Revista de Economia Contemporânea

REC

Revista de Economia Contemporânea (2019) 23(2): p. 1-19
(Journal of Contemporary Economics)
ISSN 1980-5527
http://dx.doi.org/10.1590/198055272328
elocation - e192328
https://revistas.ufrj.br/index.php/rec | www.scielo.br/rec

Articles

ALGORITHMS AND BIG DATA: CONSIDERATIONS ON ALGORITHMIC GOVERNANCE AND ITS CONSEQUENCES FOR ANTITRUST ANALYSIS

Marcela Mattiuzzo[a]

[a]Master in Constitutional Law at USP and partner at VMCA Advogados. Sao Paulo, SP, Brazil. ORCID: https://orcid.org/0000-0001-5641-1130.

Manuscript received on 2018/05/10 and accepted for publication on 2019/05/15.

ABSTRACT: This paper aims at presenting the recent rise in the use of algorithmic systems, the move by policy makers towards fighting potential harmful outcomes that may arise from the use of such tools, and the consequences of such policy proposals for antitrust. It is organized into five sections: the first introduces the topic; the second delves deeper into the expansion of algorithmic use in the data-drive economy; the third part presents the policy solutions usually put forward by the literature and by policy makers to fight harm; the fourth discusses the implications of such proposals for antitrust; finally, the fifth section concludes the paper.

KEYWORDS: big data; algorithms; competition; antitrust; algorithmic governance.

JEL CODES: L4; K2.

Corresponding Author: Marcela Mattiuzzo
E-mail address: marcela.mattiuzzo@usp.br

ALGORITMOS E *BIG DATA*: CONSIDERAÇÕES SOBRE GOVERNANÇA ALGORÍTMICA E SUAS CONSEQUÊNCIAS PARA A ANÁLISE ANTITRUSTE

RESUMO: O presente artigo visa apresentar o crescente uso de sistemas algorítmicos em nossa sociedade, o movimento que objetiva combater possíveis resultados prejudiciais advindos desse uso, e as consequências de tais propostas para o antitruste. Para fazê-lo, o texto é dividido em cinco etapas: a primeira introduz o assunto, a segunda aprofunda o movimento de expansão algorítmica na economia de dados, a terceira apresenta as propostas geralmente debatidas pela literatura e por atores para combater os resultados indesejados, a quarta discute as implicações de tais propostas para o antitruste, e a quinta conclui o artigo.

PALAVRAS-CHAVE: *big data*; algoritmos; concorrência; antitruste; governança algorítmica.

1. INTRODUCTION

The rise of Big Data, the use of analytics, and the importance of algorithms have opened new doors for the market and for the public sector, but they have also raised several legal challenges. Companies such as PredPol, which 'provides each law enforcement agency with customized crime predictions for the places and times that crimes are most likely to occur' have their entire business based on algorithmic systems.[1] The same goes for apps such as My Discount, whose purpose is to provide personalized discounts for clients registered at *Pão de Açúcar* and *Extra*, two Brazilian supermarket chains, based on their purchasing pattern. The suppliers pay all discounts, in exchange for customers' profiles.

The topic has been brought to the attention of many jurisdictions. In Europe, the High-Level Expert Group on Artificial Intelligence was created to advise the European Commission on issues regarding the challenges and opportunities of artificial intelligence (AI), and also to draft ethics guidelines for the use of AI in the Union. In the United States of America, the Federal Trade Commission has been carrying out hearings to discuss such challenges. In Australia, the government is investing to strengthen capabilities in AI and machine learning, including AI Ethics Framework.

Likewise, scholars have been looking for solutions that can simultaneously maintain the benefits brought about by these tools and minimize the problems they create. The solutions usually put forward include bringing transparency and accountability to algorithms, as well as prohibiting their use in certain circumstances or under specific scenarios. The claim is that citizens and costumers should be aware of how algorithmic systems target them, be their ultimate goal to sell advertising, to filter curriculums for job interviews, or to decide which area in a city deserves more policing. Because targeting now determines so much of daily interactions, running from professional opportunities to the credit lines one may be able to get, algorithms – or the companies that designed them – should also be somehow accountable for the outcomes they provide.

The reasons for concern are fairly straightforward: first, results provided by algorithms have a *façade* of objectivity, which runs from their use of mathematics. Nevertheless, as Kate Crawford (2013) puts it, numbers cannot speak for themselves: 'Data and data sets are not objective; they are creations of human design. […] Hidden

[1] For the purpose of this article, algorithm and algorithmic systems will be treated as synonyms. Also, the definition of 'algorithm' is simply that of a set of rules that takes given inputs and transforms them into outputs, by following a certain process.

biases in both the collection and analysis stages present considerable risks and are as important to the big-data equation as the numbers themselves'. Current algorithmic systems are mostly concerned with finding correlation in data, not causation – and I do not claim such use is incorrect or irrelevant, merely that if one interprets correlations as causations, and fails to account for the limitation of correlations, issues may arise.

