

Beyond the Scope: AI, Tax Administrations, and the Limits of the EU AI Act

Arthur Bianco

Abstract: The integration of artificial intelligence (AI) into public administration has accelerated rapidly in recent years, with tax administrations across the European Union increasingly adopting AI systems to enhance compliance, streamline operations, and improve services to taxpayers. Despite the growing reliance on AI in this context, the regulatory framework designed to govern such technologies—namely, the AI Act—offers limited protections for individuals affected by their use in tax systems. This article critically assesses the AI Act’s scope, its risk-based classification approach, and the consequences of excluding tax-related AI systems from its most stringent safeguards. The analysis situates these regulatory omissions within the broader legal and institutional structures of the EU, questioning the adequacy of the Act in protecting taxpayers’ rights and maintaining trust in automated decision-making.

1. The use of AI by tax administrations: an undeniable reality

Tax administrations in the EU, similarly to most European public administrations, have in the recent year adopted, at a particularly rapid pace, Artificial Intelligence systems to facilitate their work and improve on their capacities. In general, across all States, the vast majority have reported using these tools to some extent in their functioning.¹

Reliance on AI systems can be, broadly, categorized in three major sections: the use for traditional compliance management, the improvement of taxpayer-facing services and reliance for policy-making purposes.

Compliance management focuses, in taxation, on the methods used by the tax administration to compel taxpayers in fulfilling their tax obligations, which beyond the payment of their tax debt also includes other duties such as declaratory obligations or communication duties.² A number of tax administrations have introduced systems related, on the one hand, to fraud detection, in order to determine which taxpayers are likely to be non-com-

1 OECD, *Global Survey on Digitalization in Tax Administration* (OECD Publishing 2021).

2 Jeffrey Owens, ‘Taxpayers’ Rights and Obligations’ (1990) 18 Intertax 554.

pliant³, as well as audit selection systems, which aim at establishing the best strategy to adopt in facilitating the recovery of due taxes.⁴

The role of the tax administration is not, in itself, limited to the straightforward recovery of due taxes. It also communicates with taxpayers and offers specific services targeted at facilitating their compliance. For example, the tax administration must remain available for any inquiries from the taxpayers through different channels including in-person appointments, telephone or on the internet. Tax administrations have harnessed the power of AI systems to provide support for taxpayers by implementing chatbots or artificial assistants⁵, but also in improving communication strategies.⁶

Finally, AI systems have also been used to facilitate the work of policy-makers, mostly by providing additional ways for tax administrations to assess policy projects, including a number of sandbox-based systems to work out issues with these experiments.⁷

Literature and operational reports have underlined the advantages of the use of AI systems in taxation, including the ability for the administrations to reallocate resources towards other tasks, recover additional taxes and respond to additional pressures from increased demands in regards to the fight against tax evasion and avoidance. Nevertheless, a number of difficulties and risks with the use of AI systems in tax administrations have been identified. On the one hand, the technologies themselves have raised concerns, mostly related to biases and discriminations, transparency

3 For example, Slovakia has introduced a VAT fraud detection system comparing declared information with company invoices. See IOTA, *Data-Driven Tax Administration* (IOTA 2016) 16.

4 For example, Ireland has been using regression analytics to compare taxpayer returns with that of his peers to determine if they should be investigated. OECD, *Advanced Analytics for Better Tax Administration: Putting Data to Work* (OECD Publishing 2016) 23.

5 Spain uses a AI-powered VAT assistant named Skatti with positive success rates for resolution. IOTA, 'Applying New Technologies and Digital Solutions in Tax Compliance' (Conference Report, IOTA Annual International Conference – Tax Compliance Technology Showroom, 2020) 47.

6 For example, the Czech tax authorities has introduced a tax portal which includes an automated messaging techniques related to the taxpayer's due date for the fulfilling of their tax obligations and tax liabilities. OECD, *Tax Administration 2022* (OECD Publishing 2022) 78.

7 Spain, for example, uses a policy visualization tool allowing for the presentation of relevant data and insight on newly introduced policies. CIAT, *Manual sobre Gestión de Riesgos de Incumplimiento para administraciones tributarias* (CIAT 2020) 106.

or the position of the human agent within the decision process.⁸ On the other hand, the adoption of those tools within public administrations has also highlighted issues, such as the difficulty to ensure equality and fair treatment, enhance trust in the system and adequately allocate limited resources.⁹ Additionally, the disparate approach to legislative actions by different States, including the lack of specific regulations for the use of AI systems (or technology in general) in taxation, have shown flaws in the protection of taxpayers in cases where AI tools may threaten their rights.

The prior shows both the positive aspects, but also the negative, of the reliance on AI tools in tax administrations and justifies a deeper analysis of the existing legal framework in relation to the protections available to taxpayers in regards to these uses. Therefore, it seems relevant to discuss the EU's action in regards to adoption of AI systems by both private and public actors. The AI Act is the Union's response to a number of concerns identified in relation to this use of AI tools, and thus one may wonder how the introduction of such a regulation may affect tax administrations.

2. The AI Act: Functioning and Justifications

An appreciation of the EU's response to the growing concerns linked to the use of AI both within public administrations and the European Union in general would not be complete without an assessment of its main foray into regulating the use of AI systems in the internal market: the AI Act.¹⁰ Indeed, the following section will not only present this legislation but also critically discuss how it impacts – or not – the use of AI tools by tax administrations. The aim of this section is to consider what protections are accessible to taxpayers, but also outline both what remains outside the scope of the legislation and the potential missed opportunities for the EU legislator to extend protections to taxpayers.

8 Fernando Serrano Antón, 'Artificial Intelligence and Tax Administration: Strategy, Applications and Implications, with Special Reference to the Tax Inspection Procedure' (2021) 13(4) *World Tax Journal* 575.

9 María Amparo Grau Ruiz, 'Fiscal Transformations Due to AI and Robotization: Where Do Recent Changes in Tax Administrations, Procedures and Legal Systems Lead Us?' (2022) 19(4) *Northwestern Journal of Technology and Intellectual Property* 325.

10 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L/1689 (AI Act).

2.1. What is the AI Act and what are its purposes?

The AI Act is a regulation drafted by the European Commission which aims at regulating the use of Artificial Intelligence systems, or as defined by the regulation, within the European Union and its market. Indeed, the AI Act provides for a uniform legal framework for the development, the placing on the market and the putting into service of artificial intelligence systems in the Union.¹¹ The regulation was initially conceptualized and justified primarily by the need to regulate the use of these systems at European level rather than leaving it up to the Member States. The risk, potentially, would be that Member States may try to introduce their own legislation to regulate the use of AI, leading to discrepancies and asymmetries in the rules and protections established by those.

Before delving deeper into the actual functioning of the framework established by the Act, one should note that the European Legislator, in drafting the Act, included the protection of health, safety and fundamental rights as one of the main purposes of the legislation.¹² Similarly, the recitals of the Act also emphasize the fact that the regulation was drafted with a market orientation in mind.¹³ Indeed, the European legislator states that the Act provides grounds for the Union fundamental freedoms enshrined in the Treaties, namely the protection of the freedom of movement of AI-based goods and services across the Union, to be ensured throughout these recent technological evolutions.

Therefore, this piece of legislation should be seen as a multifaceted attempt at regulating a complex area all the while ensuring that the rules and protections found therein are sufficiently comprehensive as well as future-proof to apply to a large array of technologies anticipating unforeseen potential uses characteristic of the development of a recently introduced new technological advancement.¹⁴ Thus, in analysing the AI Act, one should nonetheless consider these potential difficulties faced by the European legislator when drafting the legislation, including in cases where the Act lacks finesse or details.

