“Error 404 – Match not found”

Tax Enforcement and Law Enforcement in the EU Artificial Intelligence Act

David Hadwick

eucrim
European Law Forum: Prevention • Investigation • Prosecution

ABSTRACT

In EU Member States, tax administrations are the public organs that make most use of artificial intelligence (AI) and machine learning (ML) systems to perform State prerogatives. At least 18 EU Member States frequently use AI tax enforcement systems. In certain areas of taxation, such as value-added tax, AI and ML are already used throughout the EU. These systems perform a relatively broad range of tasks, reflecting the wide array of prerogatives of the administration itself. Generally, these different systems can be categorized into two archetypes: coercive and non-coercive AI systems. While non-coercive AI tax systems do not generate significant risks of conflict with taxpayers’ fundamental rights, coercive AI tax systems used for tax enforcement bring about serious risks of conflict with taxpayers’ fundamental rights and tax procedure as a whole. These risks have already materialised in a number of cases and have even led to serious scandals, such as RoboDebt and the toeslagenaffaire.

Yet, substantial confusion exists around the treatment of AI tax enforcement systems in the upcoming Regulation laying down harmonised rules on artificial intelligence (‘EU AI Act’) and whether these systems will be qualified as high-risk. Recital 38 of the current draft prescribes that systems used by tax administrations specifically for administrative purposes should not be viewed as high-risk AI law enforcement systems. While prima facie logical, distinguishing between administrative and law enforcement purposes is bound to be an impractical and arbitrary exercise. Law enforcement is becoming increasingly integrated through the involvement of administrative authorities and private actors, precisely because of the use of AI. In such contexts, the boundaries between administrative and penal processes are blurred and will generate confusion. By remaining attached to that anachronistic distinction, Recital 38 not only replicates that confusion but will exacerbate its effects.

AUTHOR

David Hadwick

Doctoral researcher and PhD Fellow of the Research Foundation for Flanders (FWO)
University of Antwerp, Belgium

CITE THIS ARTICLE

Hadwick, D. (2023). “Error 404 – Match not found” : Tax Enforcement and Law Enforcement in the EU Artificial Intelligence Act. Eucrim - The European Criminal Law Associations’ Forum. https://doi.org/10.30709/eucrim-2023-005

Published in eucrim 2023, Vol. 18(1) pp 55 – 60
https://eucrim.eu
ISSN:

I. Why AI Tax Enforcement Systems Are "High-Risk" Systems

In EU Member States, tax administrations are the public organs that make most use of artificial intelligence (AI) and machine learning (ML) systems to perform State prerogatives. Publicly-available data alone reveals at least 70 AI systems leveraged by national tax administrations, unequally spread over 18 EU Member States.[1] Even the EU itself, through Eurofisc members, has developed its own ML model: Transaction Network Analysis – a data matching model meant to detect missing trader intra-Community fraud.[2] Accordingly, in certain areas of taxation AI and ML are already used throughout the EU for the enforcement of taxation rules.

These AI tax enforcement systems perform a relatively broad range of tasks, reflecting the wide array of prerogatives of the administration itself. Generally, these different systems can be categorised into two archetypes. Some AI systems are leveraged by EU tax administrations for **non-coercive purposes**, including chatbots[3], nudging systems[4], and jurisprudence analysis[5]. These non-coercive systems constitute a minority of the models used by tax administrations in the EU, albeit a significant one.[6] The remainder AI systems are leveraged for **coercive purposes**, i.e. for tax enforcement tasks such as web scraping[7], the detection of statistical risk indicators[89], and risk scoring to screen and select taxpayers for audit.[10] In a little more than a decade, predictive analysis has radically transformed tax enforcement and tax administrations in the EU. Currently, the use of statistics and ML underpins all coercive prerogatives when selecting a taxpayer for audit. Data is collected and processed through ML and taxpayers are algorithmically selected on the basis of risk indicators inferred from ML predictions. The transformative power of AI is also reflected in the human resources of tax administrations, increasingly composed of data scientists and increasingly less of tax law experts.[11]