Second, even if we assume algorithms may overcome the issue of correlation *vs* causation – which they may – there is one other aspect algorithmic systems are far from being able to grasp: fairness. What separates humans and machine in this sense is the human ability to make nuanced judgement calls, and thus to exercise or put in practice some form of justice. Algorithms, as efficient as they might be, still lack on this front.

Crime prediction is a fertile terrain for exemplifying the objectivity distortion, and its impact for fairness. Understanding which crimes are considered in the algorithms' analysis is an essential step in analyzing this tool and its accurateness. Are white collar crimes included in the model? Will the model focus on petty crimes, or will it rather focus on violence? These questions are determinant for us to understand what the system will truly be predicting. The second issue is with the data that informs the model – its inputs. The universe of crimes committed is certainly larger than the database of crimes registered by the police, thus to properly predict crime one should have in mind that if the database used by the algorithm is solely that of the police, it will necessarily be partial.

Assuming this database is completed both in the sense that it encompasses all forms of crimes and represents all crimes committed in the past leads to the risk of self-reinforcement (or of a self-fulfilling prophecy). If the available data is largely concentrated in some areas of a city, and the police force are directed towards those areas, they will likely find more crimes in the region, reinforcing the algorithm's original claim. However, that does not mean crime would not be found at similar rates elsewhere, it simply means that by spending more time and effort in a given location, police officers were able to find more irregularities in that very location.

The conclusion put forward by some authors, especially those concerned with discrimination and equality, is that some form of transparency or accountability is needed, and perhaps that the current use of algorithms should be prohibited altogether in specific circumstances. One can easily see why the proposals have room to flourish, but it is also relevant to note these solutions, however tempting, pose challenges, several of which are directly relevant to antitrust.

Signaling towards transparency, for example, could create challenges for the companies responsible for developing algorithmic systems, for some forms of transparency could undermine the secrecy of their models, which is precisely their source of differentiation and income. If algorithms are used for online advertising purposes, or for pricing of products of any kind, transparency can also open up space

for collusion – or forms of parallelism that may shift authorities' current understanding of how such conduct should be analyzed under antitrust laws. Requiring accountability would create a whole new set of issues. Who is to be responsible for the outcome, the company that created the algorithm, the institution that now uses it, the engineers responsible for developing the model, or their superiors? Placing liability on one individual or the other will certainly have an impact on prices.

The goal of this paper is to provide initial ideas on how to address the challenges faced by antitrust authorities and scholars regarding the solutions usually put forward for the issues algorithms present in other spheres and the harm they may cause individuals. I will do so by briefly presenting the expansion of the use of algorithms in several areas and for different purposes (Section 1); expanding on the policy solutions generally envisioned by scholars by the literature now known as algorithmic governance (Section 2); clarifying their implications for antitrust practice and enforcement (Section 3); and signaling towards points of conversion for this apparent conflict (Section 4).

2. BIG DATA, THE EXPANSION OF THE USE OF ALGORITHMS, AND ITS CONSEQUENCES

Equivant, formerly known as Northpointe Inc., a company established in 1989, is, by its own account, a provider of 'automated decision-support software package of industry-leading risk, needs assessment and case management tools' (EQUIVANT, 2019). It is responsible for developing a set of mechanisms that pursue such objectives, the most famous of which is COMPAS, the Correctional Offender Management Profiling for Alternative Sanctions. COMPAS provides users with a decision tree that risk assesses any person's likelihood of committing crimes; its main goal, according to its creator, is to assist the criminal justice system, and more specifically jail administrators, in managing penitentiaries, by enhancing the effectiveness of decision-making.

In 2013, Eric L. Loomis was sentenced to six years in prison and five years of extended supervision for fleeing the scene and operating a vehicle without owner's consent, in a case arising out of a drive-by shooting in the state of Wisconsin, in the United States of America. He appealed of the decision, claiming it violated his due process right, given that the sentence relied on the risk assessment evaluation by COMPAS, which, in his view, obscurely determined the danger he presented to society, leaving him helpless in trying to counter the sentence.[2] In appeal, the case reached the

[2] Loomis claimed the trial court 'referenced the COMPAS assessment and used it as a basis for incarcerating Mr. Loomis', as well as 'used the COMPAS report to justify incarceration'.

Supreme Court of Wisconsin, which rejected Loomis' claims by arguing the sentence 'would have been exactly the same' if the risk assessment tool had not been used. The court also argued that 'risk scores may not be used to determine whether an offender is incarcerated [or] to determine the severity of the sentence' and that it could never be the determining factor in sentencing.

Later on, the case was brought to the Supreme Court, but the writ of certiorari was denied, and the final decision ended up allowing the use of algorithms such as COMPAS in sentencing, though with limitations. The topic is likely to be brought forth again in other cases, as was highlighted in the brief for the United States as *amicus curiae* to the Supreme Court (2017): 'A sentencing court's use of actuarial risk assessments raises novel constitutional questions that may merit this Court's attention in a future case.'

