ISSN 1745-638X (Online)

THE COMPETITION LAW REVIEW

Volume 15 Issue 1 pp 31-49 **January 2023**

An 'AI whistle-blower' to monitor algorithmic infringements?

*Isabella Lorenzoni**

In the digital era, technology is taking over some important business decisions. Algorithms are in fact in charge to define price strategies, collect consumers' data, suggest products and services and target advertisements. Despite the countless benefits that technology brings into our society, risks should also be addressed. Algorithmic discrimination and algorithmic collusion are among the insidious practices that can harm consumers' welfare and competition. In order to keep pace with the evolution of technology and tackle the new challenges brought by a digitalised economy, competition authorities have started to build their own Artificial Intelligence (AI) arsenal for the purpose of enforcing competition law. Nevertheless, it might take time before regulators will fully benefit from AI. Therefore, other solutions for preventing and detecting anticompetitive behaviours of companies and their algorithms should be explored. At the internal level, companies that are already equipped with their AI systems are in the best position to use them also within the framework of their compliance programs. For example, in the financial sector, RegTech solutions have been implemented by companies to help them to internally detect illegal behaviours and some of these solutions could also be applied for competition compliance. In particular, the increasing importance of whistle-blowers enhanced with the power of technology, have led to speculate on the feasibility of an "AI whistle-blower" for regulatory compliance in the financial industry. In the field of competition, an AI whistle-blowing tool, able to detect algorithmic infringements could be implemented as part of companies' compliance programs and therefore as a private enforcement tool. Concerns related to privacy, data protection and the black box nature of AI should nevertheless be carefully considered.

1. INTRODUCTION

In a market dominated by big tech companies, where even traditional brick-and-mortar firms are becoming digital, competition authorities are facing new challenges, as sophisticated ways of colluding and infringing competition rules become possible. Monitoring algorithms, parallel algorithms, signalling algorithms and even self-learning algorithms are increasingly employed as pricing tools from which companies benefit to maximise their profits. But they do not come without risks for competition law. Enforcers' powers might not always succeed in detecting and proving algorithmic infringements. Especially considering the potential harm that self-learning algorithms could cause to consumers and competition, it is debated whether or not the current antitrust rules are adequate to sanction possible algorithmic infringements.[1]

Competition authorities need to understand how algorithms employed by companies work in order to assess whether or not there was an infringement of competition law and

* Ph.D. Student at the Faculty of Law, University of Luxembourg, isabella.lorenzoni@uni.lu. Supported by the Luxembourg National Research Fund PRIDE19/14268506.iog.

1 OECD, 'Algorithms and Collusion: Competition Policy in the Digital Age' (2017).

therefore a decision to fine their behaviour could be issued. However, interviews with some competition authorities reveal that most have only recently started to develop their own technological capacity, by building dedicated digital units. Most of their projects are still on an experimental phase and it might take some years before competition authorities could actually benefit from their own computational tools. Until enforcers are well equipped with their own digital expertise, traditional enforcement tools might become less powerful in the fight against digital competition infringements. For instance, studies have confirmed a general decline of leniency applications, mostly due to damages claims.[2] Many regulators that rely on their leniency programs for enforcing competition law might now face another challenge. What would happen when a wrongdoing is mostly committed by an algorithm, especially in the case of self-learning algorithms? Since some Artificial Intelligence (AI) systems are naturally black-boxes and therefore difficult to be explained, companies themselves might not even realise that they are infringing competition rules with their algorithms. Yet, as Commissioner Vestager made it clear, companies cannot hide behind a computer program to escape liability.[3] It would then be difficult for a company to apply for leniency and admit collusion with other companies, if it is not fully aware on how their own algorithms are actually working. This paper seeks to investigate whether private tools implemented by companies could be suited to prevent algorithmic infringements, and therefore become an additional aid for regulators to enforce competition law.

This paper is divided as follows: Section 2 provides the background to companies' uses of novel technologies and the potential harms of their employed algorithms for competition and consumers. Section 3 then demonstrates whether enforcers are ready to tackle the new challenges of the digital era. Finally, section 4 explores the possibilities of implementing AI within corporate compliance programs as an enforcement tool for competition law. In particular, this section aims to analyse the use of AI as an "AI whistle-blower", drawing from other policy areas, such as finance and banking, and how this could be implemented for competition compliance. Advantages and challenges will also be explored. Section 5 concludes.

2. ALGORITHMS AND THE RISK FOR CONSUMERS AND COMPETITION

In a digital era dominated by AI, Big Data and big tech companies, business strategies are increasingly delegated to algorithms for defining prices, tailoring products and services to customers and consumers' needs and enhancing efficiency.[4]

Algorithms are generally defined as a set of instructions to perform a task and solve a specific problem.[5] The increased computational power and the incredible amount of

[2] Johan Ysewyn and Siobhan Kahmann, 'The decline and fall of the leniency programme in Europe' (2018) 1 Concurrences 44.

[3] Commissioner Margrethe Vestager, 'Algorithms and competition', Speech at the Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2017 in OECD (n 1) 39.

[4] OECD (n 1).

[5] Competition & Markets Authority, 'Algorithms: How they can reduce competition and harm consumers' (2021), 4. See also World Wide Web Foundation, 'Algorithmic Accountability – Applying the concept to different country contexts' (2017) according to which "[a]lthough typically defined as a set of "encoded

available data have brought new opportunities and ventures. Among others, the development of machine learning algorithms is a breakthrough as it enables self-learning from the input data, identifying patterns and giving predictions without being specifically programmed by a human.[6]

Despite the acknowledged benefits that sophisticated algorithms bring to undertakings, consumers and therefore society as a whole,[7] red flags are nevertheless raised, which must be addressed. Algorithms can, in fact, harm consumers and competition. Algorithmic discrimination and algorithmic collusion are among the key risks identified by researchers and regulators.[8] Being aware of the different types of algorithms and how they can be dangerous for the well-being of society if used in the wrong way is the first step toward a preventive approach. The following section explains algorithmic discrimination and algorithmic collusion, how they harm consumers and competition and whether they constitute an actual risk to society.

2.1. Algorithmic discrimination

Different types of discrimination that involves the use of algorithms could be identified. For instance, price discrimination happens when the same product is sold at different prices according to consumers' willingness to pay, without a difference in costs.[9] Companies have access to consumers' data and information, which enable them to better personalise their offers to suit consumers' needs.[10] This practice can create benefits for consumers, such as lower research costs, lower prices, discounts, and a selection of products that match the expectation of a consumer.[11] However, downsides have also been flagged. For instance, price discrimination can unfairly affect longstanding customers charged with higher prices for the same product compared to the new ones

procedures" or "a logical series of steps for organising and acting on a body of data to quickly achieve a desired outcome", the term algorithm is often intended to describe a larger intersection of code, data and automated decisions. Originating from computer science and used in various social science disciplines, the term has been used to convey various meanings on the intertwining of human and machine decision inputs, and the extent to which the term includes code, data and ecosystems often varies".