11 AI Act, recital 1.

12 AI Act, recital 1.

13 AI Act, recital 8.

14 Atte Ojanen, 'Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act' (2025) 16 *European Journal of Risk Regulation* 1440.

2.2. How does the AI Act achieve those aims, and why does it choose to do so?

The most notable characteristic about the legal framework established by the Act is its risk-focused approach: The Act imposes more or less obligations on AI providers depending on the significance of the risk linked to the use of AI in certain circumstances. The Act establishes a scale of risk, that covers AI systems that pose an ‘unacceptable risk’ down to AI systems with ‘minimal-to-no risk’. Each risk category includes rules that the European legislator considered to adequately pursue the aims of the directive (namely the protection of health, safety and fundamental rights) in relation to those risks¹⁵.

This risk approach was adopted as a way to minimize unnecessary limitations to the introduction of AI systems on the European market and to focus the obligations implemented by the Act to use cases that needed them the most. According to the recitals, the European Legislator intended to focus stricter rules on AI systems that create the most significant risk.

The risk scale adopted by the Commission is separated in four categories of risks, which, in order of gravity, scale down from ‘unacceptable risk’ AI systems, following by ‘high-risk’ systems, and ‘limited-risk’ systems to finally end with ‘minimal-to-no risk’ systems. Each risk category is tied to different rules or requirements in the Act, which will be overviewed in the following. The first category focuses on AI systems presenting an ‘unacceptable risk’ and are therefore entirely banned from entering the EU market, according to article 5. This category includes cognitive behavioural manipulation of vulnerable people or to circumvent individuals’ free wills, social scoring based on social behaviour or personal characteristics, biometric identification and categorization of persons and real-time identification systems, with some exceptions for law enforcement purposes.

According to article 6, high-risk AI systems are themselves separated into two categories. The first are AI systems that are safety components or the AI system being a product itself covered by a legislation listed in Annex I, or are safety components of products that are required to undergo a third-party assessment according to EU legislations listed in Annex I is comprised of a list of Union harmonization legislation (which covers medical equipment, toys and aviation...), one part based on the New Legislative Framework and the second listing other harmonization legislations. The second paragraph

15 AI Act, recital 7.

or article 6 also extends the category to systems that are used as a safety protocol to a product covered by the legislations listed in Annex II if they require third-party conformity assessment or is put into service of that product. The second category of high-risk AI systems are called 'standalone high-risk systems', which, according to article 6(2), are AI systems that fall in one of the classifications in Annex III. This annex includes eight areas in which are listed types of AI systems that should be considered high-risk, even if they do not fall within one of the legislations listed in Annex II. The eight areas covered by Annex III are: (1) Biometrics, (2) Critical infrastructure, (3) Education and vocational training, (4) Employment workers management and access to self-employment, (5) Access to and enjoyment of essential private services and essential public services and benefits, (6) Law enforcement, (7) Migration, asylum and border control management, (8) Administration of justice and democratic processes. Only the AI systems that fall within one of the specific categories within those areas shall be considered high-risk. One should note that article 7 gives the possibility for the Commission to expand the list of standalone high-risk AI systems.

It should be noted that most of the requirements found in the Act focus on high-risk systems only. Indeed, Chapter 2 and 3, articles 8 to 49, list requirements and obligations to which high-risk systems and their providers or users are subject to. These requirements cover a broad array of obligations that aim at ensuring that these systems do not negatively affect the health, safety or fundamental rights of individuals. These requirements, include, among others, the obligation to introduce a risk management system, the introduction of data governance rules, the writing of technical documentation, the respect of transparency obligations or the inclusion of human agents in the process. This chapter also deals with the notification procedure for the conformity assessment referred to in article 19, and provides for additional rules regarding that also apply to high-risk systems regarding applicable standards, conformity assessments, certifications and registration.

Article 50 imposes transparency obligations for certain AI systems that represent a limited risk, and are therefore neither banned under article 5, the unacceptable risk, or considered high-risk. This category covers AI systems that interact with natural persons, and aim at ensuring that they are developed in a way that ensures that these persons are aware that they

are dealing with an AI system.¹⁶ Similarly, users of biometric categorization, except if used for law enforcement purposes, shall inform natural persons affected of the use of such systems.

Before its official adoption, the text of the AI Act went through several changes, the more relevant one being the addition of a chapter on General-Purpose AI ('GPAI') Models, Chapter 5. Following the recent technological developments, the EU legislator focused on amending the initial proposal of the Act to include safeguards in cases of use of GPAI systems. The Act currently provides for obligations in two categories, those that apply horizontally to all GPAI and those that only apply to GPAI systems that present a 'systemic risk'. Horizontal obligations are mostly summed up to transparency rules covering technical documentations and content on which the system was trained. As for systems that present a systemic risk, they will be subject to stricter rules, including the conducting of system evaluation to potentially respond to specific risks and the reporting to the Commission on certain incidents, among others.¹⁷

Lastly, AI systems that do not fit in any of the above categories are considered to present a minimal-to-no risk, and are not bound by any obligations. Nonetheless, the following of voluntary Codes of Conduct with similar guidelines that those included in the high-risk system requirements, by the AI providers or users, is encouraged.¹⁸

3. Effects of the AI Act on the use of AI systems in tax administrations

In the context of the use of AI systems in Tax Administrations, the relevance of the Act is easy to understand, and one can therefore wonder how the introduction of such a legislation in the European Union might impact those uses, especially in considering the issues introduced in the previous part. Considering the risk-based approach adopted by the European legislator in the Act, one should determine how tax fits within the tiers established in the legislation, which will then lead to the specific obligations that tax administration will potentially be subject to.

16 AI Act, recital 132.

17 AI Act, art 55.

18 AI Act, art 95.

3.1. Unacceptable risks systems

In regards to unacceptable risk systems, AI systems used by the tax authorities are very unlikely to fall within this category, which would otherwise completely ban them. No AI use that has been made public so far have fit in any of the specified categories that have been flagged as unacceptable. Nevertheless, should a use find itself in that classification, it would most likely be caught by domestic administrative law protecting citizens against authoritative administration (for example, should a system exploit vulnerabilities of specific populations or try to manipulate human behaviour to circumvent free will). However, depending on how the use of such systems evolves within tax authorities, AI systems may prove to be problematic in this regard.

Indeed, the use of AI tools for social scoring by public authorities based on social behaviour or personal characteristics is strictly banned by the Act. According to the Recital of the Act, social scoring corresponds to ‘evaluat(ing) or classify(ing) the trustworthiness of natural persons based on their social behaviour in multiple contexts or known or predicted personal or personality characteristics.’¹⁹. Although the reference to ‘social behaviour’ and ‘personality characteristics’ seem to fall outside of what would be traditionally seen as relevant for tax authorities, one could imagine how the examination of a taxpayer’s behaviour could be significant to the mission of the administration. For example, should a taxpayer’s lifestyle broadly differ from their declared income, the tax administration could be inclined to pursue a more diligent investigation in their affairs to determine if the taxpayer is potentially not being compliant. One could thus easily imagine the development of an AI tool that considers such traits to determine the likeliness of non-compliance. The Commission has published guidelines on prohibited artificial intelligence practices under the AI Act.²⁰ In it, the Commission states specifically that: ‘The ‘social scoring’ prohibition has a broad scope of application in both public and private contexts and is not limited to a specific sector or field.’. However, the main questions reside in the assessment of social behaviours or personality characteristics. According to the Commission guidelines, these are broad, and include, among others, income, address, level of debt and even the type of cars. Ad-