Loomis v. Wisconsin and the use of COMPAS is but one of the many recent examples that have incorporated the use of algorithms and algorithmic systems in decision-making. Some are well known to us, such as Facebook, which uses algorithms to determine the posts that should feature on your news feed. Others are less popular, such as TrueAllele, an algorithm that interprets DNA evidence and helps prepare case reports, aiding analysts in identifying perpetrators in cases when a mix of DNA samples is available, and human forensic science is flawed.

The ever more common use of algorithmic systems, not by chance, follows the rise of Big Data. Though algorithms and Big Data should not be taken as synonyms – an algorithm is but a set of rules that takes given inputs and transforms them into outputs, by following a certain process; on the other hand, the concept of Big Data is quite blurry, for the expression has become sort of a buzz word implying collection of data from different sources, at large pace and in enormous quantities – there is a clear connection between both. Big Data and algorithms together bring about new possibilities, because Big Data 'refers to things one can do at large scale that cannot be done at a smaller one' (MAYER-SCHÖNBERGER, 2015, p. 6). As stated by the Federal Trade Commission:

> As 'little' data becomes 'big' data, it goes through several phases. e life cycle of big data can be divided into four phases: (1) collection; (2) compilation and consolidation; (3) analysis; and (4) use. (…) The term 'big data' refers to a consequence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions. (FTC, 2016)

Mayer-Schönberger and Cukier state that by analyzing a vast amount of data, which sometimes may in fact represent the entirety of data, one can forego exactitude,

and abandon the former search for causality looking instead for correlations. Today's algorithms are able to provide advertisers with the type of costumer that represents the highest return for their investment, based on the selection of characteristics that certain groups of people share. The algorithm, however, is not concerned with the reasons why such groups may be interested in running shoes, leather jackets, or gym hoodies, it is solely interested in pointing out that certain people visit sports department stores more often than others, that those people go to the gym twice a week, that they look for healthy recipes online, and so forth. In the world of data analytics, it is irrelevant why people behave in the way they do, so long as we can access what and how they do it.

As clarified by the Federal Trade Commission of the United States, though the use of algorithms can be beneficial and lead to more opportunities for marginalized groups, it can also lead to discrimination. That is so because

> there is a potential for incorporating errors and biases at every stage – from choosing the data set used to make predictions, to defining the problem to be addressed through big data, to making decisions based on the results of big data analysis – which could lead to potential discriminatory harms. (FTC, 2016)

As clarified by the World Wide Web Foundation, we usually refer to discrimination and discriminatory outcomes in two different ways. Either people may be treated differently despite being the same, or differences between people may be ignored, leading to the same kind of treatment for different individuals. When thinking of discrimination, we often imagine scenarios that fall within the first category: a foreigner can be considered less deserving than a national resident, though they have the same qualifications; a man is paid more than a woman at work though they perform the same tasks, etc. Algorithmic discrimination, however, because of the characteristics intrinsic to Big Data, usually takes the second form. Individuality is left aside, and each individual is taken as part of a group or subgroup, without notice to their particular characteristics, i.e. every black person may be deemed at high credit-risk, despite the vast variety of financial situations this group embodies.

The goal of such targeting is to provide an advertiser with the 'white Caucasian 40-year-olds living in New York City who like Diet Coke' subgroup and a financial institution with the 'married women who own a car and pay their credit card bills on time' club. These categories can then be monetized for different purposes.

Because this article explores the issues the policy solutions usually put forward by the literature on algorithmic governance may pose for antitrust, I am not analyzing the

validity of algorithmic systems in themselves, their merits for public policy,[3] or if they have high false-positive or false-negative rates.[4] With that in mind, the next section will delve deeper into the literature and explain the policy solutions envisioned by authors, governments, and specialists to fight inequality as well as other harms raised by the expansion of the use of algorithms.

3. POLICY SOLUTIONS: THE ALGORITHMIC GOVERNANCE LITERATURE

Issues raising from algorithmic use are not a possibility, but a reality, and researchers, government agencies, and companies alike have been working on ways to counter them. As data scientist and activist Cathy O'Neil puts it, one way to start is by turning to the very people who create algorithmic systems and asking them to use wisely the power invested in them by the models they now yield (O'NEIL, 2016). Two organizations have recently given concreteness to O'Neil's call. The Association for Computing Machinery in the United States (ACM-US) established principles to be followed by engineers, businesses, and government when dealing with algorithms and analytics. So has the Fairness, Accountability, and Transparency in Machine Learning Organization (FAT-ML), which sets forth principles for accountable algorithms revolving around two general concepts: transparency and accountability. The overall idea is to make sure algorithms – and their outputs – are understandable to civilians (and not solely to highly specialized engineers and data scientists) and the responsibility for their decisions is properly handled. Five ideals summarize such objectives: (i) responsibility, (ii) explainability, (iii) accuracy, (iv) auditability, and (v) fairness.