6 OECD (n 1) and World Wide Web Foundation, ibid.

7 See for instance in OECD (n 1), the use of algorithms by businesses and governments (11 ss.) and how they may create pro-competitive effects (14 ss.).

8 See among others, Ariel Ezrachi and Maurice E. Stucke, 'Artificial Intelligence & Collusion: When Computers Inhibit Competition' (2017) 5 University of Illinois Law Review 1775; OECD (n 1); Bundeskartellamt & Autorité de la concurrence, 'Algorithms and Competition' (2019) Working Paper; Justin Johnson and Daniel D. Sokol, 'Understanding AI Collusion and Compliance' in D. Daniel Sokol and Benjamin van Rooij (eds), *Cambridge Handbook of Compliance* (SSRN 2020); Competition & Markets Authority (n 5); Stefano Azzolina, Manuel Razza, Kevin Sartiano and Emanuel Weitschek, 'Price Discrimination in the Online Airline Market: An Empirical Study' (2021) 16 Journal of Theoretical and Applied Electronic Commerce Research, 2282.

9 Also known as personalised pricing. Competition & Markets Authority (n 5) 10 ss; Bundeskartellamt & Autorité de la concurrence (ibid) 6 and Azzolina et al. (ibid).

10 Azzolina et al. (n 8).

11 Competition & Markets Authority (n 5) 10-11.

that are more willing to negotiate.[12] Price opacity and lack of transparency of such companies' strategies are also concerns for consumers.[13]

Discrimination can also occur when platforms in the e-commerce sector use their algorithms to discriminate against competitors' products based on their own personal interests. For instance, self-preferencing happens when online platforms favour their own products, as in the *Google Shopping* case.[14] The European Commission found Google infringing competition rules by placing its own services in the search results in a more favourable position than those of competitors.[15] Another way in which algorithms can discriminate is to favour products of sellers that are willing to pay higher fees, by giving them more visibility to the detriment of competitors, whose items would be put in a disadvantageous position.[16] In this regard, the Australian Competition and Consumer Commission (ACCC) investigated the ranking rates of *Trivago*, a famous online platform that compares online booking hotel sites to suggest to consumers the cheapest offer. However, this was not always the case, as Trivago's algorithm placed hotels that paid the highest "cost-per-click" fee on the top position of its website, misleading consumers to think that it found the cheapest option.[17]

2.2. Algorithmic collusion

Algorithms can infringe competition law also by implementing and facilitating more stable cartels and ultimately colluding. Studies have identified different scenarios where companies could use algorithms for these purposes.

Firstly, algorithms can act as facilitators of collusion, by collecting competitors' information, monitoring their prices, and automatically punishing any deviation from the

[12] ibid., and Azzolina et al. (n 8).

[13] Competition & Markets Authority (n 5). In this regard see also the study conducted by Azzolina et al. (n 8), on price discrimination applied by airlines suspected of using customers' data to exploit their willingness to pay.

[14] Case AT.39740 *Google Search (Shopping)*, 27.06.2017 and the recent judgment of the General Court of 10 November 2021, case T-612/17 *Google LLC, and Alphabet, Inc. v. European Commission* [2021] EU:T:2021:763. See also Competition & Markets Authority (n 5) 25 ss.

[15] ibid.

[16] This is the case of so-called "ranking algorithms". Competition & Markets Authority (n 5); Bundeskartellamt & Autorité de la concurrence (n 8). In this regard, see the pilot project of the Italian competition authority that aims to analyse the ranking algorithm of Amazon, the biggest platform of e-commerce in the world, which hold a dominant position with a role of gatekeeper and seller at the same time. Antonio Buttà, Andrea Pezzoli, Manuel Razza and Emanuel Weitschek, 'Inferire il funzionamento degli algoritmi nelle piattaforme di e-commerce con il machine learning – aspetti di tutela della concorrenza e del consumatore' (Ital-IA 2022 – Workshop AI per la Pubblica Amministrazione, February 2022).

[17] Competition & Markets Authority (n 5) 23 and "Trivago misled consumers about hotel room rates" 2020, in ACCC <https://www.accc.gov.au/media-release/trivago-misled-consumers-about-hotel-room-rates> accessed 27 March 2022.

agreed price.[18] Algorithms increase transparency and adjust to price changes in real-time[19] reducing the need for a price war and making collusion more stable and efficient.[20]

Secondly, algorithms could be explicitly programmed to encourage collusion and set higher prices by acting as "the agent of a human designer [with] a collusive desire".[21] This could happen when companies share the same pricing algorithm programmed to implement anticompetitive prices and avoid competition.[22] The *Topkins* case is emblematic: a seller of posters on the online platform of Amazon coordinated prices with other competitors by sharing the same pricing algorithm, designed to act according to their price agreement.[23]

Another case falling within this category is the so-called "hub-and-spoke" scenario, where a third party, which could be a consultancy or an IT company, provides the same pricing algorithm to multiple sellers, who may or may not be aware of the fact that other competitors use the same tool.[24] This would present risks for competition in several ways. Using the same pricing algorithm would mean that price decisions would be similar, as the algorithm would react in the same way to market changes.[25] Competitors could be aware of having the same algorithms and use it to set anticompetitive prices. The third party in question that provides the same software to all competing clients could also have an interest in generating collusion among them, when its remuneration is based on the revenues of the companies or the performance of the algorithm.[26] The *Eturas* case[27] sets an example in this regard. Several travel agencies used the same online booking system provided by the company Eturas which imposed constrains to the discounts that the travel agencies could offer to their clients. The Court of Justice of the European Union (CJEU) found that a concerted practice within the meaning of Article 101 TFEU would be identified if the travel agencies were aware of the measures implemented by Eturas, "unless they publicly distanced themselves from that practice, reported it to the administrative authorities or adduce other evidence to rebut that presumption."[28] The

18 Bundeskartellamt & Autorité de la concurrence (n 8) 28. Ezrachi and Stucke (n 8) called this first category of collusion as "the computer as messenger" 1784 ss. OECD (n 1) called this type of algorithm "monitoring algorithms" 26 ss.

19 Johnson and Sokol (n 8) 2.

20 OECD (n 1) and Bundeskartellamt & Autorité de la concurrence (n 8) 30-31. In this regard see the Commission decisions AT.40181, AT.40182, AT.40465, AT.40469 according to which algorithms were used to monitor online reseal prices and they intervene when low prices were offered.