19 AI Act, recital 17.

20 European Commission, ‘Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689’ C(2025) 5052 final.

ditionally, these characteristics and behaviours have to lead to a detrimental or unfavourable treatment, which the Commission highlights does not have to be solely driven by the assessment of behaviours and characteristics. However, the AI output must ‘must play a sufficiently important role in producing the social score.’²¹ Additionally, the data used to determine the social score must be used either in a social context unrelated to the context for which the data was originally collected, or disproportionate to the social behaviour or its gravity. This is particularly interesting for the tax context, as tax administrations usually collect a large amount of data, but also receive data either from other public administrations within the State, or also from other tax administrations of other Member States. This means that, potentially, tax administrations may feed into an AI system, data on which taxpayers could be scored (for example, as to determine if they are likely or not to fraud or deviate from their obligations), without that data necessarily being obtained at first for that specific purpose. The Commission also highlights that unfavourable treatments may extend to cases ‘of scoring practices where people are singled out for additional inspections in case of fraud suspicious’²². This means that AI systems specifically made to profile and flag individuals that may potentially fraud, or the best candidates for audits could be covered. Among the examples of prohibited systems provided by the guidelines of the Commission, one may find certain likely scenarios relevant for tax administration: ‘National tax authorities use an AI predictive tool on all taxpayers’ tax returns in a country to select tax returns for closer inspection. The AI tool uses relevant variables, such as yearly income, assets (real estate property, cars etc.), data on family members of beneficiaries, but also unrelated data, such as taxpayers’ social habits or internet connections, to single out specific individuals for inspections.’ It should be noted, however, that article 5 specifically prohibits the social scoring of natural persons. Taxation targets a diversified population, which includes both natural persons but also legal persons, that, according to article 5(1)(c), would not fall within the scope of the protection. This further complexify the question of the use by tax administration of scoring systems.

21 *ibid* [161].

22 *ibid* [165].

3.2. High Risks AI

Due to the importance given to those systems in regards to the number of safeguards and obligations found in the AI Act, it is evident that one should determine if AI systems used by the Tax Administrations fall within this category. As noted earlier, an AI tool is considered high-risk either because it is a safety component or a product subject to existing safety standards under EU law, or it falls in one of the class of systems listed in Annex III of the Act. Since AI tools employed by tax authorities would not be included in the first category of high-risk AI, one should determine if AI uses by tax authorities could fall in the latter classification.

Among the categories listed in Annex III, none of them specifically reflects the uses of AI tools currently used by tax administration within the EU. Indeed, while several categories refer to the use of AI systems by administrative bodies, none of them specifically include tax authorities. Paragraph 5 of Annex III states that certain AI employed in the sector of 'Access to and enjoyment of essential private services and essential public services and benefits', shall be considered high-risk. Furthermore, paragraph 5(a) classifies as high-risks systems tools that 'AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services'. However, this category of systems is relevant only if the tax authorities are also tasked with providing assessment for the distribution of such benefits and services. This would also fall outside the framework of research of this chapter. Beyond this category, no other uses described in paragraph 5 seem to fit the definition of a system potentially used by the tax administration.

Paragraph 6 of Annex III focuses on AI uses by law enforcement, and lists a number of AI uses that would lead to those systems being considered high-risk. If at first glance this category seems to fall outside of the type of systems used by tax authorities, this is further confirmed by the Recitals. Indeed, the legislator states explicitly that 'AI systems specifically intended to be used for administrative proceedings by tax and customs authorities as well as by financial intelligence units carrying out administrative tasks analysing information pursuant to Union anti-money laundering legislation should not be considered high-risk AI systems used by law enforcement

authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences.’²³

This means that the AI tools employed or potentially employed by tax administrations in the EU are unlikely to ever be considered as high-risk by the AI Act, so long as the categories of Annex III remain the same. This also excludes tax administrations using such tools from being subject to a majority of the rules found in the Act.

This conclusion is particularly surprising in taking into account that the Act alternatively defines high-risk systems covered by the legislation as ‘*hav(ing) a significant harmful impact on the health, safety and fundamental rights of persons in the Union*’.²⁴ Considering the issues outlined in earlier part of this chapter, one would be remiss to exclude AI tools used by tax administrations from the category of AI systems potentially having a significant harmful impact on fundamental rights.²⁵ The discrepancy between this definition and the categorization of high-risk systems in Art. 6 of the Act has been outlined as a major concern. Indeed, it seems that the decision to limit high-risk tools to either product or safety components or the list in Annex III does not allow for the inclusion of all tools that could potentially pose significant issues and harm, and leaves out a large number of problematic uses. This is especially concerning since the vast majority of the safeguards and obligations found in the Act concern only high-risk AI systems. This in turns means that a number of systems, including those employed by the tax authorities, are not subject to the guarantees provided, in spite of the potential harm or risk that they present. One may note that Art. 7(1) provides for the possibility for the Commission to amend Annex III to add other systems to the list, further expanding the category of high-risk AI tools. Nevertheless, this amendment is limited by the fact that such system should already fall within one of the areas listen in points 1 to 8 of Annex III. It should be noted that before the adoption of the AI Act, article 7(1)(b), has been added, which state that an AI system could also be qualified as a High-Risk system if: ‘*the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse*

23 AI Act, recital 38.

24 AI Act, recital 27.

25 David Hadwick, ‘Slipping Through the Cracks, the Carve-Outs for AI Tax Enforcement Systems in the EU AI Act’ (2024) 9(3) European Papers 936.

*impact posed by the high-risk AI systems already referred to in Annex III.*²⁶ This addition is particularly interesting, as limiting the amendment to areas already covered by Annex III would have severely limited the ability for the AI Act to be properly technology-proof, especially with the swiftness with which AI systems are being introduced in certain areas. Nonetheless, this possibility is limited by article 7(1)(a) which limits the application of those changes solely to the areas already covered by the Annex. This, in turn, restricts these changes to predetermined uses of AI systems, which seems to exclude most technologies used in tax administrations, as evidenced earlier. Ebers also questions the lack of details as to the risk-assessment and classification carried out in the drafting of the Act in order to establish the list in Annex III, and states that the solution provided by article 7 is insufficient in ensuring the flexibility and adaptability needed in the context of a technology-driven legislation.²⁷

It is possible that the choice of the Commission to limit the definition of high-risk systems to either systems that are a safety component or a product already covered by a European legislation, or to the systems comprised in one of the areas listed in Annex III comes from the fact that the European Council, during the drafting of the initial proposal, emphasized the need to provide a clear definition of high-risk AI.²⁸ Therefore, the Commission may have consciously moved away from a wide-applying definition that may create uncertainty in favour of a more limited definition. This may also be justified by the need to limit legal uncertainty for EU actors that would otherwise need to deal with an added layer of complexity if the definition of high-risk AI systems were to be changed.²⁹ However, the opposite can be argued as well, seeing as the lack of safeguards for taxpayers (and

26 AI Act, art 7(1)(b).

27 Matthias Ebers and others, 'The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)' (2021) 4(4) J 589, 593. Ebers here states that the amendment procedure for Annex III should allow for the addition of entirely new categories of systems, and not just specific uses inside pre-defined categories. Ebers also underlines the need to include ongoing research (and public consultation) in the amendment procedure to ensure that the risk assessment is based on significant and actual risks.

28 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts' COM (2021) 206 final, 2 and 8.