In sum, FAT-ML believes there is 'an obligation to report and justify algorithmic decision-making, and to mitigate any negative social impacts or potential harms' (DIAKOPOULOS and FRIEDLER, 2016). The organization proposes to address such

[3] Though this article will inevitably focus on the issues presented by algorithms, there is no denying they can be beneficial. As stated by the WWF (2017) in their paper on algorithmic accountability, 'The turn towards algorithms in governments – particularly in sectors such as criminal justice, healthcare, safety, fair employment and others – can be seen as part of a greater effort towards evidence- based decision-making and the adoption of open and transparent government principles.' (p. 6)

[4] There is however research aimed at demonstrating failures in algorithmic decision-making, such as the research conducted by ProPublica, which states that algorithms such as COMPAS are biased against blacks, for they 'turned up significant racial disparities (…) In forecasting who would re-offend, the algorithm made mistakes with black and white defendants at roughly the same rate but in very different ways'. Whereas blacks were falsely flagged as high risk and potential re-offenders twice the rate as white defendants, whites were deemed low risk more often than black defendants (ANGWIN *et al.,* 2016).

need by (i) giving a person or persons the authority to deal with adverse effects in a timely fashion, that is, determining someone as the responsible for redressing harm; (ii) making the algorithmic decisions, though not the algorithm itself, understandable by those affected by it; (iii) identifying and correcting such errors, since algorithms are certainly not perfect and may err; (iv) just as other business decisions and methods, coding algorithms in a way that allows a third party to evaluate its functioning – the level of auditability could be as high as to allow for public audits; (v) more stringently connected to discrimination and equality, probing algorithms for discriminatory effects, and making the results of such process available to the public.

Several academics have expressed similar concerns over the years and proposed solutions or paths to be followed regarding the matter.[5] Frank Pasquale (2015) has coined the now famous term black box society to refer to the issues raised by algorithms and automation:

> it can refer to a recording device, like the data- monitoring systems in planes, trains, and cars. Or it can mean a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other. We face these two meanings daily: tracked ever more closely by firms and government, we have no clear idea of just how far much of this information can travel, how it is used, or its consequences.

He advocates for the use of open technology, for the use of public options in technology and finance, and for automated decisions to be intelligible, at least to independent reviewers.

Danielle Citron (2008) follows a similar line. She has focused on the need for technological due process, and more specifically on bringing traditional due process and rule making concerns to the age of automation. She emphasizes: 'Automation is more attractive where the risks associated with human bias outweigh that of automation bias. It is advantageous when an issue does not require the exercise of situation specific discretion'.

Additionally, researchers such as Latzer *et al.* (2014) have identified categories of risk regarding algorithmic selection – manipulation, diminishing variety (echo chambers and distortions of reality), constraints on the freedom of communication and expression, surveillance and threats to data protection and privacy, social discrimination, violations of IP rights, abuse of market power, effects on cognitive capabilities and loss of human sovereignty and controllability of technology – and

[5] Unfortunately, it is not possible to cover all of the literature in this article, primarily because the topic is very current and many new publications arise every day. As such, my focus was on presenting some of the most important ideas that concern the algorithmic governance literature today.

tried to associate these categories to governance alternatives, ranging from less intrusive market mechanisms to more intrusive regulation by state authorities. They summarize their research in the following table:

Table 1 – Selected market solutions and governance measures by categories of risk

	Market Solutions					
Risks	**Demand side**	**Supply side**	**Companies: self-organization**	**Branches: self-regulation**	**Co-regulation**	**State intervention**
Manipulation		X	X	X		X
Bias	X	X				
Censorship	X	X	X			X
Violation of privacy rights	X	X	X	X	X	X
Social Discrimination	X		X			X
Violation of property rights		X	X	X		X
Abuse of market power			X			X
Effects on cognitive capabilities						
Heteronomy						

Source: Latzer *et al.* (2014).

Their work also clearly emphasizes the limits of these alternatives. Any market alternatives focused on consumers, for example, are not particularly useful if algorithms function without explicit consent. Also, if we rely on consumers to identify risks and look for solutions in the market, switching to companies that provide the same kind of service without exposure of their rights, such user must be able to properly identify and understand risk, which is by no means a trivial task. Additionally, alternative services must be available in the marketplace, for if supply of non-discriminatory algorithms does not exist, users have to resign and submit to the existing tools.

Market alternatives focused on businesses, on the other hand, can be hard to implement if their cost of implementation is expressive or if they result in competitive disadvantages. For instance, if a mapping service wishes to protect users' privacy and not collect their location at every time of every day, it may well provide a less efficient service, which consequently may turn users away. A real life example is DuckDuckGo, whose differentiation is based on not collecting sensitive information about users in providing search results.[6] The truth of the matter, however, is that many users are still

[6] DuckDuckGo bases its policy in three pillars: (i) not storing users' personal information, (ii) not storing search history, (iii) not tracking users in any scenario.

unaware of the functioning of search mechanisms (and thus unaware of what data is collected, how, and to what intent), and the reach of DuckDuckGo ends up being limited to some few who are actively engaged in internet privacy discussions.

Latzer *et al.* (2014) also consider the possibilities of self-regulation, but highlight the lack of incentives for companies to proactively engage in regulating their business, leaving this possibility only explored in well-established or high risk segments - advertising, for example, has strict rules regarding pedophilia. Lastly, in addressing state intervention, the authors underline there is little knowledge about algorithms and their risks, which makes any action by the state hard to configure and its effects even harder to predict. In the event of having to choose between type-1 and type-2 errors, governments often prefer to incur in the first kind, and let markets flow without much intervention.

