19 February 2021): https://www.europol.europa.eu/media-press/newsroom/news/police-dismantle-criminal-network-linked-to-international-vat-fraud-trading-vegetable-oil accessed April 2023.

fraudulent schemes have led to the creation of ML models, such as Transaction Network Analysis, to enable the real-time flagging and detection of fraudulent transactions.[22] Thus, the digitalization of the economy and of fraudulent schemes generated an incentive for automation and the use of ML for fiscal governance. As an authority tasked with monitoring the market, the tax administration had to closely follow and mimic its digitalisation, to keep up with its pace.

B. The typology of AI fiscal governance tools

Tax administrations are tasked with a wide array of prerogatives that extend beyond the classical punitive enforcement of taxation rules. Traditionally, tax administrations perform the recurrent verification of tax returns and are also tasked to investigate, detect, and prevent tax non-compliance and tax fraud through various methods of forensic accounting. Yet, the tax administration also serves a certain number of additional ancillary missions. For instance, tax administrations are obliged to aid taxpayers by answering specific queries or even jointly complete returns with taxpayers upon request.[23] Tax officials can negotiate advanced pricing agreements ('APA') with taxpayers who request it.[24] In some jurisdictions such as the Netherlands, the administration is also disbursing social benefits such as childcare allowances and investigating fraudulent reception of these benefits, as was seen in the *toeslagenaffaire*. Tax officials cooperate with prosecutors and police in the investigation and prosecution of criminal networks that typically commit tax fraud in addition to their core criminal activities. They also cooperate with food safety administrations, with labour inspectorates, with migration authorities or with securities and exchanges administrations. Hence, tax administrations are an extremely polyvalent regalian organ that must carry out tasks of social assistance, of cooperative compliance by answering queries and concluding APAs, of administrative nature through the recurrent verification of returns, and of criminal nature by investigating and preventing tax evasion and fraud. The aforementioned description does not consider the nuances between the different departments of the administration, such as customs administration who perform missions that are entirely different from personal taxation or large enterprises. From one department to the other, the job description and skills required for the function may be entirely at odds.

This wide array of prerogatives is also reflected in the different types of AI models leveraged by tax administrations. In society, AI and ML can be used to perform a quasi-infinite number of functions ranging from movie recommendation, weather forecasts, econometric prediction of share prices to medical diagnostics.[25] The same can be observed in the niche microcosm of tax enforcement, where ML is not a monolithic unitary ensemble, but is used to perform distinct

[22] OECD, *Tax Administration Series (TAS) Comparative information on OECD and Other Advanced and Emerging Countries* (OECD, 2021), p. 110; Thomas Wahl, eucrim 2019: <https://eucrim.eu/news/new-data-mining-tool-combat-vat-fraud/> accessed April 2023.
[23] See for instance in Belgium, SPF Finances (Belgian tax administration) website: <https://finances.belgium.be/fr/particuliers/declaration_impot/declaration/aide> accessed April 2023.
[24] Christina HJI Panayi, *Advanced Issues in International and European Tax Law* (Bloomsbury, 2015), 190-191.
[25] OECD, *Artificial Intelligence in Society* (OECD, 2019), 19-22.

functions. Based on a synthetized literature review of official policy documents, a function-based typology of these different AI systems can be drawn. Following this review, at least 70 different AI systems were identified in 18 EU Member States, which can be classified in 6 distinct archetypal functions, with several sub-types.[26]

These 6 archetypal functions are:

1. **Taxpayer assistance:** this archetype is composed of models meant exclusively to aid taxpayers in a voluntary and consensual manner. Two sub-types fall in this category: first, *Virtual Conversational Assistants* ('VCA'), so-called chatbots, who answer taxpayer queries; second, *subject identification systems*, i.e., models meant to identify taxpayers eligible to specific types of aids, such as COVID relief.[27]

2. **Data collection:** this archetype qualifies ML systems that automatically collect taxpayer data online, i.e., web-scraping systems.[28] The sources of data collection may vary but typically include e-commerce platforms, social media, financial institutions, gambling websites, data leaks such as the Panama Papers, dark web platforms, etc. Web-scraping systems are also not bound to textual formats, but can include machine-vision to process data from pictures[29], satellite images[30] or road camera footages[31].

3. **Risk detection:** are ML systems which assist tax administrations in the detection of statistical indicators of risks of non-compliance and/or fraud, by flagging 'outliers', i.e., potential abnormal transactions, under-reported income, under-valued assets, by matching taxpayer data to verify their coherence, or through the visualization of networks of taxpayers.[32] Because tax fraud is an umbrella term qualifying a large number of distinct phenomena, statistical indicators of risks vary widely. Accordingly, the ML systems used for risk detection equally differ with a number of sub-types,