21 Johnson and Sokol (n 8) 3.

22 ibid., and OECD (n 1).

23 OECD (n 1) 28; Johnson and Sokol (n 8) and Ezrachi and Stucke (n 8) 1786.

24 OECD (n 1) which calls this category "parallel algorithms"; Ezrachi and Stucke (n 8); Johnson and Sokol (n 8) and Bundeskartellamt & Autorité de la concurrence (n 8) 31 ss.

25 Bundeskartellamt & Autorité de la concurrence (n 8) 32 ss.

26 ibid.

27 Case C-74/14 *'Eturas' UAB et al., v Lietuvos Respublikos konkurencijos taryba* [2016], EU:C:2016:42.

28 ibid., [50].

CJEU provided some criteria for when a company could be found liable for the anticompetitive behaviour of a third party that it hired. [29]

Thirdly, signalling algorithms have been identified as a facilitator factor to unilaterally communicate the intention of a company to collude, by disclosing their price information in advance and negotiate price increase, avoiding explicit communication.[30] In this context "[a]lgorithms might reduce or even entirely eliminate the cost of signalling, by enabling companies to automatically set very fast iterative actions that cannot be exploited by consumers, but which can still be read by rivals possessing good analytical algorithms."[31]

Lastly, the most discussed scenario is what Ezrachi and Stucke (2017) called the "digital eye",[32] which covers situation where competing companies use their own and distinct algorithm that is able to autonomously collude without being explicitly programmed to do so.[33] This is the hypothetical case of self-learning algorithms that in order to achieve the goal of maximizing profits, they would learn that the best strategy is in fact to collude with each other.[34] In this scenario, there is no human involvement nor an explicit design to collude, but only the "self-learning and independent machine execution."[35] According to some scholars, purely algorithmic collusion (or AI collusion) would not represent a real danger for competition law as at the present there are no actual evidence of "autonomously colluding robots" on the market.[36] However, several experiments are carried out in laboratories that aim to reproduce real competitive environments and make pricing algorithms interact with each other.[37] For instance, it has been demonstrated that

[29] Case C-542/14 *VM Remonts v Konkurences padome* [2016], EU:C:2016:578. Bundeskartellamt & Autorité de la concurrence (n 8) 35-36: "an undertaking may be held liable for a concerted practice on account of the (anticompetitive) acts of an external service provider that it hired if one of the following conditions is me: the service provider was acting under the direction or control of the undertaking concerned […]; or that undertaking was aware of the anti-competitive objectives pursued by its competitor(s) and the service provider and intended to contribute to them by its own conduct; or that undertaking could reasonably have foreseen the anti-competitive acts of its competitors and the service provider and was prepared to accept the risk which they entailed". The same criteria would apply in case a third party provides a collusive pricing algorithm. When companies would not be aware and could not reasonably foresee that competitors were using the same pricing algorithms provided by the same third party, it would be a case of a "legal parallel behaviour", which nevertheless would create undesired effects for competition. Bundeskartellamt & Autorité de la concurrence (n 8) 41.

[30] OECD (n 1), 29.

[31] ibid., 30.

[32] Ezrachi and Stucke (n 8) 1795.

[33] ibid.; OECD (n 1); Bundeskartellamt & Autorité de la concurrence (n 8); Johnson and Sokol (n 8).

[34] OECD (n 1) 31-32.

[35] Ezrachi and Stucke (n 8) 1795; Bundeskartellamt & Autorité de la concurrence (n 8) 43.

[36] Ai Deng, 'From the Dark Side to the Bright Side: Exploring Algorithmic Antitrust Compliance' (2019 NERA Economic Consulting and Johns Hopkins University) 5. See also Thibault Schrepel, 'The Fundamental Unimportance of Algorithmic Collusion for Antitrust Law' (2020) JOLT Digest <https://jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law> accessed 15 March 2022.

[37] Bundeskartellamt & Autorité de la concurrence (n 8) 45.

by performing the prisoners' dilemma, algorithms can cooperate with opponents.[38] By using reinforcement learning or introducing an additional agent that rewards or punishes the algorithmic players, the latter can be guided towards a cooperative outcomes, as in the hub-and-spoke scenario.[39]

The hypothesis of self-learning colluding algorithms would represent a case of tacit collusion, which falls outside the scope of competition law.[40] Nevertheless, this topic has caught the attention of regulators[41] and it is the object of a growing literature which proposes for instance to introduce a new concept of agreement within the EU legal framework in order to include cases of tacit collusion that could capture also algorithmic infringements.[42] Whether or not algorithmic collusion represents a real harm for consumers and competitors, having unleashed algorithms in the market would potentially lead to undesired outcomes.[43] The more AI progresses the more companies experiment new business strategies so that "it cannot be ruled out that algorithms may learn to communicate and thereby increase the likelihood of algorithmic collusion."[44]

3. ARE COMPETITION AUTHORITIES READY TO TACKLE THE CHALLENGES OF THE DIGITAL ERA?

Competition authorities have to deal with an emerging reality, where undertakings are exploring new possibilities of conducting business, and where the structure of the market is becoming more complex and is evolving at a fast pace.[45] As a result, antitrust enforcers are starting to equip themselves with digital tools for enforcement purposes. Regulators are in fact looking into developing their own IT expertise and creating *ad hoc* digital units. Some more advanced competition authorities have experimented the use of AI systems

[38] See for instance Deng (n 36) and Thomas Fetzer, Damaris Kosack, Heiko Paulheim and Michael Schlechtinger, 'How algorithms work and play together' (2021) 3 Artificial Intelligence and Competition Law – Concurrences 19.

[39] Deng (n 36).

[40] See for instance OECD (n 1) 33 ss.

[41] OECD (n 1); Competition & Markets Authority (n 5) and Bundeskartellamt & Autorité de la concurrence (n 8).

[42] OECD (n 1) 37; Mario Siragusa, 'Artificial intelligence: algorithms and competition'. (2021) 3 Artificial Intelligence and Competition Law – Concurrences 24; Fetzer, Kosack, Paulheim and Schlechtinger (n 38).

[43] OECD (n 1) 33 ss. according to which "[a]lgorithms can amplify the so called "oligopoly problem" and make tacit collusion a more frequent market outcome". Ezrachi and Stucke (n 8) stated that "conscious parallelism is legal. The question is whether such practices, when implemented by smart machines in a predictable digitalized environment, ought to be condemned" 1795.