Other authors go a step further and try to find ways to counter discrimination in concrete cases, owing to the legislation in their respective countries. That is the case of Barocas and Selbst (2016), who analyze how to bring the American rules governing antidiscrimination to the specific case of algorithms. They make use of Title VII's prohibition on employment discrimination and on the concepts developed in such context, more precisely the disparate impact doctrine. Their conclusion is that though application of the doctrine is viable, it is not without its hurdles, and "will require a wholesale reexamination of the meanings of 'discrimination' and 'fairness'".

It is worth noting how this discussion has developed in the European Union, one of the regions known to be particularly concerned with the expansion and new developments of the digital economy.[7] With the approval of the General Data

[7] Though the EU is particularly concerned with this topic, other jurisdictions have recently signaled concerned as well. New York City, for example, issued Instruction N. 1696-A (2017), requiring the creation of a task force that shall recommend how to deal with automated decision systems. More specifically, the task force will make recommendations on: "(a) Criteria for identifying which agency automated decision systems should be subject to one or more of the procedures recommended by such task force pursuant to this paragraph; (b) Development and implementation of a procedure through which a person affected by a decision concerning a rule, policy or action implemented by the city, where such decision was made by or with the assistance of an agency automated decision system, may request and receive an explanation of such decision and the basis therefor; (c) Development and implementation of a procedure that may be used by the city to determine whether an agency automated decision system disproportionately impacts persons based upon age, race, creed, color, religion, national origin, gender, disability, marital status, partnership status, caregiver status, sexual orientation, alienage or citizenship status; (d) Development and implementation of a procedure for addressing instances in which a person is harmed by an agency automated decision system if any such system is found to disproportionately impact persons based upon a category described in subparagraph (c); (e) Development and implementation of a process for making information publicly available that, for each agency automated decision system, will allow the public to meaningfully assess how such system functions and is used by the city, including making technical information about such system publicly available where appropriate; and (f) The feasibility of the development

Protection Regulation (GDPR) in 2016, which came into effect in 2018, the EU has introduced specific measures aimed at dealing with automated decision-making. Article 22 of the GDPR sets forth that whenever automated decisions are made, the subject of such decision has the 'right to obtain human intervention on the part of the controller'. As noted by Goodman and Flaxman (2016), '[w]hile the GDPR presents a number of problems for current applications in machine learning they are, we believe, good problems to have'. The authors highlight problems running from the Regulation's understanding of discrimination and its take on the 'right to explanation'. They stress the difficulty in providing algorithms with entirely non-discriminatory outcomes, for '[t]he use of algorithmic profiling for the allocation of resources is, in a certain sense, inherently discriminatory: profiling takes place when data subjects are grouped in categories according to various variables, and decisions are made on the basis of subjects falling within so-defined groups'.

When it comes to explainability, the authors focus on what this concept would mean regarding algorithmic systems and call attention to the fact that

> [s]tandard supervised machine learning algorithms for regression or classification are inherently based on discovering reliable associations / correlations to aid in accurate out-of-sample prediction, with no concern for causal reasoning or 'explanation' beyond the statistical sense in which it is possible to measure the amount of variance explained by a predictor. (GOODMAN and FLAXMAN, 2016, p. 6)

In other words, algorithms are not particularly concerned with finding explanations, but rather on finding correlations, which are nothing but probabilities of events happening in the future the same way they did in the past, and have nothing to do with the *reasons* such events happen the way they do.

In Brazil, the debate is quite recent and has more directly reached the country after the approval of the General Data Protection Act (or LGPD, for its Portuguese acronym). The law establishes a set of principles that govern data protection, including the principle of non-discrimination, or 'the impossibility of data treatment for illicit or abusive discriminatory goals'. Mirroring the GDPR, article 20 of the LGPD also puts forward that 'the data owner has the right to ask for revision of solely automated

---

and implementation of a procedure for archiving agency automated decision systems, data used to determine predictive relationships among data for such systems and input data for such systems, provided that this need not include agency automated decision systems that ceased being used by the city before the effective date of this local law."

decisions based on personal data that affect her interests, including decisions taken to define her personal, professional, consumer, or credit profile, as well as aspects of her personality'. It also prescribes that the data controller must provide, when requested, clear and adequate information regarding the criteria and procedures used to reach the automated decision, observing commercial and industrial secrecy. Many questions remain unanswered, however. It is unclear how the ideas of illicit or abusive discriminatory goals will be interpreted, or what precisely the law will require when it comes to 'clear and adequate' information about automated processes.

How, then, should algorithmic governance be carried out? How should it be implemented so that it can foster goals such as equality, but also protect other objectives and promote other policies? The next section will provide focus on one specific area, antitrust law, and show some of the implications of applying transparency and accountability in light of other public policies.