[26] Hadwick (n 11) 186-187; Hadwick, 'AI TAX ADMIN EU' <https://www.uantwerpen.be/en/projects/aitax/country-reports/> accessed April 2023.
[27] US - EU Trade and Technology Joint Statement, *The Impact of Artificial Intelligence on the Future of Workforces in the EU and the USA* (2022), 9.
[28] France: Décret n° 2021-2148 du 11 février 2021 portant modalités de mise en oeuvre par la direction générale des finances publiques, des douanes et des droits indirects, Art. 4, III, 1°-2° ; Belgium: Dirk Dierickx 'The Belgian compliance model and the methodology to obtain data from "Sharing Economy" platforms'(2017) in *IOTA Disruptive Business Models : Challenges and Opportunities for Tax Administrations*, 21-23; Sweden: IOTA, *Deep Web – IOTA Report for Tax Administrations* (2012), 16-19.
[29] Décret n° 2021-2148 du 11 février 2021 portant modalités de mise en oeuvre par la direction générale des finances publiques, des douanes et des droits indirects, Art. 4, III, 1°-2°.
[30] Vincent Coste, AFP, 'Le fisc français traque les piscines non déclarées par IA et récupère 10 millions d'euros' : https://fr.euronews.com/2022/08/30/le-fisc-francais-traque-les-piscines-non-declarees-par-ia-et-recupere-10-millions-deuros - last accessed April 2023.
[31] Csilla Tamas Czinege, 'Risk management in order to enhance compliance of taxpayers in Hungary' (IOTA, 2019) <https://www.iota-tax.org/sites/default/files/documents/publications/IOTA_Papers/iota_paper_risk_analysis_in_hungary.pdf> last accessed April 2023.
[32] Ireland : OECD, *Advanced Analytics for Better Tax Administration* (2016), 23; Revenue, *Code of Practice for Revenue Audits and other Compliance Interventions* (2014), 11-12, see REAP and VAT RTRF.

ranging from Transaction Network Analysis[33], Social Network Analysis[34], clustering[35], outlier detection[36], etc.

4. **Risk-scoring:** or Risk-Management Systems ('RMS') are tools which predict the risks of non-compliance/fraud associated with individual taxpayers, attribute a score to taxpayers and segment taxpayers into categories of risks based on the score attributed. This score is computed on the basis of the risk indicators previously detected by risk detection tools. The segmentation of taxpayers can then be used as a (pre-)selection for further audits by the tax administration.[37] Risk-scoring tools can fall within two categories, *external* risk management which attribute scores to individual taxpayers, or *internal* case management which given an individual score, determine the best course of action for the administration, i.e., whether means of cooperation/coercion are most appropriate and which ones should be leveraged in a specific instance.[38]

5. **Nudging:** qualifies tools that adapt the default language used on communication sent to taxpayers based on their risk profiles. For instance, notoriously non-compliant taxpayers may receive communication with additional references to penalties, so-called 'negative nudges'; while vulnerable taxpayers may receive communication with specific references to the possibility of receiving assistance.[39]

6. **Jurisprudence analysis:** are ML systems which automatically process case-law pertaining to a specific query and predict the likelihood of success of a specific claim. These systems are used internally by tax administrations to determine litigation/prosecution strategies or to answer taxpayer queries and objections.[40]

[33] Wahl (n 22).
[34] Garcia (n 10) 'Analytics and Big Data – The New Frontier: Cases of Use at AEAT'; OECD (n10) *Advanced Analytics for Better Tax Administration* (2016), 21.
[35] OECD, *Advanced Analytics for Better Tax Administration* (2016), 23-24.
[36] OECD (n10) *Advanced Analytics for Better Tax Administration* (2016), 21.
[37] Finland: OECD, *Advanced Analytics for Better Tax Administration* (2016), p. 26; Slovakia: IOTA, *Data-Driven Tax Administrations* (2012), pp, 14-15; Spain: Ana Ortega, 'Recent and Future Developments of the Spanish Tax Agency in the Immediate Supply of Information System', IOTA: <**https://www.iota-tax.org/news/recent-and-future-developments-spanish-tax-agency-immediate-supply-information-system**> accessed February 2023.
[38] Belgium: OECD, *Tax Administration Series 2017 Comparative Information on OECD and other Advanced and Emerging Economies*, 110-111 (Box. 6.15); OECD, *Tax Administration Series 2019 Comparative Information on OECD and other Advanced and Emerging Economies*, 52.
[39] van Hout (n 10), 928; van Luts & van Roy (n 10), 23 & 36.
[40] OECD Forum on Tax Administration (FAT), Inventory of Tax Technology Initiatives, Table TRM1: <https://www.oecd.org/tax/forum-on-tax-administration/tax-technology-tools-and-digital-solutions/tax-rule-management-and-application.htm> accessed April 2023.

Section 2 – Should AI fiscal governance tools be regarded as high-risk systems?

A. The regulatory structure of the EU Artificial Intelligence Act

Prior to diving in the specific question of whether high-risk AI systems are used by tax administrations, it may be judicious to remind readers of the regulatory structure and objectives of the AI Act.