Some of these models were used by tax administrations in the EU as far back as 2004. This is for instance the case of XENON, a web scraping model leveraged by the Dutch tax administration (*Belastingdienst*).[12] This means that tax administrations were pioneering public algorithmic governance long before debates over other popular buzzwords in predictive policing, such as facial recognition, biometric surveillance, social scoring, etc. The primary reason for the prominence of the use of AI systems by tax administrations is the immense documentary burden placed on tax officials. Each year, tax administrations must process billions of documents[13], answer millions of queries, and spend several millions of minutes on the phone.[14] Processing such volumes of data manually with the human resources of national tax administrations is simply impossible. Accordingly, long before the advent of AI, tax administrations were already using traditional statistical approaches and heuristics to perform their fiscal prerogatives. The transition from traditional statistics to automated statistics and machine learning did thus not constitute a major scale-up.

1. The risks of AI tax enforcement systems

The EU AI Act follows a risk-based approach, meant to strike a proportional balance between the two policy goals of the instrument, namely: the promotion of innovation and the protection of citizens fundamental rights. Accordingly, the Regulation outlines four levels of risk ranging from prohibited to minimal risk. Minimal risk systems (level 1) generally escape the scope of the instrument aside from the invitation to self-regulation through codes of conduct and limited risk systems (level 2) are only bound to minimum transparency requirements in specific use cases, particularly chatbots and deep fakes. Models deemed as bearing unacceptable risk (level 4) are prohibited. By sheer number of articles, the majority of obligations in the instrument are imposed on high-risk systems (level 3). According to the current draft proposal, organisations

https://doi.org/10.30709/eucrim-2023-005

with high-risk systems must comply with strict requirements such as certification, data governance, transparency, human oversight, record-keeping and cybersecurity. Comparatively to the other levels of risk, the obligations imposed on high-risk systems are numerous and substantively detailed, often requiring granular control of specific externalities. Hence, the risk-based approach seeks to ensure that obligations imposed on an AI system are proportional to the risks it generates.

In that regard, AI tax enforcement systems should be viewed as "high-risk" because these systems have been shown to contain various sources of conflict with EU citizens' rights, documented in jurisprudence and doctrine. This is less true for **non-coercive AI tax systems**, in fact, some of these models are truly a net plus both for the administration and for taxpayers. Chatbots, for example, enable taxpayers to request information from the administration at any time of the day and year. Processing little to no taxpayer personal data[15],these systems have opened up a new channel of communication with tax officials, while alleviating the substantial administrative burden of tax officials. Reports indicate that chatbots reduce the number of queries directly sent to the administration by a margin of up to 90%, with very high satisfaction rates amongst taxpayers.[16] The same can be said of nudging, simply by adapting the language of default letters sent to taxpayers, e.g. referring to a taxpayer by his or her first name or by adding references to the benevolent purpose of tax collection, the speed and rate of compliance increase in noteworthy ways.[17]

Conversely**, coercive AI tax systems** used for tax enforcement bring about serious risk of conflict with taxpayers' fundamental rights and tax procedure as a whole. These risks have already materialised in a number of cases. Coercive AI systems can conflict with the principle of legality because they disrupt procedures to such an extent that these no longer reflect procedural codes. For instance in *eKasa*[18], the Slovak Constitutional Court ruled that machine-learning bolstered surveillance to such an extent that it required a specific framework and tailored safeguards to negate the risks of abuses. Currently, the majority of tax administrations in the EU use coercive AI systems without a specific legal basis to that effect and without safeguards to negate demonstrated risks of such systems.[19] This is problematic in terms of legality as the different externalities these systems generate cannot be systematically captured by existing procedural rules.[20] Most notably, these systems entail risks of conflict with the right to a private life and right to data protection, as seen for example in *SyRI*[21] or the State Council (*Conseil d'Etat*) on the use of web scraping[22]. The primary source of friction lies in the fact that tax administrations have adopted tools that increase their surveillance capability based on procedural rules that pre-date the internet. Through web scraping, tax administrations are capable of surveilling the internet, e-commerce platforms, social media, or satellite images without differentiation between compliant and non-compliant taxpayers. As these data processing activities are generally regarded as an administrative process, tax officials do not have to secure any form of prosecutorial assent to use web scraping systems and collect taxpayer personal data.[23] These tools collect bulks of data and match the data to the different taxpayers at a speed unrivaled by any human tax official, drastically increasing the scope of data collected and number of taxpayers surveilled by the administration. In spite of the apparent interferences with privacy, the use of web scraping by tax administrations in the EU, the scope of data collected, the sources of data collection, the limits and safeguards, etc. remain largely unregulated.[24]