29 This has been confirmed by the Commission in its Staff Working Document. European Commission, 'Commission Staff Working Document, Impact Assessment Accompanying the Proposal for AI Act' SWD (2021) 84 final, 50. However, the

individuals affected by AI uses not classified as high-risk) could lead to uncertainty as to their treatment and available remedies. While tax administration may be bound by domestic legislations in that regard, taxpayers operating on a cross-border basis would find themselves unable to predict how each Member State would handle infringement to their fundamental rights. Moreover, while the addition of new requirements could lead to legal uncertainty for private actors adopting AI tools, the same may not be said for public bodies. Indeed, even if a larger area of public administration were to be added to the list of standalone high-risk AI systems, and thus subject to more obligations, the national legislator would thus have to introduce such obligation at domestic level (as well as ensuring coordination with domestic protections), though the administrations themselves (including taxation) would not necessarily be as impacted by this additional uncertainty as private actors. Indeed, public actors are better equipped at dealing with potential legal uncertainty, especially when they themselves are at the source of administrative decisions.

In analysing the protection afforded by the Act, authors have underlined the fact that safeguards are dependent on the coverage of the list in Annex III, and should this list not be sufficiently comprehensive or up-to-date, the actual purpose of the Act would not be reached. This has been acknowledged as a difficult task, due to the evolving nature of the technology and the digital scene in the European Union.³⁰ Nevertheless, the importance of the adequacy between the list in Annex III and the systems potentially creating major harm to health, safety or fundamental rights seems paramount to the success of the Act.³¹ Authors have criticized the list-based categorization of standalone high-risk AI systems by stating that

Commission here acknowledges the fact that the current approach may limit the Act's ability to cover all potentially harmful systems.

30 Nathalie Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (LEADS Lab, University of Birmingham 2021) 13.

31 The Commission, in its Staff Working Document, has emphasized this by stating that the main objective of the legislation is to ensure that AI systems are 'safe and respect the existing law on fundamental rights'. Similarly, the Commission also pointed out that currently national and European authorities do not have sufficient power or resources to effectively ensure and monitor compliance with those requirements. This shows that protection of fundamental rights is paramount to the goals pursued by the Commission, and therefore the disparities in applications of requirements may limit the ability for the Act to ensure protection of fundamental rights. See European Commission (n 29).

the narrowly defined classification ‘fails to capture the nuanced reality of the way AI systems are used – and have an impact on fundamental rights’.³² This pushes potentially high-risk systems in the no risk category and limit the ability for the Act to effectively provide fundamental rights protection. Literature further indicates that while the prescriptive list-based approach might be intended to secure legal certainty, it might have the opposite effect in leaving major areas in the shadows.³³ Mahler also criticizes the risk assessment approach adopted by the legislation by underlining the fact that the Commission, in drafting the Act, claims to have used a quantitative risk-analysis to determine which systems should be qualified as high-risk when it most likely also took into account political and societal aspects that are hardly quantifiable. For that reason, it should also be noted that the risk-assessment carried out is necessarily thus context dependent and may vary according to the actor performing the assessment.³⁴ This may further provide explanation as to why AI systems employed by tax administrations may not have been considered as presenting sufficient risk to be included in that category. As tax remains a largely sovereign area of action, it is possible that the Commission underestimated the potential risk these used may cause. This argument could nevertheless be nuanced by the fact that VAT, for example, is a harmonized area and therefore gives the Commission sufficient knowledge of the relationship between taxpayers and fundamental rights protection for it to be able to determine exactly which risks may arise from the introduction of AI tools in this field.³⁵

Stuurman and Lachaud explain the choice of the Commission in delimiting the categories of high-risk AI by the fact that the Act focuses not on the actual functioning of the system, but on the purpose intended by the use of the system.³⁶

32 Smuha and others (n 30) 13.

33 Smuha and others (n 30). Smuha also argues in favour of a more extended risk-based approach rather than the sectorial one adopted by the Act, and underlines the solution used by the GDPR in allowing for the criteria used to cover most realities that would create risks.

34 Tobias Mahler, ‘Between Risk Management and Proportionality: The Risk-Based Approach in the EU’s Artificial Intelligence Act Proposal’ in *Nordic Yearbook of Law and Informatics 2020–2021* (2021) 267.

35 This is further comforted by the fact that the ECJ has rules in several instances on the issue of fundamental rights in regards to taxpayers, allowing the Commission to assess more easily how the adoption of AI tools may affect them.

36 Kees Stuurman and Eric Lachaud, ‘Regulating AI: A Label to Complete the Proposed Act on Artificial Intelligence’ (2022) 44 *Computer Law and Security Review* 105657, 3.

Additionally, the Commission has stated that it has elected to adopt a risk tier system for the Act following an in-depth evaluation of societal and economic impact of each policy option considered for the development of the legislation. This included, as underlined by the Commission itself, a focus on the potential impact of the policy on fundamental rights.³⁷ This is further proof of the significance placed on the risks of detriment to fundamental rights that AI systems could cause. If so, in approaching the question of high-risk AI systems, that is to say which systems should require further scrutiny from the EU legislator, this focus on fundamental rights should be considered. It is thus even more surprising that the Commission then opted to limit the category of standalone high-risk AI systems to the areas found in Annex III.

Indeed, seeing as the Commission opted to leave the enforcement of the AI Act requirements to national authorities, it could potentially have been more relevant for the purpose pursued by the Commission to also give the opportunity for such authorities to determine which AI systems should be considered as high-risk, also depending on the specific AI uses in each Member States. In that case, it could have been feasible for the Act to impose distinction between low and high-risk AI on the basis of their potential impact on health, safety or fundamental rights rather than adopting a sectorial approach.

Another issue in relation to the AI Act's treatment of tax administration systems is the lack of definition of the individuals affected by the use of those tools.³⁸ Indeed, it seems that the Act may associate this status as being users of the AI tool, although there are many situations where this is not the case. This is particularly relevant to the area of taxation, as most affected by the use of AI tools, that is to say the taxpayers, are distinct from the user, the administration. This could also inform the reasons behind the exclusion of tax systems from the high-risk tier, as the potential negative effects to fundamental rights, health and safe do not affect the user per se, usually the tax administrations, but a third party, the taxpayers, who is subject to the decisions made using the AI system. This may have impacted the risk-assessment carried out by the Commission in determining what system should be considered high-risk. It could be preferential for the Act to also consider the subjects for an AI system use, as it seems to have played

37 AI Act Proposal (n 28), 9.

38 Anna Kiseleva, 'Comments on the EU Proposal for the Artificial Intelligence Act' (SSRN, 2021) 1.

a role in determining which systems should be high risk. For example, law enforcement systems covered are mostly comprised of tools that have natural persons as their subject. This is particularly interesting in regards to taxation as the subjects of most AI uses are a broad and diverse category. AI systems in tax administrations could apply to both natural and legal persons, indiscriminately, which of course changes greatly the impact of such tools on fundamental rights. In the same vein, the diversity, even within natural individuals, could lead to complexity as to the Commission's ability to properly assess the fundamental rights effect of AI systems.

Interestingly enough, the inclusion of law enforcement AI tools in the high-risk category due to the possibility for 'over-policing' in case feedback looks exacerbates already existing discriminatory practices. One example is the SyRI case³⁹, where an AI system was used by the Dutch tax administration to detect welfare frauds, and led to indirect discrimination due to the criteria that were chosen for their risk-assessment.⁴⁰ The justification used for law enforcement tools could also very easily apply to tax administrations, especially in the context of tax fraud detection or audit selection. Although the Recitals of the Act explicitly excludes tax AI tools from the law enforcement category, it does not provide any justification for such exclusion. In taking into account the definition provided by the Act of high-risk AI systems (posing significant risk of harm, including to fundamental rights), this exclusion does not, once again, seem justified by such concern. The question of the reasoning behind the decision of the Commission thus remains.