As stated in the Explanatory Memorandum, the EU AI Act seeks to address two competing interests: first, the promotion of responsible technological innovation; and second, the protection of EU citizens' fundamental rights.[41] To that end, the proposed Regulation emphasizes on proportionality, as a mean to ensure that only AI systems deemed the riskiest for fundamental rights are subject to the strictest and most extensive obligations. Accordingly, the AI Act is structured on the basis of a 'risk-based approach' with 4 mutually exclusive categories of risks: prohibited systems, high-risk systems, minimal risk systems and limited risk systems as the remainder category.[42] Depending on the deemed attribution of risks, the obligations incumbent on the controllers of AI systems will vary. Prohibited systems are outright banned. High-risk systems must comply with strict requirements such as conformity assessments, strict transparency requirements, record-keeping, and human oversight obligations. Minimal risks systems must simply comply with selected minimal transparency requirements. Limited risks systems are encouraged to comply with unspecified voluntary codes of conduct, i.e., self-regulation, and are otherwise not subject to any of the aforementioned obligations. Hence, the higher the level of risks within the risk-based approach, the stricter the regulatory regime will be, in line with proportionality.

There does not seem to be a clear methodology to establish whether a system should be qualified as a high-risk system for the purpose of the Regulation. Veale and Borgesius have pointed out how the Regulation follows a form of 'standalone' methodology, where specific functions of AI systems within specific sectors are deemed high-risk system by the AI Act, in Annex III of the instrument.[43] The same should be said of the entire risk-based approach, where systems that are deemed prohibited or as having minimal risks, are not qualified using a clear and transparent methodology. So much so, that in several sectors and several functions prescribed in the instrument, the qualification seems arbitrary. Having regard to literature on the subject, and to systems used in other jurisdictions, the Commission designated the models to ban and those to promote in the Internal Market, in concert with specific European Parliament ('EP') committees. This is also reflected in the different categories of high-risk

[41] EU Commission, Explanatory Memorandum to the Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final, 1.1. (21st April 2021).

[42] *Ibid.*, See in 3.3. Impact Assessment : Option 3+ *''Horizontal EU legislative instrument following a proportionate risk-based + codes of conduct for non-high-risk AI systems''* was chosen after consultation with the 'Regulatory Scrutiny Board'.

[43] Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 4 Computer Law Review International 102.

systems, which correspond to the thematic of certain committees, such as transportation, environment and public health, culture, legal affairs – corresponding both to EP committees and points of attention in the AI Act.[44] In that regard, one cannot deny the highly political nature of the instrument, echoing statements of 'European exceptionalism' in law-making, somewhat akin to the General Data Protection Regulation ('GDPR').

The initial approach of the Act to designate specific sectors and specific functions as high-risk categories by virtue of this specific function and specific sector of activity should be lauded. This 'function-based and sector-based' approach assert the Commission's view of AI systems as functional tools, whose risks depends on how they are used, for what purposes and by whom. Similarly to most purposive tools, their function, i.e. the purpose for which the AI system is used, is the best predictor of the risks of that system. For instance, the same K-nearest neighbour model can be used to predict tax fraud[45], to approximate colours when zooming on a picture[46], or to predict the weather[47] – all activities which generate vastly different risks for individuals. Such an approach clearly adds substantial nuance to the GDPR, where AI systems were either treated as any processing activity or as automated decision-making without differentiation of the purpose of the model, the controllers, and its end consequences.[48]

However, this standalone methodology bears one major shortcoming, namely: it is static, as new AI systems that do not fall within the already established categories will not be subjected to any obligations. These new systems are *ipso facto* 'loopholes' that risk subjecting the instrument to legislative obsolescence. For an instrument meant to regulate fast-developing technology, it is ironic. Systems used by tax administrations provide an example of such sector, which despite exhibiting risks to citizens' rights, do not fall within existing categories and thus whose current treatment under the law is not clear. Hence, while this functional approach represents a step in the right direction, it should be coupled with a clear methodology to determine the risks of each AI systems. Article 7 and 73 of the Act do provide that the Commission may adopt delegated acts to amend the list of high-risk systems in Annex III without adding new sectors, if risks of these new systems would be equivalent or greater than

[44] See for instance, Opinion of the Committee on Transport and Tourism on the proposal for the artificial intelligence act, COM(2021) 2021/0106(COD) – Rule 56 Opinion, Amendment 7, advocating for biometrics in transport and tourism (12 July 2022); Opinion of the Committee on Culture and Education, COM(2021) 2021/0106(COD) – Rule 57 Opinion, Amendment 10, advocating for the prohibition of biometrics in publicly accessible spaces (21 February 2022); Opinion of the Committee on Industry, Research and Energy – Rule 57 Opinion, advocating against barriers to industrial research and development, COM(2021) 2021/0106(COD) (14 June 2022).

[45] Darshan Kaur and Shubhpreet Kaur, 'Machine Learning Approach for Credit Card Fraud Detection (KNN & Naïve Bayes)' (2020) *Proceedings of the International Conference on Innovative Computing & Communications* (ICICC) 2020, available at SSRN: https://ssrn.com/abstract=3564040 or http://dx.doi.org/10.2139/ssrn.3564040 accessed April 2023.

[46] Vandna Bhalla & Santanu Chaudhury, 'Artificial Immune Hybrid Photo Album Classifier' in Raman and others (eds.), *Proceedings of International Conference on Computer Vision and Image Processing* (Springer, 2016), 475-477.

[47] Yousif Elfatih Yousif, 'Weather Prediction System Using KNN Classification Algorithm' (2022) 2 European Journal of Information Technologies and Computer Science 10.