[44] Ulrich Schwalbe, 'Algorithms, Machine Learning, and Collusion' (2018) 14 Journal of Competition Law & Economics 568; Bundeskartellamt & Autorité de la concurrence (n 8) 44.

[45] Thibault Schrepel, 'Computational Antitrust: An Introduction and Research Agenda' (2021) 1 Stanford Journal of Computational Antitrust, 1. See also Cary Coglianese and David Lehr, 'Regulating by Robot: Administrative Decision Making in the Machine-Learning Era' (2017) 105 Georgetown Law Journal 1147, 1171 "Antitrust Division might conceivably come to rely on machine learning to predict what effects a proposed merger would have on future competition and market pricing, perhaps entirely automating the antitrust review process".

(machine learning or deep learning solutions) as tools to help in cartels detection or analysis of data during investigations.[46]

Interviews conducted with some competition authorities revealed that despite the efforts to develop their own AI arsenal to boost *ex officio* investigations and tackle the challenges of the digital market, we still have a long way before they will be fully equipped to face algorithmic infringements. Problems related to lack of data that hinder the implementation of fully AI tools have been flagged by many competition authorities, due to information asymmetries between regulators and undertakings.[47] Platforms so far implemented work only with publicly available data, but they still miss important (and private) data (such as costs, outputs etc.), that only companies know and are reluctant to share without an official request for information. Other obstacles that prevent competition authorities from developing such computational tools relate to lack of resources. In fact, building in-house technologies mean for competition authorities to make clear choices of resources allocation.[48] Some competition authorities also reported that because they have too few cases, the implementation of sophisticated AI tools for cartel detection is not a high priority at the moment, as they need to decide how to allocate resources efficiently. Even if the use of AI and other digital investigation tools for enforcement purposes are still in their infancy, it is believed that in the near future, competition authorities will heavily rely on these computational tools.[49]

But until then, alternative ways based on AI, machine learning and Big Data could be implemented by undertakings (and maybe even imposed) as a good strategy for prevention, detection and deterrence of anti-competitive behaviours by companies and their algorithms. In fact, companies should be aware that the use of complex algorithms, that are difficult (if not impossible) to understand even for IT experts could lead to anti-competitive outcomes, such as discrimination or collusion. They could infringe competition rules even if not programmed to do so explicitly. On the one hand, enforcers might struggle to prove an anticompetitive behaviour by only relying on traditional enforcement tools, such as whistle-blower or leniency programs. On the other hand, companies might not be able to recognise an infringement of competition law in order to file a leniency application, due to the inscrutability of certain algorithms. Thus, such uncertain situations may lead to (unwanted) chilling effects on innovation, as companies fearing to be fined for competition infringements may decide not to invest in new

[46] Ioannis Lianos, 'Computational Competition Law and Economics: Issues, Prospects - An Inception Report' (2021) Hellenic Competition Commission 17-18.

[47] Jay L. Himes, Jason Nieh, and Ron Schnell, 'Antitrust Enforcement and Big Tech: After the Remedy Is Ordered' 1 Stanford Journal of Computational Antitrust 64, 78; Schrepel (n 45) 5; Helena Quinn, Kate Brand and Stephan Hunt, 'Algorithms: helping competition authorities be cognisant of the harms, build their capabilities and act' (2021) 3 Artificial Intelligence and Competition Law – Concurrences 5, 11.

[48] Rosa M. Abrantes-Metz, 'Proactive vs Reactive Anti-Cartel Policy: The Role of Empirical Screens' (8th European Summer School and Conference in Competition and Regulation, Corfu, Greece, July 2013).

[49] Schrepel (n 45). Even smaller competition authorities that have not developed any digital tools are participating in working groups within the European Competition Network to learn from the most technological authorities and exchange best practices.

technologies. Other solutions could be experimented that would make compliance easier and therefore decrease the risk of breaching competition rules.

4. HOW AI CAN ENHANCE REGULATORY COMPLIANCE

Among competition enforcement tools, corporate compliance programs are important for prevention, detection and deterrence of competition infringements.[50] Compliance programs can assume different forms, from training programs for employees and managers to monitoring and auditing tools.[51] In a digital world, where price strategies are more and more set by algorithms which can discriminate, and ultimately collude, compliance programs would need to be adjusted accordingly. Commissioner Vestager stated that "business can – and must – […] ensure antitrust compliance by design. That means pricing algorithms need to be built in a way that doesn't allow them to collude."[52] The position of Commissioner Vestager is clear: companies will be held responsible for what their algorithms do.[53]

Leaving aside the discussion on whether or not algorithmic collusion is first and foremost a real danger for competition law and whether it should be fined since it would be a case of tacit collusion, the focus is now on how algorithms and new technologies could be used to enhance compliance programs and compliance by design.

If algorithms such as machine learning systems can be used as screening tools to detect wrongdoings outside a company, they could also be used within a company, especially when the firm has already developed its own pricing algorithms. Undertakings should implement AI tools for "effective compliance programs", as "companies should consider engaging in more proactive compliance approaches"[54] which includes also the use of AI. As some competition authorities already "recommended [screening] tools for internal detection of cartels" (Chile's Guidelines on Competition Law Compliance of June 2012),[55] the same should now apply to new and breakthrough technological means for detecting cartels. Competition authorities should then issue guidelines to recommend

---

50 OECD, 'Competition Compliance Programmes' (2021) OECD Competition Committee Discussion Paper, http://oe.cd/ccp.

51 ibid and Abrantes-Metz (n 48). It is assumed that especially for managers at the highest level, it is important to involve them in compliance programs and introduce a "culture of compliance." OECD (n 50) 34 ss.

52 Commissioner Margrethe Vestager, "Algorithms and competition," Speech at the Bundeskartellamt 18th Conference on Competition, Berlin, 16 March 2017, in Deng (n 36). She further stated that "some of these algorithms will have to go to law school before they are let out. You have to teach your algorithm what it can do and what it cannot do, because otherwise there is the risk that the algorithm will learn the tricks… We don't want the algorithms to learn the tricks of the old cartelists… We want them to play by the book also when they start playing by themselves" Commissioner Vestager, Interview at the 2017 Web Summit, in Deng (n 36).

53 Commissioner Vestager's speech: "The challenges that automated systems create are very real. If they help companies to fix prices, they really could make our economy work less well for everyone else. (...) So as competition enforcers, I think we need to make it very clear that companies can't escape responsibility for collusion by hiding behind a computer program." Commissioner Margrethe Vestager, 'Algorithms and Competition', (2017) Speech at the Bundeskartellamt 18th Conference on Competition, Berlin, in OECD (n 1), 39.