4. IMPLICATIONS FOR ANTITRUST: SOME IMPACTS OF ALGORITHMIC TRANSPARENCY AND ACCOUNTABILITY TO COMPETITION POLICY

The ideals and principles of algorithmic governance go a long way in providing a much-needed framework for dealing with the matter, but they are by no means the end of the discussion, as they leave many questions unanswered – intentionally so. One of such questions is precisely how to create rules and proceedings that, in addressing issues such as inequality, do not interfere with the structure of incentives of other public policies, such as antitrust.

When inquired about the Loomis case and on the claim that COMPAS was a secret tool that rendered it impossible for defendants to properly understand how they had been risk-assessed, equivant said '[t]he key to our product is the algorithms, and they're proprietary (…) We've created them, and we don't release them because it's certainly a core piece of our business' (LIPTAK, 2017). As Loomis exemplifies, if principles of full transparency were to be followed by businesses, there certainly would be questioning of the validity of such requirements, since providing the subject with vast information on the outcome produced by a given algorithm may render the process less useful or more exposed to manipulation.

Say, for instance, that explainability becomes a well-established requirement when it comes to ad targeting in social networks. That means any social network must make users aware of how it sells ads to companies, meaning which categories of users it is able to target and how such targeting takes place. Certainly, providing users with some information is different from handing your code to competitors, but the way results

are reached is arguably a commercial secret businesses are unwilling to disclose. They may claim that (i) their competitive advantage rests on the bundles of users they are able to target, and providing users with information on what data is collected and how such data is processed to form groups and subgroups could well be the same as providing competitors with their 'Coca Cola formula'; and (ii) they are a private network, which has its own private terms and conditions, and any user who is in the platform has already agreed to have her data collected and processed in a certain way, which means there is no additional requirement to disclose information. This claim is particularly interesting in light of the GDPR, for the Regulation adds the conditions of Article 22 on top of those in Article 7 (users' consent), meaning consent by the user is presumed and *still not sufficient* to comply with the automated decision-making requirements.

The solution to reaching balance between algorithmic transparency and antitrust lies in a more complete and thorough understanding of the idea behind transparency. The literature has already clarified that it is much less important to 'open the black box' and show precisely what happens inside it, and much more useful to focus on why things happen the way they do (DESAI and KROLL, 2017). It is no different from other fields of expertise: when we go to the doctor and she asks for an MRI, we often receive the images of the exam – and have 'full access' to what is wrong with our bodies. However, it is common for the exam to be hard to understand, and, sometimes, impossible. That is why we go back to the doctor and ask for their specialized assessment, who rather than explaining every single detail of the image focuses on explaining what (if anything) is wrong. Similar approaches must be considered for algorithms, especially when it comes to machine learning and dynamic systems, whose processes are hard to analyze even for their own makers.

An ancillary solution can be establishing auditing for algorithms. If it is problematic to share an algorithm's functioning publicly, alternatives of independent or even regulator-led audits could provide a way forward. Companies could provide the necessary information for auditors to understand the workings of their systems, and regulators would then analyze whether that system presents any particular form of harm to citizens. The GDPR has a tool that could be adapted for such purposes, the Data Protection Impact Assessment, and so does the Brazilian LGPD, in the figure of the personal data impact report (art. 5, XVII). Moreover, we should consider the problem of discrimination and bias from the outset, and think about building systems that are antidiscriminatory by design.

Issues more properly related to accountability also arise. It is not immediately clear who should be responsible for redressing harm if algorithms have caused it, nor who

precisely should be held accountable if laws were violated.[8] Should an engineer be fully responsible for having written lines of a code that were later used as part of a system that determines recidivism for individuals in criminal proceedings? Should the company's CEO? Or the company itself? On that regard, and relating specifically to antitrust, the topic that comes to mind is naturally pricing algorithms.

In a paper aimed at tackling the algorithmic collusion discussion, the OECD (2017) puts forward four ways by which automated decision systems can facilitate collusion. It claims algorithms can have the role of (i) monitoring – these programs are focused on surveilling the conduct of economic agents to ensure collusion is carried out; (ii) parallelism – directed towards maintaining collusion by automatizing decision-making processes, 'so that prices react simultaneously to any changes in market conditions, replicating thereby a scenario of conscious parallelism'; (iii) signaling – designed to reveal to competitors the intention to collude;[9] and (iv) self-learning – by use of machine learning, algorithms may learn by themselves that collusion is efficient enhancing, thus achieve such result in a learn-by-doing process (p. 31).[10] The practice 'may include the collection of information concerning competitors' business decisions, data screening to look for any potential deviations and eventually the programming of immediate retaliations'.

In addressing this same matter, Freshfields (2017) lays out four possible scenarios, all of which contain some form of algorithmic interference. In the first, embodied by the David Topkins case (2015), the code is the mechanism for implementing a cartel previously agreed upon by players in the market. The agreement happened just as it would in any regular cartel, and the algorithm was the mechanism to implement, maintain, and monitor the agreement.