[48] As a model either qualifies as 'automated processing' by virtue of Art. 22 GDPR, or is treated as any data processing activity.

those already listed. Yet, again these provisions do not prescribe a methodology for such risk-analysis. Plenty of such methodologies exists, even within EU policy documents.[49] The lack thereof in the AI Act will inevitably generate issues, either of lack of enforcement for specific functions, for new sectors, and/or of 'loopholes' for new types of AI systems, as can be seen with the case of AI systems used by tax administrations.

B. The specific treatment of AI systems used by tax administrations

Accordingly, the question is whether under a teleological *de lege lata* interpretation of the current proposal of the EU AI Act, AI systems used by tax administrations in the EU should qualify as high-risk systems. To answer this question, one must first examine Art. 6(2) in conjunction with Annex III, which contains the Commission's list of high-risks systems used by public authorities. By elimination, two sectors appear as the likeliest candidates for AI systems leveraged by tax authorities, namely: law enforcement (Annex III (6)) or access to essential public services and benefits (Annex III (5)).

High-risk systems used by law enforcement

Among the different public authorities identified as high-risk sectors in the current draft proposal for the EU AI ACT, the best fit seems to be law enforcement. After all, tax administrations are the authorities tasked with the enforcement of taxation rules, both in administrative and penal instances. Tax administrations can qualify as a 'competent authority' by virtue of Article 3(7) of the Law Enforcement Directive ('LED'), as a public authority competent for the prevention, investigation, detection or prosecution of criminal offences, e.g., tax fraud, to cite just one. Hence, tax administrations are regarded as a form of law enforcement in other EU law instruments. This qualification of tax administration as a law enforcement authority is also reflected in tax procedural codes, where several of their provisions are direct transposition of the LED.[50] For instance, certain limitations and exceptions to data subjects' right to access and right to information in Articles 13(3) and 15(1) LED have been transposed in national tax procedural rules. This follows the fact that the LED is a Directive and thus in principle requires transposition in national law, unlike the GDPR which is a Regulation. Direct transposition of LED rules is testimony to the fact that legally tax administrations are, in certain instances at least, viewed as a form of law enforcement.

[49] See Opinion of the German Data Ethics Commission on Algorithmic Systems (October 2019), submitted within the framework of Germany's AI strategy – a five-tiered risk-based approach, based on a casuistic assessment of potential harms, pp. 19-22; Ezeani and others, *EY survey of artificial intelligence risk assessment methodologies – The global state of play and leading practices identified* (Ernst & Young, 2021), 1 – 44.

[50] See, in Belgium : Loi du 5 Septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, Art. 89, 1° and 2°. In France: 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 » (as amended by Arrêté du 8 mars 2021), Art. 4(1) ; Or in Poland: STIR law, Art. 119.

The Explanatory Memorandum explicitly states that the proposal for the AI Act is without prejudice to the GDPR and the LED and completements these instruments. Technically AI is a specific form or instance of data processing, thus the AI Act will be *lex specialis* to the GDPR and the LED.[51] Thus a literal application of these pre-existing instruments should dictate that tax administrations also qualify as a law enforcement authority in the AI Act. On that basis AI systems that can potentially be used by tax administrations to predict the occurrence of a crime, such as data collection, risk-detection, and risk-scoring tools, should qualify as high-risk systems in accordance with Art. 6(2) and Annex III 6(e-f) of the AI Act. In essence, these tools should be regarded as 'predictive policing', a category of high-risk AI systems. Hence these tools should be subjected to the strict obligations in Articles 8 to 15 of the AI Act, e.g., conformity assessments, obligations of human oversight, transparency, record-keeping, etc.

However, under the initial proposal of the EU AI Act, published on the 21st of April 2021, Recital 37 prescribed that "*systems used by tax administrations should not be regarded as high-risk systems of law enforcement authorities*".[52] This Recital was surprising as the first draft of the proposal was published only three months after the revelation of the *toeslagenaffaire*, when the Dutch cabinet had just resigned and victims of that scandal caused by the Dutch tax administration had not yet been compensated.[53] The scandal was arguably the most striking example of the materialization of the risks of AI systems used by public authorities, such as discrimination, unfair trial, privacy infringements. To this day, the *toeslagenaffaire* remains the case with the highest fine imposed on any actor by the Dutch Data Protection Authority (DPA).[54] By essentially creating a carve-out specifically for tax administrations, the first draft of the proposal sharply contrasted with the gravity of these events. The obligations imposed on high-risk systems in the AI Act could have mitigated the severity of the events of the *toeslagenaffaire*, if not entirely prevented it. Data governance obligations (Articles 10(2)) and transparency requirements (Art. 13(3)(b)) imposed on high-risk systems would have shown at the outset that the *Belastingdienst* was using sensitive features, such as nationality, that generated a disproportionately prejudicial effects for minority groups. In addition, record-keeping obligations (Article 12 (1)) and human oversight (Article 14(2)) would have drastically shortened the audit process for the DPA. From a perspective of *de lege ferenda*, it seems senseful to include such systems as high-risk, as it could avert another scandal of such magnitude.