54 Abrantes-Metz (n 48) 12.

55 ibid.

developing AI systems as monitoring tools for companies in the framework of their compliance programs.[56]

4.1. AI as a monitoring tool

Projects for developing AI that would act as a "guardian" for regulatory compliance are ongoing in the field of competition law. For instance, Deng (2019) suggested to build algorithms following several criteria to ensure that they comply by design, since software are first and foremost products of a human programmer.[57] Algorithms should not be designed in a way that would facilitate communication with competitors, nor it should be given an explicit goal to collude or coordinate.[58] He suggested to directly incorporate compliance into algorithm design for example by using reinforcement learning (RL) systems, in order to avoid the problem of translating the Sherman Act provisions into "if" and "then" instructions for computer programs, as this task is considered difficult if not impossible. Since a company has to take into consideration a number of variables and constraints (costs, regulatory, ethical and competition compliance) for its ultimate goal of maximizing profit, an RL system would be based on an "actor-critic approach". An actor tries to learn the strategy with the best outcome to maximise profit, and a critic one would look at the compliance score for the pricing strategy and provide negative or positive feedback to the actor in order for it to adjust its strategy to comply with antitrust. However, the author highlighted also a number of technical and practical problems that would need to be solved before such a model could be implemented.[59]

Other examples include the use of algorithms in compliance programs to directly monitor the "symptoms" of competition infringements, such as an unexplainable price increase or other factors not related to price, such as output restrictions.[60] Algorithms can be used for monitoring the behaviours of humans as well as algorithms.[61] For instance, in the Regulatory Technology industry, AI systems have been developed to help companies to meet their regulatory compliance needs, by using techniques of natural language processing (NLP) and natural language understanding (NLU) to capture and understand voice and text communication. These AI systems could also be implemented to flag any problematic communications in real time between competitors to detect and prevent potential collusive behaviour.[62] Screening techniques have also been proposed as an internal monitoring tool to detect algorithmic collusion.[63] Internal screening methods are

[56] For instance, the "European Commission asks for auditing and monitoring as prevention and detection tools, in particular when a firm is active on tendering markets […] similarly to the US, which asks for the use of screens and communication monitoring tools […]. Chile and Peru also refer to screening and use of software to, for example, monitor conversations with competitors." OECD (n 50) 39.

[57] Deng (n 36).

[58] ibid.

[59] ibid., 8 ss.

[60] ibid.

[61] See also Fetzer, Kosack, Paulheim and Schlechtinger (n 38).

[62] Deng (n 36) 4.

[63] OECD (n 50) 40 ss., and Johnson and Sokol (n 8). Abrantes-Metz (n 48) proposed the implementation of screening tools internally by companies.

already used in regulatory fields such as fraud and anti-corruption. For instance, the company AB InBev developed an in-house data analytic platform (BrewRIGHT) that uses machine learning and AI techniques to identify patterns in their transactions across the world. They mainly concentrate on eliminating corruption, fraud and money laundering and operating ethically and responsibly.[64]

4.2. Lesson learned from the *RegTech* in the financial sector: whistle-blowing

In the banking and financial sector, whistle-blowing tools have become extremely important to detect corporate wrongdoings and have been recognised as an efficient regulatory device[65] and "a private enforcement tool for the authorities."[66] Major scandals in this sector, such as LuxLeaks, Panama Papers, and Cambridge Analytica, have been revealed by whistle-blowers. As a result, regulators worldwide are paying more attention to the protection of whistle-blowers.[67] Lately, in parallel with an increase in importance for whistle-blowers, technology has become the key element for enhancing corporate regulatory compliance. First coined in the financial sector, the term "RegTech", a subfield of FinTech, is becoming popular also in other industries. It can be described as "technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities."[68] Therefore, technological innovations can ensure more robust compliance programmes to regulatory requirements and discover more efficiently internal wrongdoings.

In corporate compliance, the next step was to merge technology and whistle-blowing tools to empower whistle-blowers and take advantages of the disruptive impact of innovation. It is assumed that "whistleblowing may be just the latest human endeavour to be taken over by machines."[69] Interaction between technology and whistle-blowers can take two different paths. First, technology can help to better protect (human) whistle-blowers.[70] Second, it has been suggested that AI can even replace human whistle-blowers

[64] OECD (n 50) 40. According to AB InBev, there is now more awareness from companies that want to implement compliance programs "in the fight for transparency and against corruption. At the 2020 annual meeting of the World Economic Forum, AB InBev CEO Carlos Brito along with leaders from Microsoft, called on other CEOs and world leaders to join the first anti-corruption data analytics consortium, based on the BrewRIGHT platform. The consortium will help participants better detect corruption and protect against it without revealing underlying company data". <https://www.ab-inbev.com/news-media/innovation/how-brewright-is-rooting-out-corruption-at-ab-inbev-and-beyond/> accessed 21 March 2022.

[65] Vivienne Brand, 'Corporate Whistleblowing, Smart Regulation and Regtech: The Coming of the Whistlebot?' (2020) 43(3) University of New South Wales Law Journal 1, 2.

[66] Dimitrios Kafteranis, 'Can Artificial Intelligence Replace Whistle-Blowers in the Business Sector?' (2019) 3 International Journal of Technology Policy and Law 160, 161.

[67] Kieran Pender, Sofya Cherkasova and Anna Yamaoka-Enkerli, 'Compliance and Whistleblowing: How Technology Will Replace, Empower and Change Whistleblowers' in Jelena Madir (ed), *Fintech Law and Regulation* (Elgar Online, 2019) 327. See for instance the EU Directive 2019/1937 on the protection of persons who report breaches of Union Law.

[68] Brand (n 65) 2 and Christopher Woolard, 'The FCA's Regional FinTech Engagement' (Speech, Leeds Digital Festival, 26 April 2017).

[69] Pender, Cherkasova and Yamaoka-Enkerli (n 67) 337.

[70] ibid. See also Kalliopi Zouvia, 'Artificial Intelligence and Whistleblowing: Can A.I. Be Useful for Whistleblowing Processes?' (2020) 2844 CEUR Workshop Proceedings. This is also referred to as "First generation RegTech" to indicate technology that assists and empowers whistle-blowers. Brand (n 65).

with an "AI whistle-blower" or an "algorithmic whistle-blower."[71] They will be briefly addressed in turn.

a) Enhanced protection for whistle-blowers by technology.