The second is the hub-and-spoke scenario, also known to be an issue in other markets where Big Data is not present. The hub, in this case, is an algorithm developed by a given company, which is used by several other companies. Because the system used by several players is identical, the market tends to collusion.[11]

---

[8] The World Web Foundation (2017), for instance, talks about algorithm justice when referring to harm alleviation.

[9] As noted by the OECD, this kind of behavior raises several challenges for antitrust authorities and it is by not clear if it should surmount to a violation.

[10] This part talks about the 'risk that some algorithms with powerful predictive capacity, by constantly learning and readapting to the actions of other market players (who may be human beings or artificial agents themselves), will be able to collude without the need for any human intervention'.

[11] The closest thing to a hub and spoke cartel using algorithms that has surfaced so far is probably the Eturas' case in the European Commission, C-74/14 (2016).

The third instance is very much in line with the OECD's observations pointed out above. It considers the possibility of machine learning applied to pricing algorithms, and the event of the machines reaching coordination without any interference from the developers. It would be a case in which machines learn that the most efficient price allocation is when players reach collusion. The point here is that collusion may be reached without any explicit invitation by any economic agent – and thus there would be no agreement between parties, but between systems.

The forth is even more challenging, for it encompasses a scenario in which there is no collusion, but extremely efficient price parallelism. Algorithms are in a market where transparency is at its fullest, and the machines access such data, adopting prices that maximize their investments and adjusting such prices second by second. Prices may end up being supra competitive, but no collusion, explicit or tacit, ever took place. Perhaps, a recent example that hints at this discussion is the Bundeskartellamt investigation into Lufthansa. The company defended itself against fares hikes by claiming it does not control its pricing algorithms.

When asked about accountability for algorithmic collusion, EU Commissioner for Competition Margrethe Vestager, in a speech at the Bundeskartellamt 18th Conference on Competition (2017), clearly puts that 'companies can't escape responsibility for collusion by hiding behind a computer program'. Likewise, the ACM-US states 'institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results'. In the EU, where cartels are not punished as criminal violations, this statement may be less of a hurdle, but in countries such as Brazil and the United States, where individuals and not just companies are criminally accountable for collusion, the answer is of particular relevance.

Some angles of the debate circle around the effective culpability of individuals for outcomes. In traditional collusion scenarios, it is usually stated that a person does not need to have effectively carried out any action to be punished, but such person must at least have been made aware of the situation – or it must be clear that for the illicit behavior to be carried out, it was imperative for such person to have condoned, which is the case for most high-level personnel. In algorithmic collusion scenarios, should we then hold an engineer accountable for designing part of a code that would later be used in a much larger algorithmic system, one which they do not control and whose design they did not take part in? And in the case of tacit collusion, should the company be responsible for charging supra competitive prices, regardless of the fact that tacit parallelism is not punishable in other industries and when reached through other mechanisms? It seems that, unless aspects of tacit collusion in this industry arise that are as of now unknown, this is a scenario in which punishment would be ill advised.

5. FINAL CONSIDERATIONS

As I hope to have demonstrated throughout this paper, algorithmic systems present a remarkable opportunity for economic and social growth, but not without risk. These risks include, most prominently, the fight against inequality, but touch upon several other areas. When fighting inequality, other ideals and principles will be affected, and one of the challenges of algorithmic governance is to balance all interests adequately. Antitrust is one of the many policies that must be taken into consideration when building algorithmic governance solutions. It is also a field little permeable to concerns that go beyond economic efficiency and harm to consumers in the restricted sphere of competition.[12]

The message that the analysis of this specific interaction between competition policy and algorithmic governance can convey is that we must always have in mind the impacts of our interventions on the structure of incentives of not just one, but several policies, otherwise we risk creating mechanisms that solve a problem, but simultaneously create many others. That is not to say that some concerns cannot be more relevant than others, nor that we cannot on occasion forego the objective of convergence and simply focus on the most pressing objectives – for instance, ensuring equality can often be more important than preserving economic incentives for innovation.

To what concerns antitrust and algorithms, much has yet to surface and the debate will certainly develop in the coming years. What must be kept in mind is simply that convergence on policy is possible, and that fighting inequality can be attained while fostering other goals. Research on how to build convergence is needed, and this article has aimed at presenting the relevance of the debate, as well as some paths that can be explored by future academics.

REFERENCES

ANGWIN, J. et al. Machine bias. *ProPublica*, May 23, 2016. Available at: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>. Access on: May 5, 2019.

BAROCAS, S.; SELBST, A. Big data's disparate impact. *California Law Review*, p. 672, 2016. Available at: <http://www.courts.ca.gov/documents/BTB24-2L-2.pdf>. Access on: May 5, 2019.

[12] Or, at least, it has been so ever since the developments by the school of Chicago in the 1960s. It does not mean, however, that antitrust has failed to incorporate elements other than price into its analysis, but rather that the current antitrust framework tends to consider some important concerns are outside its reach. To give one example, that would be the argument against bringing fake news into antitrust's sphere of influence. Freedom of expression, though extremely relevant, is not to be dealt with by competition authorities.