With the adoption of the common position of The Council, so-called 'general approach' on the AI Act, the text of this Recital was amended. Under the current version of the draft proposal

[51] Bogucki and others, *The AI Act and Emerging EU Digital Acquis – Overlaps, gaps and inconsistencies* (CEPS, 2022), 7.
[52] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206, Preamble Recital 37 (21st April 2021).
[53] Tweede Kamer der Staten-Generaal (n 9), 1-7.
[54] Autoriteit Persoonsgegevens [Dutch Data Protection Authority] (2022): <https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-zwarte-lijst-fsv> accessed April 2023; see also Autoriteit Persoonsgegevens, *Belastingdienst – Verwerking van persoonsgegevens in de Fraude Signale Voorziening*, Rapport no. z2020-04615 (2021), 1 – 89.

for the EU AI Act, Recital 38 (formerly Recital 37) of the Preamble prescribes a form of negative test, where systems used by tax administrations specifically intended for administrative purposes do not qualify as high-risk systems used for law enforcement. Accordingly, Recital 38 establishes a strict dichotomy between administrative purposes and law enforcement. Under a literal reading of Recital 38, only the latter would qualify as high-risk systems. Recital 38 espouses the logic that a criminal sanction is typically graver than an administrative one, so models used to detect crimes should warrant stricter compliance norms. Thus, under the current proposal, a predictive model to allocate resources to areas for the prevention minor offences, e.g., to detect graffiti (minor vandalism), an offence punishable with a maximum of 200 euros, would qualify as high-risk.[55] While a system used to detect tax non-compliance, where fines can reach millions, would not qualify as high-risk. Notwithstanding the risks to privacy, data protection, non-discrimination and fair trials, the sanctions are of the same nature, i.e., a pecuniary sentence, yet for tax offences the fine can be thousands of times more important.

Hence, to determine whether systems used by tax administrations qualify as high-risk systems used by law enforcement, one must examine whether the system is used to detect criminal offences. Arguably, answering taxpayer queries through chatbots can be regarded as an administrative task, no different than responding to a query via the phone or email. The same could be said of automated jurisprudence analysis and nudging which *in fine* only examines jurisprudence or slightly change the language of letters sent to taxpayers, hence can never bear a coercive or punitive consequences. Yet, the three other archetypal systems (data collection, risk detection and risk-scoring) used by tax administrations can be both used with a purely administrative end-goal and as penal punitive enforcement tools. Thus, the negative test prescribed in Recital 38 begs the question of whether there are criteria in the law or in jurisprudence to differentiate between situations of administrative and law enforcement nature.

The ambivalence of the administration as an authority whose prerogatives include both administrative and penal matters is not novel. As previously said, tax administrations are an extremely polyvalent organ, meant to perform a wide array of missions and to cooperate with a number of other State institutions. In several EU tax procedural codes, the severity of the fine or sanction attached to a tax offence often hangs primarily on whether the discrepancy in a tax return was intentional or not, and thus qualifies as a criminally reprehensible fraud or not. The difference between fraud or administrative non-compliance is often simply one of intention of the perpetrator, i.e., the subjective element of the crime. Yet, this salient feature bears substantial consequences on the severity of the sanction, procedural safeguards prior or during the investigative process and the rights of the defendant at potential proceedings. Accordingly, the distinction between administrative and penal matters, although blurry at times as it almost exclusively rests on subjective elements, is crucial and regularly debated before courts. With the advent of the GDPR and the LED, a layer of complexity was added to that distinction as data subject rights equally rests on that distinction. Several rights of the GDPR, particularly

[55] When comparing the Belgian sanctions: Art. 559 Code Pénal and Art. 444 CIR 92.

rights to access and rights of information are limited in the LED, based on the rationale that providing a data subject with extensive access to information could jeopardize an investigation. Two cases of the Court of Justice of the European Union ('CJEU'), referred by a Latvian court, dealt with this very question: whether a public authority tasked with both administrative and penal matters may be regarded as either bound by the GDPR or by the LED. In *B v Latvijas Republikas Saeima*[56], the Court was asked whether agents preventing road traffic offences qualified as competent authority under the LED. According to Latvian road traffic regulation, penalty points imposed on drivers on accounts of traffic offences, would be inscribed in a publicly accessible national register. The question of which instrument applied, whether GDPR or LED, was crucial to determine whether the register could indeed be accessed by the public. Ultimately, the Court sided with the defendant and ruled that a competent authority under the LED, acting for purposes other than purely criminal matters should be regarded as bound by the GDPR. The Court explicitly prescribed that Article 2(2) of the GDPR, which excludes from the scope of the Directive acts carried out by competent authorities for the prevention of crimes, should be interpreted strictly and narrowly in light of the maximum harmonization objectives of the GDPR. Accordingly, the LED should be viewed as a *lex specialis* to the GDPR, with a narrow scope that only triggers in cases that exclusively concerns criminal matters.