One of the main issues for employees that decide to blow the whistle about an illegal behaviour of their company is the fear of retaliation, which comes as a consequence for being identified when anonymity cannot be properly ensured.[72] In order to deal with this problem, web portals that use encrypted solutions were developed. Users can create an account with a random name and submit a report form.[73] Chatbots embedded with natural language processing technology can interact with and help whistle-blowers to submit their allegations by providing instructions and avoid the risk to have incomplete reports.[74] AI can also be used to analyse structured and unstructured data and extract relevant information from a whistle-blower's report, which will help to assess the truthfulness of whistle-blowing allegations.[75] Finally, blockchain is considered the most promising technology for whistle-blowers, given the possibility of remaining anonymous while providing the authority with the advantage to further contact the whistle-blower to ask for additional information.[76] Blockchain also offers the possibility of compensating whistle-blowers through smart contracts, in which anonymity is still secured and reward is provided with the use of cryptocurrency once all the necessary conditions are satisfied.[77]

b) Algorithmic Whistle-blowers

Given the potential of AI to take over tasks traditionally performed only by humans, suggestions have been made to develop an "AI whistle-blower" for compliance purposes in the financial sector. AI whistle-blowers may be able to generate internal reports that flag companies' wrongdoing, based on intelligent data analysis.[78] An algorithm could be trained to access data stored by the company and recognise wrong activities that would automatically be reported internally to the higher level.[79] This would help raise awareness before any investigation from regulators starts and take the necessary steps to end illegal

71 Also referred as "Second generation RegTech". Brand (n 65); Kafteranis (n 66); Pender, Cherkasova and Yamaoka-Enkerli (n 67). Adam Waytz, 'Why Robots Could Be Awesome Whistleblowers' *The Atlantic* (2014), <https://www.theatlantic.com/business/archive/2014/10/why-robots-could-be-awesome-whistleblowers/381216/> accessed 20 January 2022.

72 Pender, Cherkasova and Yamaoka-Enkerli (n 67).

73 ibid 338 ss.

74 Zouvia (n 70).

75 ibid.

76 Pender, Cherkasova and Yamaoka-Enkerli (n 67) 340.

77 ibid.

78 Kafteranis (n 66).

79 ibid.

behaviour internally. It would be an ideal "win-win" solution for the private side and also for regulators as it would reduce the burden of external enforcement actions.[80]

4.3. An AI whistle-blower as a private enforcement tool in competition law

Similarities between the financial sector, which pushes for better compliance, and competition enforcement are evident. In both cases, wrongdoings, whether corruption, bribery, or competition infringements may lead to high fines and criminal charges for individuals.[81] In both cases, investing in compliance programs could benefit a company that may be able to detect at an early stage the problem and deal with it internally, saving time consuming and costly external investigations. An effective compliance program could also be a way out for a company in case wrongdoings would happen anyway.[82]

In competition law enforcement, technology can as well empower and better protect whistle-bowers that wish to report an anticompetitive practice and remain anonymous.[83] This paper aims to provide food for thoughts for implementing an AI or algorithmic whistle-blowing tool as part of a company's compliance program, that would be able to report internally anticompetitive wrongdoings, along the same lines of what has been suggested in the financial sector within the RegTech regime.

In the financial sector, some concerns seem to row against developing an AI whistle-blower. Firstly, it is assumed that AI, at least in the present state, as a narrow AI,[84] would not be able to recognize and report immoral actions.[85] Secondly, an AI may risk wrongly reporting a company's perfectly legal activities. This could damage the reputation and image of a company and waste time and resources in hours and hours of internal investigations on what at the end it reveals to be a legal behaviour. This is a consequence of AI limits when discretionary decisions should be made.[86] In fact, its subcategory of machine learning is well-suited to replace human administrative tasks based on a series of steps, but unable to provide judgments where exceptions and individual circumstances

[80] Brand (n 65).

[81] In the field of competition law, some jurisdictions impose criminal charges for competition infringements, for instance the ACCC.

[82] For instance, some jurisdictions recognize and reward a genuine compliance program. Among others, Australia, Brazil, Canada, Italy and Germany give credits for compliance. OECD (n 50). On the other hand, in the financial sector, "section 7 of the UK's Bribery Act 2010 – one of the strictest examples of international anti-bribery legislation – makes the failure of an organisation to prevent bribery an offence. However, it is a defence under section 7(2) for the organisation to 'show that [it] had in place adequate procedures designed to prevent' such conduct". Pender, Cherkasova and Yamaoka-Enkerli (n 67) 333.

[83] The European Commission has put in place since 2017 a web portal based on an "intermediary's encryption tool" that aims to ensure anonymity <https://ec.europa.eu/competition-policy/cartels/whistleblower_en> accessed 21 March 2022.

[84] See for instance Rembrandt Devillé, Nico Sergeyssels, and Catherine Middag 'Basic Concepts of AI for Legal Scholars' in Jan De Bruyne and Cedric Vanleenhove (eds), *Artificial Intelligence and Law* (Intersentia 2021).

[85] For instance, the LuxLeaks scandal "did not entail illegal acts but obscure legal practices that were considered immoral by society" Zouvia (n 70) 3.

[86] Brand (n 65).

need to be carefully weighted.[87] Furthermore, it is believed that, given the complexity of ethical implications around the whistle-blower universe, it is unlikely that an AI would completely take over on whistle-blowing tasks, but a more plausible scenario would be to have AI and human interaction.[88]

Some of these concerns are not unrelated to competition law. However, an AI whistle-blower as part of a company compliance program could be implemented to report anticompetitive practices of algorithms, such as algorithmic discrimination or algorithmic collusion, eliminating the problem of dealing with human actions. This could be implemented whether an algorithm would define a strategy by itself (even if, at the moment, no commercial evidence is available) or under the direction of a human whose aim is to collude. A machine learning system could be trained to discern wrong behaviours from competitive legal practices and raise internal awareness at the managerial level before any external investigation begins.

AI as a compliance tool could even be imposed in some risky areas where algorithmic solutions replace some of the business strategies. As seen in the previous section, companies could be more or less aware of the risks and implications that algorithms could create for competition and consumer welfare. This is even more evident when technical solutions may be delegated to a third-party provider, giving rise to the risk of the so-called hub-and-spoke scenario.[89] In such a case, implementing a sophisticated AI tool, like an AI whistle-blower, that is able to flag possible algorithmic collusion between clients of the same IT provider may be beneficial in order to raise awareness among companies that could then decide on a different strategy before it is too late. However, imposing an AI whistle-blower as a mandatory compliance tool would raise some practical challenges. First of all, imposing a compliance system as such could be seen as an "over-enforcement" act that may lead to the unwanted effect of "dampen AI progress".[90] In fact, having "a thriving AI developer ecosystem is presumed to be vital to the ongoing advancement of AI-based technologies and capabilities".[91] It is therefore important that companies will continue to invest in disruptive technologies without fearing that they would need to allocate their resources also for implementing sophisticated enforcement measures, which could have a negative impact in their investment plans. However, a balance between the need for AI progress and a sound antitrust system should be struck.[92] Furthermore, in order to impose an AI whistle-

[87] ibid. In this regard, see also Jennifer Cobbe, 'Administrative Law and the Machines of Government: Judicial Review of Automated Public-Sector Decision-Making' (2019) 39 Legal Studies 636; Herwig C.H. Hofmann, 'An Introduction to Automated Decision-making (ADM) and Cyber-Delegation in the Scope of EU Public Law' (2021) Indigo Working Paper.