Moreover, predictive models such as risk detection and risk scoring tools are prone to errors, statistical biases and discrimination. These models are **predictive**, hence these systems only forecast a **probable** outcome based on what is statistically likely. Such a process by nature involves a great deal of uncertainty, errors, and deviations from objective reality. For these reasons, predictive models have already resulted in serious scandals such as *Robodebt*[25] in Australia and the *toeslagenaffaire*[26] in the Netherlands. The latter is perhaps the best illustration of the devastating consequences that AI tax enforcement systems may occasion, particularly when these are not sufficiently regulated.

2. The *toeslagenaffaire*, stark example of the risks of AI tax enforcement

In the *toeslagenaffaire*, the Dutch tax administration (*Belastingdienst*) attempted to automate the assessment of childcare allowance (*kinderopvangtoeslag*) fraud with a predictive model. The model had the power to, without any human input, discontinue the allowances of welfare recipients and request the reimbursement of all aids ever received. Parents labelled as fraudsters by the AI system were made to pay back large sums of money (€35,000 on average – up to €250,000), testimony to the high childcare costs in the Netherlands, among the highest in the OECD.[27] As the label was disclosed to other public and private actors, following so-called "linkage of records"[28], parents were denied credit cards, bank accounts, loans, other means of public assistance, etc. In some cases, child protective services paid visits to their children's school or homes to forcibly separate them from their parents.[29] Later inquiries by the State Secretary revealed that the predictions of the models were erroneous in 94% of cases.[30] A substantial part of these errors were the result of discrimination induced by the historical biases in data of the administration, data inaccuracies, and the processing of data on nationality and ethnicity by the risk scoring model.[31] A central element of the scandal was the fact that the model contained a feature "Dutch/non-Dutch" (*Nederlander/niet-Nederlander*) whereby the predicted risk of fraud of non-Dutch individuals was systematically increased. The application of such a model meant that foreign residents and dual nationals would be excessively targeted by the model, and thus disproportionately became the victim of unlawful reimbursement requests. Upon revelation of the scandal, the entire Dutch cabinet resigned. Estimations suggest that the cost may be totaling €5.5 billion in compensation for the estimated 40,000 victims.[32] Although the affair was revealed more than two and a half years ago, over 1,500 children have not yet been returned to their parents[33], and testimonies suggest that compensations could last until the year 2030.[34] The scandal perfectly illustrates the potential risks of AI tax enforcement to data protection, privacy, non-discrimination, fair trial, and good governance. The models of the tax administration target a wide and highly heterogeneous population, often based on inaccurate data sources[35], using opaque and potentially biased features. Leveraging statistics to profile taxpayers under such conditions significantly increases the risk of disparity and discrimination.

II. AI Tax Enforcement Systems and the Notion of "Law Enforcement" in the EU AI Act

Despite widespread use and empirically demonstrated risks, substantial confusion remains around the treatment of AI tax enforcement systems in the upcoming EU AI Act. Tax enforcement systems are conspicuously absent from the draft proposal despite AI tax enforcement systems having given rise to the most unsettling case of automation bias to date. The notion that such systems would not constitute a priority in an instrument meant to regulate the externalities of AI is astonishing. Yet, unlike justice, education or law enforcement, tax enforcement is not singled out as a specific area in Annex III of the proposal, where sectors with high-risk systems are listed. The absence of AI tax enforcement from the draft raises questions, particularly as the initial proposal was published in April 2021, a couple of months after the revelations around the *toeslagenaffaire*. To be qualified as high-risk, the only alternative is thus for tax enforcement systems to be allocated to another category listed in Annex III. By elimination, law enforcement appears as the likeliest candidate given that tax enforcement is, in part at least, a form of law enforcement. Tax officials enforce taxation rules, investigate tax crimes, and are viewed as a competent authority in the Law Enforcement Directive (LED).[36] However, Recital 37 of the Preamble of the initial draft proposal specified that AI systems used by tax administrations should not be regarded as systems used for the purpose of law enforcement. In a move completely at odds with the lessons learned in *toeslagenaffaire*, the draft proposal