However, the question remains for public authorities when in light of what transpires in the data processed, an initially administrative matter evolves into a criminal investigation. As said, the difference between administrative fiscal non-compliance and fraud is often only a matter of subjective intention. These intentions may not be clearly established upon reception of the data, but become clear upon further investigation. Initially, the data will only reveal a discrepancy between tax returns and estimations of the administration, suggesting grounds for an investigation. Upon further inquiries, it may be shown that in fact these discrepancies are verified, and are due to the intentional acts of a taxpayer. Accordingly, the initial request of the tax administration to obtain data is of an administrative nature, but has evolved into a criminal matter. Such a situation begs the question of what instrument the tax administration should comply with. In February 2022, The Court responded to such preliminary question referred in the course of a litigation between a company and the Latvian tax administration. In *SS SIA*[57], the CJEU found that because the requests for information did not initially have the specific purpose of combatting crimes, the tax administration was bound to the GDPR. As the request for tax data was a recurrent request not specifically designed to investigate or prevent a crime, the processing of data by the tax administration did not fall within the LED in that specific instance. The Court acknowledges that the tax administration is a competent authority under the LED, but points out to Recitals 10 and 11 of the GDPR which stipulate that a competent authority acting for purposes other than those mentioned in the LED, is bound to the GDPR. Accordingly, having regard to Recital 38 of the AI Act and to jurisprudence on the subject, the conclusion is that only AI tools designed exclusively to investigate fiscal crimes may be regarded as high-risk systems. Ultimately, the two aforementioned CJEU cases simply formulate the dichotomy of Recital 38 in the reverse way. Whereas Recital 38 excludes models

[56] CJEU, Case C-439/19 *B v Latvijas Republikas Saeima*, ECLI:EU:C:2021:504, paras 65 to 71.
[57] *'SS' SIA* (n 8), paras 39 to 45.

used specifically for administrative purposes from high-risk systems, CJEU jurisprudence only regards models designed exclusively to investigate crimes as high-risk systems.

The question is thus how to practically operate the distinction between AI systems used by tax administrations for administrative purposes or exclusively for criminal matters. In practice, AI systems are never designed nor used for an exclusively administrative or exclusively criminal purpose. AI systems are meant to predict material situations, such as gradients between declarations of taxpayers and statistical predictions based on objective risk-factors. What differentiates a situation of 'administrative' non-compliance from a 'criminal' case of fraud, is not material tangible facts, but the subjective intention of the perpetrator. The salient factor between the two is not the '*actus reus'* but the '*mens rea*' in legal terminology.[58] Yet, intention is an element for which AI systems are virtually powerless, as the intention of the perpetrator can hardly be statistically determined. The same risk detection models may reveal correlations and risk-indicators that apply both to administrative offences and to crimes. The same web-scraping system can both be used to collect data to verify administrative compliance or to investigate crimes. Risk-scoring models are used to select taxpayers for audit prior to whether these are suspected of tax fraud or tax compliance, hence prior to any determination of subjective intention. Yet, according to Recital 38 and the jurisprudence of the Court, unless the tool was used for an exclusively criminal purpose, it cannot be regarded as a high-risk system. In practice, such a high threshold will never be fulfilled by virtue of the nature of AI technology, as a system that is not designed to detect subjective intention.

Moreover, the dichotomy in Recital 38 entirely rests on the internal qualification of the offence under national law. Yet, the definition of tax criminal offences are far from being harmonized in EU Member States, so much so that not all types of fraud are uniformly viewed as the same type of offences.[59] What is regarded as a crime according to the national law of one Member States, is not necessarily regarded so in another. This was the *raison d'être* of the Directive on the Protection of the Union's Financial Interest ('PIF'), namely the harmonization of the most serious types of frauds.[60] However, it only harmonized the gravest types of frauds, e.g., VAT frauds exceeding 10 million euros. Other types of fraud remain unharmonized and at the whims of national law.[61] Accordingly, the same types of AI systems combatting the same offences, would not always be regarded as high-risk systems in every jurisdiction by virtue of differences in Member States' national law. Applying a strict reading of Recital 38 would thus result in a substantial fragmentation of taxpayers' rights, depending on the jurisdiction.[62] Hence, Recital

[58] See for instance, Art. 444 (administrative sanction) and Art. 449 (criminal sanction) in Code de l'impôt sur les Revenus 1992 (Belgian tax code) (CIR 92).
[59] Günter Heine, 'Changes in Criminal Law and Cooperation through, in Particular, the Schengen Agreement and Europol' in Husabo & Strandbakken (eds.) *Harmonization of Criminal Law in Europe* (Intersentia, 2005), 43-45.
[60] Directive 2017/1371 of the EP and the Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law *O.J.* L 198/92 ('PIF')
[61] *Ibid.*, PIF, Art. 3(2)
[62] See EU AI Act, Articles 8 to 15, these obligations include: Art. 15 accuracy and cybersecurity; Art. 14 human oversight; Art. 13 transparency, etc.

38 does not constitute an adequate criteria for a Regulation, where the end-goal is to harmonize standards of EU law.