[88] Brand (n 65) 17.

[89] OECD (n 1).

[90] Lance B. Eliot, 'Antitrust and Artificial Intelligence (AAI): The Antitrust Vigilance Lifecycle And AI Legal Reasoning Autonomy' (2020) ArXiv abs/2012.13016.

[91] ibid., 2.

[92] It is assumed that "the impact of antitrust on AI does not necessarily need to be in one direction only. There is a possibility that antitrust enforcement, or the lack thereof, could accelerate the progress of AI. Likely, the use of antitrust enforcement is bound to have both an encouraging effect on the AI innovation ecosystem and simultaneously a dampening effect, dependent upon how the antitrust efforts are guided and utilized" Ibid. 9.

blower, competition authorities would need to design *ad hoc* rules and a monitoring system to make sure that companies comply and efficiently employ such an AI private enforcement tool. This would create problems in terms of which rules should apply, and which monitoring procedure should be enforced. If at the present state competition authorities are not enough equipped to check upon companies' algorithms that might infringe competition law, how could they have instruments for imposing and checking another AI system, even if developed for enforcement purpose?[93] In this regards, two main solutions could be envisaged.

First, competition authorities could directly provide the enforcement tool for companies: either by designing themselves an AI whistle-blower, tested in sandboxes for example[94] (this if and when they would have enough resources for hosting such projects); or by designating a third-party provider in charge of creating an AI whistle-blower able to detect potential anticompetitive algorithmic infringements that private companies would have to mandatory apply. This solution could have some advantages in terms of Intellectual Property (IP) rights of the AI system's owner, because either it would be their own tool (as in the first hypothesis), or it would be delegated to a third party whose IP rights could be covered under licencing agreements (as in the second hypothesis). In those cases, enforcers would not have to face the problem of asking companies to disclose their property algorithms, protected by IP rights.[95]

Second, another possible solution, often discussed in the research community for monitoring companies' algorithms, could be to develop an auditing procedure (so-called auditing algorithms[96]) also for AI whistle-blower systems.[97] In this case, competition authorities would need to have the necessary tools and a sound procedure for applying an efficient auditing procedure to AI systems.[98]

---

93 Ariel Ezrachi and Maurice E Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-driven Economy* (Cambridge Mass. London: Harvard U, 2016). "[T]he current antitrust tools will be inadequate in prosecuting and remedying some of our anticompetitive scenarios. The dynamic has changed in many markets – competition as we know it has given way to new forms of rivalry. […] the real issue is designing new tools to address the new problems. […] we must be open-minded to new enforcement instruments". 218.

94 ibid. Sandbox is "a controlled environment that tests [algorithms'] operation". 231.

95 In literature, this is usually related to the problem of "algorithmic opacity" and one form is called "intentional opacity, where the system's workings are concealed to protect intellectual property". Cobbe (n 87) 638-639.

96 Ezrachi and Stucke (n 93). See also the Digital Regulation Cooperation Forum (DRCF) 'Auditing algorithms: the existing landscape, role of regulators and future outlook' (2022), according to which "[a]lgorithmic auditing refers to a range of approaches to review algorithmic processing systems. It can take different forms, from checking governance documentation, to testing an algorithm's outputs, to inspecting its inner workings. Audits can be undertaken by external parties appointed by the organisation, or by regulators, researchers or other parties carrying out an audit of a system on their own initiative. Audits can be done for the purposes of internal assurance, as a route to signalling transparency and establishing trust with users or other parties that are affected, or they can be done to establish whether a system may comply with regulatory requirements. The style and depth of audits will vary depending on the nature and size of risks, the context in which algorithms are deployed and existing regulatory requirements. Algorithmic audit differs from traditional financial audit, which is already well established, professionalised and regulated along clearly defined parameters".

97 ibid.

98 For instance, "Regulators could establish principles for best practice, including what organisations need to disclose about their systems and to whom, and they could assist with the development of audit standards, exploring when they are well placed to set principles or standards themselves and when they may look to be a

A mandatory AI whistle-blower as a private enforcement tool would therefore create problems in terms of monitoring companies' AI systems, which would mirror the struggle that competition authorities currently have in reverse engineering pricing algorithms to understand whether or not they are infringing competition law. A more suitable approach could be for competition authorities to recommend companies to put in place a robust AI whistle-blower to detect potential algorithmic wrongdoings, especially for those undertakings that already use their own AI systems for other decision-making processes. In this context, it would be desirable for competition authorities to set specific guidelines and recommendations and to encourage companies that have already invested in AI technologies to use their resources also to develop an AI as a compliance or monitoring tool against possible competition law infringements by their algorithms.

4.3.1. Why an AI whistle-blower could succeed in competition law

Compared to the financial sector, where wrongdoings have often been uncovered by whistle-blowers,[99] in competition law, the EU Commission mostly rely on its leniency program.[100] A company is incentivized to come forward with proofs of being involved in a cartel in exchange of fully or partial immunity.[101] The Commission has also implemented a web portal based on encrypted messages for external whistle-blowers, where complaints about an anticompetitive behaviour can be brought to the attention of the Authority to start a possible investigation.[102]

In the financial sector, bribery, corruption, fraud, and money laundering are all actions that can be easily recognized as criminal infringements by an employee or in general by a human being, sometimes because they are simply "immoral". Everyone knows more or less what a bribery or corruption are. In this context, a human whistle-blower would be able to identify and eventually report a corporate crime. As already explained in the previous section, technology comes to play to enhance human whistle-blower protection, by guarantying anonymity against the fear of retaliation or of losing their job. This is the scenario mostly envisaged: technology and humans working together under the RegTech regime.[103]

On the contrary, in the field of competition, employees that may want to report a wrongdoing need to be aware that their company is infringing antitrust law, which means

facilitator". Ibid., 3. Ezrachi and Stucke (n 93) assumed that "the audit route may become feasible as technology and enforcers' proficiency develop" as "[o]ne risk is that the government will remain several steps behind. Competition authorities may have a difficult time overseeing firms' design and development of sophisticated algorithms". 231.