Interestingly enough, the Commission justifies the exclusion of AI systems used by tax administrations from the high-risk category by saying that these are already sufficiently covered by existing legislation and that there is no evidence of significant potential harm. The Commission, however, does not reject the possibility for these areas to be reintroduced in the category by future amendments to the Annex.⁴¹ These claims are particularly surprising, as these do not align with the current conclusions established in the context of this research.

Firstly, it would be hardly right to say that current legislation covers the area of taxation sufficiently to ensure that taxpayers are effectively protected

39 Adamantia Rachovitsa and Nora Johann, 'The Human Rights Implications of the Use of AI in the Digital Welfare State: Lessons Learned from the Dutch SyRI Case' (2022) 22 Human Rights Law Review 1.

40 Smuha (n 30) 33.

41 European Commission (n 29) 51.

in cases of AI uses. Indeed, beyond the requirements set by the AI Act (which has not yet been adopted, and may not even cover taxation), both primary and secondary EU legislation seems particularly lacking, due to the EU's lack of competence in direct taxation (which further justifies the need for this research). The Commission may refer to VAT, which is indeed harmonized, but does not necessarily include specific protections for taxpayers. In case the Commission here refers to domestic legislation, which, depending on the Member State, does indeed provide protection for taxpayers, but should not be the basis for the exclusion of taxation AI systems from the class of high-risk AI systems, as discussed earlier in the research: disparate and different level of protections in the EU may lead to severe limitations as to the freedom of movements of taxpayers.

Secondly, the Commission claims that no evidence of potential risks has been identified in the area of AI us in taxation. This assertion is difficult to contradict as the Commission has not made its risk-assessment practices public, and therefore it is difficult to establish which harms would constitute sufficient concern to be classified as 'high-risk'. Nevertheless, the relationship between high-risk systems and potential harm to fundamental rights could inform this assessment. As established earlier in this research, fundamental rights are currently and will be impacted by the use of such systems, and it is therefore doubtful that these uses show no evidence of potential harm.

Finally, the Commission asserts that should additional risks be unearthed in the area of taxation, Annex III could be amended for such systems to be included in the high-risk category. Once again, this claim seems dubious. As discussed earlier, the amendment procedure only empowers the Commission to add specific AI uses in the Annex should these uses fall within one of the eight predetermined categories, none of which seem to encompass taxation.

The treatment of AI systems used by tax administrations by the AI Act also raises several issues in relation to the use of such systems specifically in public administrations. Fink discusses the specificities of the risk presented by such systems when used by public authorities, and argues that these deserved accrued scrutiny from the European legislator when discussing the Proposal. Specifically, the use of AI tools in the decision-making process may require additional safeguards, which, for the time being, seem not to be the case for taxation. Indeed, in the absence of a high-risk system, the only transparency requirement is that under article 52 triggering if an AI

system is used directly with a natural person. This, as discussed earlier, does not extend to decision-making involving such tools. Fink identifies two distinct issues that have not been properly addressed by the Act: transparency and automation bias.⁴² One could imagine the AI Act inserting such specific obligation specifically in all cases of uses of AI system by public bodies, separate from the existing requirements. This would also be in line with the philosophy adopted by the Commission in limiting obligations only to situations that pose sufficient risk. Furthermore, Fink also examines the issue of the potential lack of available remedies for individuals affected by AI-driven administrative decisions, which, has not entirely been addressed by the Act either. Indeed, the Proposal lacks a specific individual procedure in those cases⁴³, which would therefore be left up to national administrative rules and courts, further exacerbating the aforementioned discrepancies in protections available to taxpayers.

While the Commission expressly refers to the protection of fundamental rights against potential infringements by AI systems as one of the main goals pursued by the Regulation, concerns over the effectiveness of the rules laid out by the Commissions in reaching this goal have been raised by several authors. The Act lacks effective protection due to the market-specific approach adopted by the Commission. Indeed, the focus granted to the preservation of innovation within the EU market may have discouraged the Commission from taking a more radical approach to the protection of fundamental rights. Moreover, the Regulation very explicitly balance these market interest with the protection of fundamental rights, which severely limits the Regulation's ability to ensure the latter. Authors have indeed criticized the fact that the interests of individuals affected by AI usage are given the same weight as that of other actors, included AI developers and providers. This results in a number of issues leading to a weakened fundamental rights protection.⁴⁴

3.3. Low-Risk AI systems

Beyond the first two categories outlined before, AI systems used by tax authorities would therefore be considered low-risk according to the frame-

42 Melanie Fink, 'The EU Artificial Intelligence Act and Access to Justice' (EU Law Live, 2021) 2.

43 *ibid* 3.

44 Smuha (n 30) 16.

work set by the Act. In that case, the number of guarantees or safeguards applicable to them is highly limited.

As far as this research goes, there has been no use of General-Purpose AI use made public in any tax administration within, or outside of the European Union. This could be due to the very recent development of such technologies, or from the highly-specialized needs of tax administrations which lend themselves poorly to the use of GPAI. Nevertheless, this means that the rules introduced to better safeguard natural persons against harmful uses of GPAI do not concern this research.

Art. 50 of the Act does provide for additional transparency obligations for certain AI systems, depending on their purpose. While paragraphs 2, 2a and 3 concern respectively biometric categorization, emotion recognition and image, audio or video content manipulation, paragraph 1 of Art. 50 focuses on AI tools developed to interact with natural persons. This is relevant for tax administrations as AI-driven chatbots and digital assistants have been made available by several tax authorities. Art. 50(1) thus imposes the obligation for those providers to ensure that the natural persons are aware of the fact that they are interacting with an AI system. This may be paramount to tax authorities as the communications means between taxpayers and authorities have been rapidly evolving towards an AI-centric support to taxpayer rather than a human-to-human system.⁴⁵ One could however wonder if such transparency obligations could be extended to other cases beyond those specific cases: for example, in the context of the tax administration, could it be also preferable to impose a transparency obligation when a natural person is affected by a decision taken on the basis of an AI system? Depending on the risk targeted by those transparency requirements, it could also be beneficial to consider those other situations. Furthermore, authors have raised the issue of the content of the information to be provided to natural person affected by an AI system, as this has not been specified in the Act, and runs the risk of varying among providers.⁴⁶ This could mean that different providers would provide different information to individuals, depending on the transparency assessment of each system.

45 It should be noted that this category of AI tools lacks specific risk definition. The Commission in the draft seems to imply that as soon as an AI system interacts directly with a natural person, it presents an inherent risk that should be minimized (through additional transparency requirement), but there is no clear description of the actual potential harm these could pose. See Mahler (n 34) 249.

46 Stuurman and Lachaud (n 36) 5.

The Act only suggests that minimal-to-no risk AI system providers and users follow a Code of Conduct (and potentially holding themselves to the same standards as those imposed on high-risk systems) though this seems of limited impact. Indeed, while the costs of complying with the requirements found in the Act seem particularly high⁴⁷, which will most likely drive non-high-risk AI providers away from following these codes of conducts, these rules could add another layer of complexity that AI providers are unlikely to choose to follow by themselves. This is interesting as the Commission has underlined, in its justification for the Proposal, that voluntary self-regulation is unlikely to sufficiently ensure protection of fundamental rights and safety within the Union. While the Act provides regulation in regards to high-risk systems, the Commission must have known that simply suggesting the following of codes of conduct would not be sufficient in the context of low-risk systems. Therefore, even according to the logic of the Commission, the Act does not extend any regulation to low-risk systems.