seemed to create an exemption for tax administrations whereby AI tax enforcement systems would not be regarded as high-risk. This position was striking as it was in direct conflict with the LED, of which the AI Act will be *lex specialis*.[37] The proposal was later amended by the common position of the Council.[38] Recital 38 (formerly 37) now prescribes that AI systems specifically intended for administrative purposes should not be regarded as high-risk systems used by law enforcement, establishing a strict dichotomy between AI used either for administrative or law enforcement purposes. A *prima facie* distinction between criminal and administrative processes seems to make sense under a risk-based approach. Crimes typically result in harsher sentences compared to administrative offences. In the Recital, the severity of sanctions for criminal offences is explicitly mentioned as a factor that should be taken into account. Yet, upon closer analysis, it appears that this dichotomy will generate additional confusion around the treatment of AI tax enforcement systems and whether these qualify as high-risk systems.

In the context of taxation, distinguishing between administrative and criminal offences is a complex and arbitrary exercise. Rare exceptions aside, what distinguishes administrative from criminal offences in taxation is the subjective intention of the perpetrator. Simply put, a tax crime is a fiscal administrative offence committed intentionally. Hence, the salient feature is the *mens rea*. However, AI tax enforcement systems are not used to predicting the subjective intention of a perpetrator. These tools merely predict a risk of non-compliance based on objective material factors. This risk is forecast by examining the gradient between what is declared by a taxpayer, and what level of wealth is stochastically and comparatively probable. In other words, AI tax enforcement systems detect *actus reus,* not *mens rea.* As a result, AI tax enforcement systems are all used **interchangeably** both for administrative and criminal tax offences, none are used **specifically** for administrative purposes. Predictive policing tools of the tax administration are exclusively used in the audit phase, when subjective intentions have not yet been determined. Taxpayers are subjected to the same AI tax enforcement scrutiny whether they are subsequently suspected of fraud or cleared of any suspicion. The fact that the AI system is used to detect what is later qualified as an administrative or criminal offence has little bearings on the model itself and the risks resulting from its use. By the time the offence has been qualified, the model has generated all its potential risks. Yet, the obligations imposed on high-risk systems in the EU AI Act are not retroactive; in fact, most of these are pre-emptive and should be performed prior to using the model. In such a context, it is hard to see how the dichotomy of Recital 38 could be correctly applied. Furthermore, the definitions of fiscal crimes have not been harmonised in the EU, hence some offences may be of administrative nature in one Member State, while being a crime in another.[39] Based on the *Engel*[40] criteria, the dichotomy would rest primarily on the national law qualification of the offence, and whether it is viewed as a crime or an administrative offence in the respective jurisdiction. Since that qualification has not been harmonised, two identical tools may be categorised differently under the AI Act.

Seemingly, Recital 38 attempts to uphold a binary and obsolete notion of "law enforcement" in an era where policing is increasingly integrated. Law enforcement is an organic process involving a multitude of stakeholders, including the traditional police, administrative authorities, and even external corporate actors. This is particularly true for tax administrations that must, by virtue of the wide array of prerogatives performed, involve numerous public and private actors. Tax evasion and tax fraud are umbrella terms meant to qualify an enormous number of offences. Importing an excessive amount of cigarettes or liquor, illegal species of fauna and flora, counterfeited goods, not declaring workers, employing migrant workers, under-valuing an asset, and hiding financial assets are all considered forms of tax evasion and fraud. To detect these offences, the tax administrations continuously collaborate with other agencies, such as food safety administrations, asylum authorities, financial administrations, labour inspectorates, corporate brands, etc. In such a context, distinguishing between different actors and whether their role was incremental to administrative or punitive aspects of a procedure, is so complex that it is bound to be arbitrary. Tax enforcement is becoming increasingly integrated, precisely because of the integration of AI, as the use of certain models relies on the know-how of specific stakeholders. Corporations provide support to police forces and tax administrations,

https://doi.org/10.30709/eucrim-2023-005

online, in public spaces, through proprietary models, etc.[41] NGOs and investigative journalists use web scraping to detect fraudulent schemes and tax evaders using offshore entities.[42] These actors are neither administrative nor criminal, yet play an integral role in the law enforcement apparatus.