Finally, the dichotomy in Recital 38 reinforces the current power imbalance between the administration and citizens, by virtue of the epistemological gap regarding AI systems used by tax administrations. Simply put, no one but the tax administration knows for what purpose the AI system is designed and used. Despite being required by the principle of legality, AI systems used by tax administrations that pose a limit to the exercise of fundamental rights are often not regulated by law. Prior studies have shown how the vast majority of EU Member States do not have a legal basis authorizing the use of AI by tax administrations, both for administrative and criminal matters.[63] In the absence of any legal basis, the tax administration may solely and arbitrarily decide to use AI systems for any purposes, or even interchangeably. In addition, without any legal basis, taxpayers simply cannot determine for what end-goal an AI system is used. This epistemological gap between what is publicly reported by the administration and what actually occurs with AI systems reinforces the opacity of the administration, empowered to simply cherry-pick the most favourable regime and the models it wants to see bound by the AI Act.

Conclusively, determining whether a specific AI system qualifies as high-risk system used by law enforcement for the purpose of the AI Act is an entirely casuistical exercise. At the outset, several functions identified in the typology may be excluded, namely: taxpayer assistance, nudging and jurisprudence analysis. The reason being that these tools are exclusively or predominantly used specifically for administrative purposes. For the three remainder functions: data collection, risk detection and risk-scoring, whether these qualify as predictive policing tools will depend on their end-goal as specifically administrative or penal. Yet, given the nature of these tools and the high threshold set by Recital 38, it is likely that very few of these tools will qualify as high-risk systems. In practice, AI systems used by tax administrations do not fit within a binary dichotomy, as either exclusively administrative or law enforcement purpose. Most systems will initially detect instances of non-compliance whose qualification will organically transform into fraud investigations at the behest of tax officials. Accordingly, in practice very few AI systems if any are used exclusively for administrative or criminal matters. Hence very few ML models, if any, would thus qualify as high-risk AI systems.

High-risk systems for access to essential public services

The second category to which AI systems used by tax administrations could belong to are AI systems used to determine access to and enjoyment of essential public services (Annex III (5)). As explained in Recital 37 of the Preamble, systems used to evaluate eligibility to essential public services should be deemed high-risk systems, as such systems ultimately determine a person's access to crucial resources or services. These systems are thus liable to have a significant impact on a persons' livelihood or fundamental rights and potentially lead to discrimination and historical patterns of unfairness. Recital 37 provides a number of examples

[63] Hadwick (n 11), 198 – 200.

for this category such as creditworthiness assessments for housing, electricity, communication services, etc.

The question is thus whether tax administrations or certain of their missions qualify as an essential public service, or whether tax benefits qualify as an essential public benefit. Pragmatically, one could say that taxation is an essential part of Statehood and that tax benefits are essential in the financing of public infrastructures. Thus, tax enforcement could be seen as an essential public service. Moreover, the systems used to assess creditworthiness or revoke a benefit often have the same end-goal, verifying through various means whether what is declared by the welfare recipient is in fact correct financial information. Hence, these systems whether used by any public authority including the tax administration or by private actors, are in their very essence, economic profiling tools. To that end, public authorities and private actors often use the same means of control, whether that is web-scraping, risk-detection, and risk-scoring. Consequently, following the logic of the functional risk-based approach of the instrument, AI systems used by tax administrations could qualify as high-risk systems to determine access to essential public services. If it quacks like a duck and walks a duck, it should be a duck. Yet, similarly to Recital 38, the issue with this provision is the fact that there is no guidance on what constitutes a 'public service', let alone an 'essential' one.

The closest notions in EU law to that of 'essential public service' as described in Recital 37, seem to be 'Service of General Economic Interest' ('SGEI') and 'Social Services of General Interest' ('SSGI'), often cited in EU State aid cases and in competition law.[64] In essence, these are services previously provided under a state monopoly, which by virtue of free competition are provided by private companies. Through deductive logic, it seems likely that the Commission when using the term 'public services' refers to SGEI, as all the examples provided of housing, electricity and telecommunication are SGEIs. If by essential public service, the Commission in fact is referring to SGEI or SSGI, then the systems used by tax administrations would not fall within Recital 37 and Annex III paragraph five. EU jurisprudence informs that activities that intrinsically form part of State prerogatives cannot qualify as SGEI or SSGI – two notions that presupposes that a private undertaking is carrying out these duties for the State. Accordingly, the administration of taxpayers and the enforcement of taxation rules, similarly to the police, the army or other regalian State prerogatives, cannot be regarded as SGEI.[65] As a result, the AI systems used by tax administrations will not qualify as systems used to determine the access to essential public services.

There is perhaps one exception to that: in certain Member States, disbursement and revocation of certain public benefits is managed by the tax administration. This is for instance the case in the Netherlands, where the *Belastingdienst* is managing the disbursement of certain social aids such as childcare allowance, as well as investigation into revocations and social security frauds. As transpired in the *toeslagenaffaire,* the eligibility and access to these benefits is determined

[64] Communication from the Commission on the application of the European Union State aid rules to compensation granted for the provision of services of general economic interest, 3.2. (11 January 2012), 2012/C 8/02.
[65] *Ibid.*, 2.1.2.; see also Case C-118/85 *Commission v Italy*, paras 7 and 8.

by AI systems that also investigate errors, frauds, and revocations of said benefits.[66] Under a teleological interpretation of Recital 37, the systems used in the *toeslagenaffaire* would thus qualify as high-risk systems. Yet, among EU Member States, the Netherlands is an exception, as most other States tend to have a separate institution specifically dedicated to social assistance, such as the CPAS in Belgium or the CAF in France. For other systems used by tax administrations not explicitly and literally meant for social assistance, a *de lege lata* interpretation should lead to the conclusion that these systems are not high-risk in accordance with Recital 37 and Annex III (5) of the AI Act.