Apart from the obligations outlined in the previous paragraph, AI tools employed by the tax administrations seem to pose, according to the tiered approach of the AI Act, no to minimal risk and therefore warrant little to no safeguard.⁴⁸

Beyond the issues related to the determination of high-risk AI systems and exclusion of potentially harmful systems, the difference between the requirements imposed on high-risk systems and those (or lack thereof) for low-risk systems is particularly jarring.⁴⁹ Indeed, the Commission only suggest the following of a Code of Conduct for providers and users of low-risk AI tools, while high-risk ones are subject to a number of obligations. One may wonder if the Commission could have alternatively chosen to not simply reject any requirements for low-risk systems, but more so to impose

47 See Dimitar Lilkov, 'Regulating Artificial Intelligence in the EU: A Risky Game' (2021) 20(2) *European View* 169. According to research, the costs linked to the compliance with these requirements could reach the tens of thousands of euros, which could further increase the more staff is needed to fulfil these obligations.

48 Mahler does regret the fact that the Act puts the lowest level of regulation on the widest category of AI tools. Mahler (n 34) 250.

49 It should be noted however that literature does praise the Commission for foregoing a completely binary approach to risk and does not simply differentiate between high and low risks but also adds categories of unacceptable risks and lower-risk AI still requiring transparency obligations. For example, see Smuha and others (n 30) 2. This categorization still remains very limited, especially in regards to legal obligations, the majority of which only apply to high-risk AI systems.

a more limited number of requirements to systems that present less of a risk. While this would have required to adopt a different assessment of what constituted a high-risk system in the Act, it could also have avoided the situation where AI systems that are not considered to be entirely high-risk by the Commission would still be subject to requirements, albeit limited. Similarly, this would also have necessitated to elect which obligation should apply only to the highest risk AI systems, and which would also apply to lower risk systems. While this could have potentially added a layer of complexity to the functioning of the Act (which the Commission tried to curb), it could have solved a number of issues identified here regarding the treatment of AI systems used by tax administrations in the Act.

3.4. Why are AI systems in tax administrations are excluded from protections?

The prior sections have shown that despite focusing the use of AI in the EU, in both the private and the public sphere, the AI act has a limited impact on AI systems used in tax administrations. Thus, one may not rely on this legislation to ensure taxpayer protection. Nevertheless, these limitations do raise a question: For what reasons has the European Legislator considered that the use of AI by tax authorities should not be considered a High-Risk use of AI system? Could these reasons provide insight as to the state of taxpayer protections at EU level in general?

As mentioned earlier, the Commission has justified the exclusion of the AI systems used by tax administrations from the scope of the High-Risk AI category because it was ‘considered sufficiently covered by existing legislation and there is no sufficient evidence for harms caused by AI’.⁵⁰ This justification is unfortunately not being evidenced by the Commission in its Staff Working paper, which, considering the prior section of this research, weakens its position. Interestingly, the prior could be contradicted by the European Parliament’s initial identifications of high-risk sectors, which the Commission decided not to follow entirely. Indeed, the Parliament had considered the use of AI in tax administrations to raise a number of concerns, which would have justified its inclusion in Annex III of the Act.⁵¹

50 European Commission (n 29) 5.

51 European Commission (n 29) 51.

Nonetheless, one could also explain this exclusion by examining the specificities of taxation in allowing the European legislator to regulate it. Indeed, tax remains today a special case due to the importance of the collection of revenue for the State as a sovereign prerogative. This leads Member States to be somewhat reluctant to surrender the power to legislate in the area of taxation to the European Union. The EU has already legislated in this area, and even harmonized the Value Added Tax framework among Member States; yet tax remains a controversial topic at EU level.⁵² Therefore, extending the obligations of AI providers to tax administrations may have been more politically complicated for the Commission and the European legislator to justify.

Additionally, the AI Act was adopted on the basis of article 16 of the TFEU, regarding the adoption of legislation aiming at the protection of personal data, but more importantly on the basis of article 114 TFEU, which allows for the European legislator, in accordance with the ordinary legislative procedure, to adopt legislation to approximation of laws to ensure the functioning of the internal market. The reference to the ordinary legislative procedure is interesting, as it involves both the Parliament and the Council, thus no unanimity in the Council is required (unlike the special procedure). This could have alleviated some of the tensions regarding the introduction of tax rules in the Act, as all Member States would not have to agree on the extension of the protections for tax AI. However, article 114(2) states that *'Paragraph 1 shall not apply to fiscal provisions'*. While this seems to exclude the possibility for the act to apply to AI systems in tax administration, this solution does not seem satisfactory. If the use of AI in tax is not considered High-Risk, they are still in scope of the Act in general: tax administration may employ AI techniques falling under the category of unacceptable systems, or General-Purpose AI models, and these administrations are still in scope of the article 50 transparency requirements. Therefore, either the European legislator made a mistake in relying on article 114 as a legal basis for the Act if tax administrations intended to still be in scope of the Act, or the protections found in the Act do not constitute a fiscal provision, as understood in article 114.

52 Taxation is a sensitive topic for EU Member States, as tax remains an expression of a State's sovereignty, although the EU has legislated in both indirect and direct taxation. Member States remain reluctant to give up on their sovereignty in those areas. See, for example, Tjaša Zgaga, 'The Fiscal Sovereignty of the European Union after the COVID-19 Pandemic and the War in Ukraine' (2023) 45(4) *Journal of European Integration* 703.

This question raises concerns, as the Court of Justice has, previously, stated that article 114(2) should be interpreted as prohibiting the use of the article as a legal basis ‘*not only for all areas of taxation, without drawing any distinction between the types of duties or taxes concerned, but also all aspects of taxation, whether material rules or procedural rules*’.⁵³ The Court also extends this prohibition to any arrangements of the collection of tax, as they cannot be dissociated from the system of taxation of which they form part.⁵⁴ Therefore, the use of AI systems by tax administrations, as described in the first section of this research, would most likely be considered as forming part of the taxation system, and regulating them could not be done on the basis of article 114. Additionally, reliance on article 114 TFEU as a legal basis could also exclude the use of article 7(1)(b) of the Act in order to modify the list in Annex III and add AI systems used by tax administrations in the category of High-Risk AI systems, further limiting the future prospects of application of the Act to protect taxpayers.

One should conclude that the all AI systems used by tax administrations should be excluded from the scope of the Act. The fact that this has not been clearly stated by the legislator in the text of the Act or in the recitals could indicate that this was an oversight, and may not have been a conscious overall exclusion. It is nonetheless a precarious situation, as it even excludes taxpayers from the minimum protections introduced in the Act, including the relevant prohibition of the use of unacceptable risk AI tools. As discussed in an earlier section, certain systems that rely on the social scoring of taxpayer to assess risk of fraud could fall under the definition of article 5 and Prohibited AI Practices.⁵⁵

4. Could and should the AI Act apply for tax administrations?

4.1. Future possibilities for applicability

A first possibility would be to introduce a reform to the recently adopted AI Act in order to ensure that AI systems used by tax administrations are included within the category of high-risk AI, and would then benefit from the obligations and protections that have been provided in cases of use of other AI systems. As discussed in chapter 5, Annex III of the AI Act, which lists

53 Case C-674/20 *Airbnb Ireland UC v Région de Bruxelles-Capitale* EU:C:2022:303 [27].

54 *ibid.*

55 AI Act, art 5.

the sectors in which AI usage would be considered high-risk, and currently does not include tax administrations, may have changes brought by the Commission in order to expand what can be considered high-risk. These changes are, however, impossible, as article 7(1)(a) limits those changes to the areas already covered by Annex III. As discussed, the use of AI by tax administrations does not fit in any of the predetermined categories set by the European legislator in the Annex, and an expansion to cover these systems is not an appreciable solution. Moreover, had the possibility been opened to the Commission, such changes to Annex III would not be likely, as, in the context of tax administrations, the Commission has stated that it does not find the adoption of AI systems to be creating particular risks of harm to fundamental rights. This could change, should the use of AI in taxation prove to be harmful, although cases such as the Dutch childcare allowance scandal may have evidence this fact already.