III. Conclusion

Overall, the treatment of AI tax enforcement systems in the upcoming EU AI Act is riddled with uncertainty and confusion. Despite several amendments to the draft proposal, Recital 38 seems to raise more questions than it provides answers. Distinguishing between administrative and criminal processes is bound to be an arbitrary, impractical, and reductionist exercise. Moreover, given the state of harmonisation of fiscal crimes in the EU, a literal application of Recital 38 is likely to result in the fragmentation of EU law. While AI is upending pre-existing notions of tax enforcement and law enforcement as reflected in tax and criminal codes, EU legislators remain attached to an anachronistic vestige of public law. As such, this dichotomy is not novel, with this issue also reflected in the GDPR and the LED.[43] Yet, by resting a crucial part of the EU AI Act on this very distinction, the AI Act not only replicates that confusion but strongly exacerbates its effects.

The treatment of AI tax enforcement systems reveals a certain arbitrariness inherent to the risk-based approach in the EU AI Act. Discussions on the potential inclusion of ChatGPT and generative AI as high-risk systems in the proposal[44] indicate that the risk-based approach is excessively focused on buzzwords and may not be the product of a consistent methodology. Conversely, despite the empirically demonstrated prejudicial effects of these systems, tax enforcement is not viewed as warranting its own risk category in Annex III. Factually, the AI systems used by tax administrations are quite unique and do not always correspond to traditional predictive policing. Tax administrations perpetually oscillate between administrative and law enforcement in ways that are hard to capture in a binary legal construct. This is perhaps indicative of AI tax enforcement systems requiring their own *sui generis* category with specific rules and limits, different from "law enforcement" as intended in the instrument. With its wide array of AI systems, both coercive and non-coercive, it is clear that AI tax enforcement escapes traditional dichotomies and legal qualifications. Attempting to fit tax enforcement within a pre-existing mold may thus not be the best strategy. The uniquely ambivalent nature of the tax administration and diversity of AI systems should warrant a dedicated sectorial instrument or specific area of attention in Annex III of the AI Act. In that regard, a risk-based approach should distinguish between non-coercive AI tax systems and coercive systems as suggested in this article.

---

1. D. Hadwick, "Behind the One-Way-Mirror: Reviewing the Legality of EU Tax Algorithmic Governance", (2022) 31(4) *EC Tax Review*, 1, 18. – for a complete breakdown of all the ML systems identified, see: D. Hadwick "AI Tax Admin EU" <https://www.uantwerpen.be/en/projects/aitax/country-reports/> *accessed 4 April 2023.*↩
2. OECD, *Tax Administration Series: Comparative information on OECD and Other Advanced and Emerging Countries*, 2021, p. 110; U. Turksen, *Countering Tax Crimes in the European Union: Benchmarking the OECD's Ten Global Principles*, 2021, p. 244; T. Wahl, "New Data Mining Tool to Combat Vat Fraud", *eucrim*: <https://eucrim.eu/news/new-data-mining-tool-combat-vat-fraud/> *accessed 4 April 2023.*↩
3. OECD, *Tax Administration Series: Comparative Information on OECD and other Advanced and Emerging Economies*, 2019, pp. 175-181.↩
4. M. Luts & M. Van Roy, "Nudging in the Context of Taxation – How the Belgian FPS Finance Uses Behavioural Insights to Encourage Taxpayers to Pay Faster" (2019) *IOTA Papers*, p. 7; D. van Hout, "Gedragsbeïnvloeding in het belastingrecht: Are you 'nudge'" (2019) *Tijdschrift voor Fiscaal Recht*, p. 928-936.↩
5. 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 4 April 2023.*↩
6. Web-scraping, Risk-detection and risk-scoring tools are significantly more prevalent in the EU (65% - 46 out of 70 models are coercive).↩
7. Décret n° 2021-2148 du 11 février 2021, Art. 4, III, 1°-2°.↩
8. OECD, *Advanced Analytics for Better Tax Administration* (2016), p. 23.↩
9. C. Williams, "Developing efficient risk assessment tools to tackle undeclared work: a toolkit" (2021), pp. 17-19 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3944128> *accessed 4 April 2023.*↩
10. OECD, *Tax Administration Series: Comparative Information on OECD and other Advanced and Emerging Economies,* (2019), p. 52.↩
11. Dutch tax administration, Vacatures – out of 70 starter positions, 36 are IT and data analytics, while 20 are fiscal and juridical services: < https://werken.belastingdienst.nl/vacatures/starter/fiscaal-juridisch?order_by=publication_date> *accessed 5 April 2021.*↩