99 See for instance scandals on tax evasion and tax optimization (Panama Papers and LuxLeaks), data misuse (Cambridge Analytica), money laundering (Danske Bank), in Pender, Cherkasova and Yamaoka-Enkerli (n 67) 327 and Kafteranis (n 66) footnote 17.

100 Ysewyn and Kahmann (n 2).

101 See for instance <https://ec.europa.eu/competition-policy/cartels/leniency_en> accessed 1 March 2022.

102 See for instance <https://ec.europa.eu/competition-policy/cartels/whistle-blower_en> accessed 1 March 2022.

103 Brand (n 65) 17.

that they need to know principles of competition law.[104] A study demonstrated that employees, and even managers are not aware of what competition law is, and neither a cartel.[105] This means that an employee would probably not be able to fully recognize an anticompetitive behaviour and therefore an infringement of competition law. In this scenario, how could they use a whistle-blower internally within the company? Following this line of thought, in competition law, an AI whistle-blower (as a substitute of a human) could be more suitable than in the financial sector, where wrongdoings can be well recognized by humans (considering the high number of scandals uncovered through whistle-blowers).[106] In competition law, an AI could be trained to internally recognize anticompetitive behaviour of a company, especially when algorithms already take over some of their strategical decisions, which makes wrongdoings even more difficult to be identified by a human.

4.3.2. Ethical problems of an AI whistle-blower

Concerns and ethical problems should also be taken into consideration in the field of competition law. Privacy and data protection are among the main concerns when AI's big data analysis is involved.[107] The need to enhance transparency with AI may come at the cost of privacy and data protection. In fact, AI can have access to huge amounts of data and extract meaningful information that can disclose illicit behaviours of a company.[108] At the same time, AI risks disclosing data and information that do not have any evidentiary value but are related to employees and disclose other confident information which would result in a breach of privacy and personal data.[109] Would an AI be able to discern between data that should be disclosed and flagged as relevant for the company and information containing personal data that should fall outside its scope?[110]

Another problem that AI systems often display is their "black-box" character. Accordingly, this would raise problems for understanding the reasons for a decision taken by an AI and its logic, which would be necessary in order to decide whether the outcome is reliable and the system (with or without human input) infringes competition law.[111] This may lead to the paradox of having an AI monitoring or explaining another AI that delivers an outcome that is obscure to the decision-maker.[112] As a result, this might lead to the consequence of cutting the human out of the loop as he/she would need to purely

[104] Jones Day, 'European Commission launches Competition Law Anonymous Whistleblower Tool' (Commentary April 2017). See also OECD (n 50) according to which most people in a company are not aware of competition infringement, especially at the managerial level, 22 ss.

[105] OECD (n 50).

[106] Pender, Cherkasova and Yamaoka-Enkerli (n 67).

[107] See for instance Giovanni De Gregorio and Sofia Ranchordas, 'Breaking down Information Silos with Big Data: A Legal Analysis of Data Sharing' in Joe Cannataci, Valeria Falce and Oresto Pollicino (eds), *Legal Challenges of Big Data* (Edward Elgar 2020).

[108] Pender, Cherkasova and Yamaoka-Enkerli (n 67) 329.

[109] ibid.; Kafteranis (n 66) and Brand (n 65).

[110] Kafteranis (n 66).

[111] Pender, Cherkasova and Yamaoka-Enkerli (n 67).

[112] Deng (n 36). See also Clément Henin and Daniel Le Métayer, 'A Framework to Contest and Justify Algorithmic Decisions' (2021) 1 AI and Ethics 463.

trust and rely on technology without the possibility of exercising any supervisory power. This, however, would bring the discussion outside the scope of this paper, but further research is needed in this field.

Another pitfall is quite obvious: would a company have an interest in implementing an AI whistle-blower? For instance, in the UK, in the financial sector, a company can demonstrate to have put in place a sound compliance program as a defence.[113] In competition law, could the implementation of an AI monitoring tool save a company from liability? Not all competition authorities reward firms for having established a compliance program (e.g. the EU Commission), mainly because an infringement of competition law shows that the program was not efficient enough to prevent a wrongdoing.[114] Even if this tool could be imposed or recommended by competition authorities, how would a company use it? They may use it as a façade, only to demonstrate that they have put a program in place, but without using it as a real monitoring or as a whistle-blower tool. In this scenario, authorities may nevertheless ask the company to provide documents of the process for implementing the AI system (as it has been suggested for making AI accountable) in order to prove their robustness and accuracy, as previously considered.[115] Ultimately, implementing such tools could benefit companies that want to invest in compliance programs.

5. CONCLUSIONS

In a digital era where decisions are more and more delegated to sophisticated algorithms whose "mind" is difficult – if not impossible – to read and interpret, not only enforcers, but also companies should be aware of the potential risks for consumer welfare and competition. Despite the countless benefits that technology brings to society, concerns should also be addressed. Competition authorities have only taken the first steps into developing their own AI arsenal in the fight against algorithmic infringements. However, it is believed that enforcers would be able to take full advantage of the potential offered by AI in the near future.[116] Behaviours that would traditionally fall outside the scope of competition law, such as tacit collusion or parallel conduct, would assume a different connotation when technology is involved. Theories of harm might evolve to include such practices within the scope of competition enforcers' actions.[117]

Companies interested in developing algorithms for maximising their profits should be aware of their potential risks. An infringement of competition law might result in high fines and even criminal liability in some jurisdictions. Regulators welcome compliance programs as a private enforcement tool. Companies should take advantage of technologies not only to increase their revenues, but also to avoid any conscious or unconscious breach of competition law that their algorithms may cause. Given the similarities with the financial sector, where RegTech solutions have become an efficient

[113] Section 7(2) of the UK's Bribery Act 2010 (n 82) and Pender, Cherkasova and Yamaoka-Enkerli (n 67) 333.

[114] OECD (n 50).

[115] Section 4.3 of this paper. See also Cobbe (n 87) and Hofmann (n 87).

[116] Schrepel (n 45).

[117] Ezrachi and Stucke (n 8).

mean for regulatory compliance and whistle-blowers have started to benefit from technological innovations, they should inspire competition compliance programs. AI, Big Data and machine learning could make companies' compliance programs more efficient, whether in the form of AI monitoring tools, screening tools, or AI whistle-blowing that would internally report potential anticompetitive behaviours of a company and its algorithms. What is certain is that solutions for a better synergy between the two sides of the same coin, i.e. benefits and risks of technology, should also be developed by companies at the private level, before competition authorities trigger any investigation. An AI whistle-blower for competition purposes could be an efficient help, and a tool that could be looked into in the future of competition law enforcement.