One could imagine an entire reform of the AI Act to better accommodate protections for AI in tax administrations. This is particularly unlikely, for two distinct reasons. Firstly, the political opportunity of such an amendment might be difficult to imagine, in taking into account both the recency of the adoption of the Act, but also in considering the four years that passed between the initial proposal and the adoption, which is proof of the difficulty the Member States found in reaching a consensus, especially considering that the use of AI in tax was consciously exempted from the definition of high-risks systems. However, this possibility is also limited by the legal basis on which the Act relies on: indeed, the Act was adopted on the basis of both article 16 TFEU, which focuses on the protection of personal data, and article 114, which allows for the European legislator to adopt legislation, but not in the area of taxation or fiscal policy. While article 114(1) allows for the action of the legislator according to the ordinary legislative procedure, it also states in its second paragraph that *'Paragraph 1 shall not apply to fiscal provisions, to those relating to the free movement of persons nor to those relating to the rights and interests of employed persons.'* Therefore, reliance on article 114 for any tax-related legislation is impossible. Article 114 has however been relied upon to draft several legislations that are relevant to this research, including the AI Act, mentioned in a prior chapter. This is of particular relevance in the context of this research, as underlined in chapter 5, due to the fact that the main AI regulation drafted by the EU legislator is based on an article that specifically excludes fiscal provisions from that legislation. Beyond the fact that this does show the lack of willingness from the European legislator to introduce AI rules at EU level, it is also possible

that relying on article 114 was the only path forward for the adoption of such rules. This could raise a number of questions relating to the feasibility, going forward, of the adoption by the European legislator of AI-centred rules that also include tax administrations and taxpayers. Thus, it seems unlikely that the legislator may rely on another legal basis to introduce an amendment to the Act.

Another possibility open to the legislator is the adoption of a technology-centric text, similar to the AI Act, but would cover the use of AI systems in tax administrations. This is all the more unlikely as the AI Act was drafted as a general legislation that would be the European Union's overall and unique response to the issues raised by the use of AI systems. This means that the Union may see little interest in writing additional legislation which, on top of proving difficult to pass as a consensus across Member States, could lead to overregulation and complications in ensuring that all legal frameworks function together.

4.2. Assessment of the usefulness of the protections for tax purposes

Following the previous conclusion, one may wonder if it would be preferable for the AI Act to extend applicable rules and safeguards also to AI systems used in tax administrations. Indeed, this reflects on the question of the efficiency of the Act in properly regulating the introduction of AI systems on the European market all the while guaranteeing adequate protections against potential harms posed. Before arguing in favour of an amendment of the Act to include tax administration use of AI systems, it may therefore be preferable to first determine how effective would the protections provided in the Act be in those cases. In doing so, one should compare the obligations and safeguards offered by the Act with the issues identified in relation to the adoption of AI systems by tax authorities. As outlined in the previous part, most of the relevant standards set by the Act apply solely to high-risk systems, and these are thus the rules that should be analysed here.

The second chapter of the Act focuses on requirements for High-Risk AI systems, articles 8 to 15, providing broad requirements which all systems should comply with. The aim of the requirements seems not to set up strict rules that would inherently dictate how high-risk AI systems should be developed, rather provide for general obligations focusing on allowing developers and providers to ensure themselves that their systems present

minimal risks. One of the better examples of this is article 9, which requires a high-risk AI system provider to establish a risk management system, thus all foreseeable risks should be identified, their probability of arising evaluated and potential countermeasures should be adopted in the view of eliminating or minimizing those risks. Although the phrasing of the article remains particularly vague, as the article remains silent on the nature of the risk-assessment test or how it should be carried out, probably in order to leave enough flexibility for AI providers to tailor their risk-assessment mechanisms to the specificities of their systems, it does ensure that the AI providers is tasked with the responsibility to carry out this assessment. In the same vein, article 13 imposes transparency obligations on high-risks system providers in order to secure proper information for users. While this article is slightly more precise as to the requirement imposed on the provider, including the nature of the information to be made available, it still gives providers the liberty to determine how this transparency obligation should be applied to their systems all the while requiring that specific steps be taken to ascertain that the use of the system is in line with the goals set by the Act.

For the purpose of providing adequate protection to taxpayers in cases of use of AI systems in tax administrations, the inclusion of those systems in the category of high-risk AI tools would have been preferable, as these requirements correspond to major issues outlined in literature as well as the limitations established by the Act itself (mainly related to risks linked to fundamental rights). Specifically, the adaptability of the articles aforementioned fits relatively well in the context of the discrepancies of uses and mechanisms used in tax administrations, which seems to align with the goals of the EU legislator. Furthermore, the obligations found in this chapter of the Act, while broad, may inform a more prudent approach from AI users and providers in tax administrations, decreasing potential risks linked to their uses. It is difficult to determine how much a soft law approach would impact the use of AI systems by tax administrations, however it could be considered a first step towards a uniformed approach.

Interestingly, the Commission in developing the Act emphasized the need to avoid unilateral national actions by Member States to regulate AI systems themselves, as it runs the risk of leading to market fragmentation and probably would effectively limit the movement of AI tools on the European Market. Moreover, the existence of distinct national rules could

also lead to increased compliance costs by AI system providers or users.⁵⁶ This reflects well on the issues identified in this research regarding the discrepancies that currently exist in the treatment of AI systems used by tax administrations and the need for additional safeguards for taxpayers. Indeed, by focusing on finding solutions at European level rather than leaving Member States to their own devices, one may hope that a somewhat uniform taxpayer protection would limit either compliance costs or fragmentations. Certain authors have criticized the choices made by the Commission in introducing this proposal by outlining the risks that such a legislation could still stifle innovation by leading AI providers to move outside of the European Union to jurisdiction that do not apply these rules. While this could be mitigated by nudging other countries to adopt such rules, certain authors have indicated that an alternative to a wide-ranging legislation could be to focus on specific areas of the introduction of AI systems, especially areas that may create specific issues.

Nonetheless, the obligations found in this chapter of the Act have been heavily criticized for their lack of effectiveness in relation to the goals pursued. Indeed, it seems that the broadness of the requirements also leads to a limited impact of those rules on the issues the Act is trying to fix. One of the better examples of that fact is article 14, which establishes the need for High-risk AI to function with the proper human oversight. Fully automated decision-making based on AI systems is one of the major issues which have been discussed in literature in the last few years, although the Act does very little to ensure that the human oversight it tries to implement is going to be necessarily relevant to the high-risk system it should supervise. The lack of specific definition of oversight, what constitute sufficient control or even who should be entrusted with the task, severely limits the effectiveness of the rule. Similarly, article 10 seems to try to establish a framework of data governance in the functioning of high-risk tools, although leaves major gaps as to how this data governance relates to the functioning of the AI system and what exactly is understood by the EU legislator as ‘good data governance’.

These prior conclusions paint a mixed picture of the potential performance of the AI Act as an adequate tool in facilitating the protection of taxpayers in the context of AI uses by tax administrations. The EU legislator did address several issues that impact taxpayers and have to be corrected, much seems to have been left out of the Act that significantly limits its

56 Lilkov (n 47) 169.

effectiveness. Does that mean that the exclusion of tax administration AI tools from the high-risk tier is a non-issue? Although the impact of the Act would be limited, the message sent by the European legislator that those systems present minimal-to-no risks to those affected by them is concerning. It is more than possible that these systems will, and already have had, potentially harmful consequences, although the Act does not consider them as risky.