12. European Commission DG Taxation and Customs Union, Risk Management Guide for Tax Administrations – Fiscalis Risk Analysis Project Group (February 2006), p. 67.↩
13. Report from the EC to the Council and the EP COM (2017) 780 final, Eighth report under Article 12 of Regulation (EEC, Euratom) n° 1553/89 on VAT collection and control procedures, p. 11.↩
14. Dutch Tax Administration, *Belastingdienst* "10 miljoen telefoontjes aan de Belastingtelefoon in 2021' <https://over-ons.belastingdienst.nl/organisatie/feiten-en-cijfers/10-miljoen-telefoontjes-aan-de-belastingtelefoon-in-2021/> *accessed 4 April 2023*.↩
15. In fact, chatbots such as "steuerchatbot" in Germany advise taxpayers not to input any personal data, see: <https://steuerchatbot.digital-bw.de/steuerbw.html> *accessed 4 April 2021*.↩
16. OECD, *Tax Administration Series: Comparative Information on OECD and other Advanced and Emerging Economies, op. cit.* (n. 3).↩
17. M. Luts & M. Van Roy, (2019) *IOTA Papers*, *op. cit.* (n. 4); D. van Hout, (2019) *Tijdschrift voor Fiscaal Recht, op. cit.* (n. 4).↩
18. Constitutional Court of the Slovak Republic PL. ÚS 25 / 2019-117 (*eKasa* case) ↩
19. OECD, *Tax Administration Series: Comparative information on OECD and Other Advanced and Emerging Countries*, *op. cit.* (n. 2).↩
20. For instance, the German Tax Code dates from 1919, see: K.-D. Drüen, "Tax in History: Hundred Years Tax Code in Germany", (2019) 47(11) *Intertax*, pp. 979-985.↩
21. Rechtbank Den Haag, 5 Februari 2020 ECLI:NL:RBDHA:2020:1878 (*SyRI* case).↩
22. Cour Constitutionnelle, Décision n° 2019-796 du 27 décembre 2019 sur la loi de finances pour 2020, §§79–96 ;Commission Nationale Informatique & Libertés (CNIL), Déliberations n° 2019-114 du 12 Septembre 2019 portant avis sur le projet d'article 9 du projet de loi de finances pour 2020.↩
23. D. Dierickx, "The Belgian compliance model and methodology to obtain data from 'Sharing Economy' platforms" in: *IOTA* (ed.) *Disruptive Business Models – Challenges for Tax Administrations* (2017), pp. 21-23.↩
24. With the exception of Décret n° 2021-2148 du 11 février 2021, Art. 4, III, 1°-2° in France, *op. cit.* (n. 7), no procedural rules regulate the specific use of web scraping by tax administrations.↩
25. Court settlement *Robodebt* case: Federal Court of Australia, 23 Dec. 2020, *Prygodicz v. Commonwealth*, Order no. VID1252/2019.↩
26. Autoriteit Persoonsgegevens [Dutch Data Protection Authority], Belastingdienst/Toeslagen – De verwerking van de nationaliteit van aanvragers van kinderopvantoeslag, Rapport no. z2018-22445 (2020); Tweede Kamer der Staten-Generaal [Netherlands 2nd Parliamentary Chamber], Eindverslag Parlementaire ondervragingscomissie Kinderopvantoeslag "Ongekend Onrecht", pp. 3-7 (The Hague, 17 Dec. 2020).↩
27. S. Ranchordás, & L. Scarcella, "Automated Government for Vulnerable Citizens: Intermediating Rights" (2021) 30(2) *William & Mary Bill of Rights Journal*, 373-418.↩
28. Dutch Ministry of Justice (Ministerie van Justitie en Veiligheid), "Nota naar aanleiding van het verslag inzake de Tijdelijke wet uitwisseling persoonsgegevens UHP KOT" (11 January 2023), pp. 2-4.↩