Again, the ambiguity and the lack of guidance on crucial notions of the EU AI Act should be pointed out. The instrument resorts to alien *sui generis* notions such as 'essential public service' without prior existence in EU law or asserted definition in the text. Given the importance of these concepts in determining the appropriate risk-category, the lack of guidance is striking. Furthermore, the overall coherence of these Recitals with the risk-based approach of the EU AI Act, should be called into question. Many tax benefits, although not essential public service in name, are carrying out a mission for the benefit of the public. For instance parents, the elderly, persons with a handicap in addition to receiving direct public subsidies, also receive specific tax benefits. The only material difference between these benefits is the method of disbursement: public assistance is typically disbursed through direct subsidies, while tax benefits are computed as a minus on an outstanding burden. Yet, for parents the benefits and risks that emanate from each AI system would be identical and bear the same economic effects on their livelihood, the same effects on their fundamental rights, the same risk of discrimination, unfairness, etc.

Conclusion

Several key drivers, such as the enormous administrative burden, the reduction of human workforce and the necessity to detect fraud in real-time, designate the tax administration as a perfect candidate for automation. Yet, cases such as *SyRI, eKasa, SS SIA* or the *toeslagenaffaire* have shown how AI systems can generate serious risks to citizens' fundamental rights when leveraged by tax administrations. These cases demonstrate that the use of AI systems by EU tax administrations remains characterized by a serious opacity, unlawfulness, and a lack of safeguards or concerns for taxpayers' rights. From a perspective of *de lege ferenda* the AI systems used by tax administrations that bear serious risks on taxpayers' fundamental rights should be qualified as high-risk systems. Based on the typology laid down in this paper, these systems would be AI models belonging to at least three specific archetypes, namely: data collection, risk detection, and risk-scoring. These archetypes generate serious risks of conflicts with taxpayers' fundamental rights, such as privacy, data collection, fair trial, good administration, and risks of discrimination. Qualifying these three archetypes as high-risk systems would greatly enhance the protection of EU citizens vis-à-vis the externalities emanating from fiscal algorithmic governance.

[66] Autoriteit Persoonsgegevens (n 9), 5 - 6.

Yet, based on a teleological interpretation of the AI Act, it is unclear whether AI systems used by tax administrations would qualify as high-risk systems under the EU AI Act. Tax administrations not being singled out as a specific high-risk sector in the instrument, the current draft remains ambiguous regarding the treatment of fiscal governance algorithms. The AI Act, and in particular Recitals 37 and 38 of the current proposal, create unclear artificial dichotomies: for Recital 38 - between systems used exclusively for administrative purpose or not; for Recital 37: between systems used to determine access to essential public service or not. These distinctions are unclear, as these rest on undefined or ill-fitted notions of EU law. Accordingly, these Recitals do not provide real guidance on whether one specific model used by a tax administration would qualify as high-risk systems. The static nature of the instrument renders the regulatory approach excessively rigid, where systems must either fit within a specific sector/function or evade the application of the Regulation altogether. However, given the far-reaching consequences the label of high-risk bears for an institution as data controller or for taxpayers as data subject, these distinctions are paramount. More guidance or delegated acts on these specific provisions is required from the Commission, as the Regulation currently ignores a substantial part of predictive policing models used by tax administrations. These models have already resulted in jurisprudence and in scandals such as the *toeslagenaffaire*. Their absence from the regulation represents one of the major questions marks over the Commission's regulatory approach to AI.

The distinction in Recital 38 is incoherent with the risk-based approach advertised by the Commission. It follows from a literal reading of that provision that predictive policing models used to detect minor non-violent crimes would be qualified as higher risk systems in comparison to predictive models used to detect administrative offences that may result in million euros debt for individuals. Accordingly, this Recital and the distinction for systems used solely for administrative purposes call into question the risk-based approach as a whole. Despite the central importance of the approach in the instrument, it does not seem to follow a clear methodology to qualify systems within categories of risks. In the interests of harmonization, the Commission should disclose its methodology and not leave the interpretation of crucial concepts of the instrument to national law. The case study of AI tax systems perfectly illustrates the result of the lack of transparent methodology for their risk-analyses: arbitrariness and a Regulation that will fragment and erode citizens' fundamental rights. Recital 38 represents a rupture with the function-based and sector-based approach espoused by the Commission in the rest of the instrument. Yet, divorcing from the approach initially espoused comes at the price of simplicity, coherence, and effective protection for taxpayers' rights. A simpler, more effective, and coherent approach would be to persist with this initial methodology and assess the types of systems which may present a risk for citizens' rights in other sectors. Articles 7 and 73 of the AI Act prescribes the possibility for the Commission to do exactly that. It may perhaps arrive sooner than later, given some of the sectors and functions that are inexplicably absent from the instrument, fiscal governance algorithms being one of those.