Furthermore, if the Commission has acknowledged the fact that self-regulation is most likely insufficient to ensure that the eventual risks posed by AI systems be suppressed or limited, the current obligations imposed on AI providers and users still leave a lot up to these actors. Indeed, every rule found Chapter 2 mostly provides general instructions but entrusts providers and users with filling themselves the gaps in the requirements set by the Act. For example, if article 9 requires that a risks assessment test be carried out for high-risk systems, the nature, content and consequence of such test is left entirely up to the providers. The same can be said of the necessity to introduce human oversight in the AI process.

The exclusion of tax AI systems from the framework of obligations for high-risk systems could also present another problem. Indeed, one should consider the relationship between the introduction of a binding legal framework that commits to the protection of fundamental rights in the area of AI regulation (as well as considers the rule of law and democracy implications) with the EU goal of trustworthiness established by the HLEG.⁵⁷ Trustworthy AI can only be attained by establishing responsibilities in cases of harms caused by the systems, but also by maintaining a legal framework that effectively enforces the protection of fundamental rights and ensuring accountability and transparency.⁵⁸ In the absence of such prerequisite, trust in these systems, especially for those affected by them, is unlikely to subsist. While such ideals seem to take form in the requirements set for high-risk AI systems, the same cannot be said for systems that fall outside the category. Therefore, the lack of protection provided by the Act to taxpayer could also endanger the trust placed in the tax administration's use of AI tools, especially when those systems are used in processes leading to potentially adverse decisions, and to an extent, the tax administration itself. As discussed in the earlier chapter of this research, trust is paramount to ensure taxpayer compliance, and it is likely that that adoption of AI systems

57 Smuha (n 30) 5.

58 Smuha (n 30) 6.

in tax administration without prior introduction of safeguards may weaken taxpayer confidence in the tax system. Therefore, the current definition of high-risk AI could lead to adverse effect on taxpayer trust.

Similarly, if the Commission considers the use of AI tools in tax administration to not be high-risk, this does not necessarily mean that Member States will think of it the same way. Since the Act effectively does not regulate these uses, Member States could be inclined to unilaterally provide safeguards and protections by imposing their own requirements on AI systems used by their tax systems. This is interesting, as some may argue that Member States are better placed to determine how to provide adequate protections for taxpayers in the specific context of their own tax systems. Nonetheless, the potential disparity the introduction of unilateral legislations by each Member States could lead to negative effects on the abilities of taxpayers to seamlessly move within the internal market, as identified in the earlier parts of this research.

Specifically, the lack of risk-assessment requirements for AI systems not considered high-risk is regretful, which would have given providers the opportunity to review their systems and identified risks and voluntarily followed a code of conduct or certain requirements set for high-risk AI tools.⁵⁹ This risk-assessment requirement creates doubt as to when exactly are risks considered when establishing the high-risk category. Indeed, all high-risk systems are required to carry out this risk assessment which should also have been initially done by the legislator when establishing this category. This identification of risks at several level may put into question this initial step in classifying systems according to their risks.

Another regrettable consequence to the exclusion of tax AI systems from the high-risk category is the fact that according to the Proposal, standalone high-risk systems would be listed in an EU-wide database, providing increased transparency as to the use of AI tools in Europe. This could have been particularly beneficial for taxpayers in knowing the types of systems are used by the authorities. This might however also explain why tax has been sidelined from the classification; it is possible that this inventory of systems could restrict the tax administration's mission if specific knowledge of the tools being used by the tax were to be disseminated to taxpayers. Indeed, the information provided in the database could endanger the necessary secrecy needed by tax administration to ensure that no taxpayer may

59 Smuha (n 30) 13.

‘game’ the system by collecting confidential information on the workings of the tax administration.

Beyond those requirements, taxpayers could have greatly benefited from the obligations set in article 10 regarding data management, specifically in allowing taxpayers to communicate with the administration to ensure that the data on which the authorities base themselves (and their AI processes) are up-to-date and accurate. Such obligation would incite tax administrations to keep a flow of communication with data subjects.

One of the main criticisms from literature focuses on the reliance by the AI Act on internal compliance by AI providers and users, with particularly limited cases of external and independent assessment of certain requirements. Entrusting AI providers with complying with those obligations with little supervision could effectively limit the effectiveness of the Act.⁶⁰ This is particularly exacerbated by the fact that the requirements in the Act are formulated in a broad way that give providers a large margin of discretion.⁶¹ Accordingly, even if tax administrations were to be subject to the requirements established in the Act, it is, for the time being, difficult to determine how effective those obligations would be to ensure the safeguards necessary to avoid harms to fundamental rights.⁶² In the same vein, the fulfilment of the rules in the Act actually hinges on the Art. 9 risk assessment procedure, and whether it has been carried out properly by the provider. Indeed, providers, in order to fully respond to those very broad requirements, have to actively know the weaknesses and risks of their systems to provide adequate response, even within the confines of those rules.⁶³ This is further exacerbated by the fact that the risk assessment procedure aims at determining what potential harms an AI system may pose to health, safety or fundamental rights, the latter which is potentially very difficult for every provider to assess properly. Indeed, it is up to the provider to decide which risk is to be deemed ‘acceptable’, which gives the provider

60 See, for example, Mauritz Kop, ‘EU Artificial Intelligence Act: The European Approach to AI’ (2021) 2 *Transatlantic Antitrust and IPR Developments* 1, 8.

61 Ebers and others (n 27) 593.

62 For example, Ebers discusses the human oversight requirement in art 14, and highlights how impractical the rule seems, especially in regards to the ability for a human to have a good enough understanding of the system to provide sufficient oversight, leading either to an effective ban of certain AI tools if supporting staff is not trained, or a circumvention of those rules, rendering the obligation in the Act useless. Ebers and others (n 27) 596.

63 Smuha (n 30) 34.

much liberty in deciding how to treat their systems.⁶⁴ This concern is also echoed by authors in analysing the other obligations set in the Act. For example, the data governance rules in article 10 do not define exactly what should be considered an appropriate and accurate data set, leaving it to the consideration of the provider. Similar doubts were raised in relation to the article 14 human oversight rules, where the lack of specificities could lead to discrepancies among providers on their application of the rules.

5. Conclusion

The AI Act marks a significant step in the European Union's effort to regulate the development and deployment of artificial intelligence systems, yet its current configuration reveals a critical shortcoming: the failure to account for the specific risks posed by the use of AI in tax administrations. By categorizing such systems as low-risk or excluding them altogether from the high-risk designation, the legislation overlooks potential harms to taxpayers' fundamental rights and fails to offer meaningful safeguards against opaque or discriminatory practices. This exclusion appears rooted in political sensitivities surrounding fiscal sovereignty and the limitations of the EU's legislative competences. It should be noted that both the legal basis on which the Act is constructed as well as the opportunities for expansion to the Act's scope of protection severely limit the opportunities for AI systems used by tax administrations to be included and meaningfully treated by the obligations under the legislation. Thus, the consequences are practical and far-reaching. Without harmonized protections, the burden of safeguarding rights falls unevenly across Member States, reinforcing disparities and undermining legal certainty. In light of these findings, the article calls for a reconsideration of the regulatory approach to AI in public administration, particularly in areas where the stakes for individual rights and democratic accountability are high.

64 Smuha (n 30) 34.