29. L. Kok, "Kabinet: Mogelijk meer dan 1115 kinderen in toeslagenaffaire gedwongen uit huis geplaatst", *AD*, 21 October 2021: <https://www.ad.nl/politiek/kabinet-mogelijk-meer-dan-1115-kinderen-in-toeslagenaffaire-gedwongen-uit-huis-geplaatst~ad7a83e4/> *accessed 4 April 2023*.↩
30. Tweede Kamer der Staten-Generaal, Eindverslag "Ongekend Onrecht", *op. cit.* (n. 26), pp. 22-23↩
31. See Autoriteit Persoonsgegevens, *op. cit.* (n. 26).↩
32. J. Frederik, "De compensatieregeling voor de toeslagenaffaire is een fiasco van 5,5 miljard. Wat nu?", *De Correspondent*, 2 February 2022: <https://decorrespondent.nl/13097/de-compensatieregeling-voor-de-toeslagenaffaire-is-een-fiasco-van-5-5-miljard-wat-nu/787932533003-ef601d9e> *accessed 4 April 2023*.↩
33. See Autoriteit Persoonsgegevens, *op. cit.* (n. 26).↩
34. I. de Kruif, "Compensation ouders toeslagenaffaire kan zomaar tot 2030 duren", *NOS*, 18 January 2023: <https://nos.nl/nieuwsuur/artikel/2460354-compensatie-ouders-toeslagenaffaire-kan-zomaar-tot-2030-duren> *accessed 4 April 202*.↩
35. E.g. data collected on social media platforms or data emanating from denunciations made by other taxpayers.↩
36. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union legislative acts, COM(2021) 206 final.↩
37. Art. 2 & Art. 3(7), Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA *OJ L 119, 4.5.2016, p. 89–131*.↩
38. Council of the European Union 'General approach' to Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (AI Act) and amending certain Union legislative acts, 25 November 2022, Interinstitutional File: 2021/0106 (COD), p. 38.↩
39. J. Cremers, "EU Company Law, Artificial Corporate Entities and Social Policy" (2019) *European Trade Union Confederation*, p. 36.↩
40. ECtHR, 23 November 1976, *Engel and others v Netherlands*, Appl. no. 5100/71 et al., para 82.↩
41. B. Kennedy & L. Ryder, "IBM Public Safety Solutions for a Safer Planet", 2021, pp. 5-7.↩
42. A. Palionis, "Web Scraping for Transparency", *New Digital Age*, 30 September 2022: <https://newdigitalage.co/?s=Web+Scraping+for+Transparency> *accessed 4 April 2023*.↩
43. CJEU Case C-175/20, 24 February 2022, SIA 'SS' v Valsts ieņēmumu dienests, para 35 to 42.↩
44. G. Volpicelli, "ChatGPT broke the EU plan to regulate AI", *Politico*, 3 March 2023: <https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/> *accessed 5 April 2023*.↩

ABOUT EUCRIM
eucrim is the leading journal serving as a European forum for insight and debate on criminal and "criministrative" law. For over 20 years, it has brought together practitioners, academics, and policymakers to exchange ideas and shape the future of European justice. From its inception, eucrim has placed focus on the protection of the EU's financial interests – a key driver of European integration in "criministrative" justice policy.
Editorially reviewed articles published in English, French, or German, are complemented by timely news and analysis of legal and policy developments across Europe.
All content is freely accessible at https://eucrim.eu, with four online and print issues published annually.

Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union