CITRON, D. K. Technological due process. *Washington University Law Review*, v. 85, n. 6, 2008. Available at: <https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview>. Access on: Apr. 28, 2019.

CRAWFORD, K. The hidden biases in big data. *Harvard Business Review*, April 1, 2013. Available in: <https://hbr.org/2013/04/the-hidden-biases-in-big-data>. Access on: May 5, 2019.

DESAI, D. R.; KROLL, J. A. Trust but verify: a guide to algorithms and the law. *Harvard Journal of Law and Technology*, v. 31, n. 1, 2017.

DIAKOPOULOS, N. et al. *Principles for accountable algorithms and a social impact statement for algorithms*. FAT/ML, 2019. Available at: <https://www.fatml.org/resources/principles-for-accountable-algorithms>. Access on: May 9, 2019.

DIAKOPOULOS, N; FRIEDLER, S. How to hold algorithms accountable. *MIT Technology Review*, November 17, 2016. Available at: <https://www.technologyreview.com/s/602933/how-to-hold-algorithms-accountable/>. Access on: May 7, 2019.

EU - EUROPEAN UNION. *General data protection regulation*. Article 22: automated individual decision-making, including profiling. Privazy Plan, 2016. Available at: <http://www.privacy-regulation.eu/en/article-22-automated-individual-decision-making-including-profiling-GDPR.htm>. Access on: May 5, 2019.

EUROPEAN COMMISSION. Eturas' Case. *InfoCuria*, C-74/14, 2016. Available at: <http://curia.europa.eu/juris/liste.jsf?&num=C-74/14>. Access on: Apr. 9, 2019.

FTC - FEDERAL TRADE COMMISSION. *Understanding algorithms, artificial intelligence, and predictive analytics through real world applications*. FTC, 2018. Available at: <https://www.ftc.gov/news-events/audio-video/video/ftc-hearing-7-nov-13-session-2-understanding-algorithms-artificial>. Access on: May 9, 2019.

FTC - FEDERAL TRADE COMMISSION. *Big data*: a tool for inclusion or exclusion? Understanding the issues. FTC, 2016. Available at: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>. Access on: May 2, 2019.

FRESHFIELD BRUCKHAUS DERINGER LLP. *Pricing algorithms: the digital collusion scenarios*. Freshfields Bruckhaus Deringer LLP, 2017. Available at: <https://www.freshfields.com/globalassets/our-thinking/campaigns/digital/mediainternet/pdf/freshfields-digital---pricing-algorithms---the-digital-collusion-scenarios.pdf>. Access on: Apr. 9, 2019.

GOODMAN, B.; FLAXMAN, G. European Union regulations on algorithmic decision-making and a "right to explanation". *AI Magazine*, v. 38, n. 3, 2017.

KRITIKOS, M. *What if algorithms could abide by ethical principles?* European Union, 2018. Available at: <http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/624267/EPRS_ATA(2018)624267_EN.pdf>. Access on: Apr. 09, 2019.

LATZER, M. et al. Algorithmische Selektion im internet: ökonomie und politik automatisierter relevanz zuweisung in der informations gesellschaft. *Abteilung für Medienwandel & Innovation*, Universität Zürich, IPMZ, Forschungsbericht, 2014.

LIPTAK, A. Sent to prison by a software program's secret algorithms. *The New York Times*, New York, May 1, 2017. Available at: <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?_r=0>. Access on: May 5, 2019.

MAYER-SCHÖNBERGER, V.; CUKIER, K. *Big data*: a revolution that will transform how we live, work, and think. Boston, MA: Houghton Mifflin Harcourt, 2015.

MAZETTO, L. Com descontos especiais, apps do Pão de Açúcar disparam em downloads. *It Midia*, Oct. 3, 2017. Available at: <https://itmidia.com/com-descontos-especiais-apps-do-pao-de-acucar-disparam-em-downloads/>. Access on: May 9, 2019.

NORTHPOINTE. *Northpointe suite*. North Point Inc., 2019. Available at: <http://www.northpointeinc.com/files/downloads/Northpointe_Suite.pdf>. Access on: May 9, 2019.

OECD – ORGANIZATION FOR THE ECONOMIC COOPERATION AND DEVELOPMENT. *Algorithms and collusion*: competition policy in the digital age. Paris: OECD, 2017. Available at: <https://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf>. Access on: Apr. 9, 2019.

O'NEIL, C. *Weapons of math destruction*: how big data increases inequality and threatens democracy. New York: Broadway Books, 2016.

PASQUALE, F. *The black box society*. Cambridge, MA: Harvard University Press, 2015.

PEARCE, R. Budget 2018: Government seeks to boost Australian AI capabilities. *Computer World*, May 8, 2018. Available at: <https://www.computerworld.com.au/article/640926/budget-2018-government-seeks-boost-australian-ai-capabilities/>. Access on: May 9, 2019.

PERLIN, M. W. *Cybergenetics TrueAllele technology enables objective analysis of previously unusable DNA Evidence*. MathWorks, 2013. Available at: <https://la.mathworks.com/company/newsletters/articles/cybergenetics-trueallele-technology-enables-objective-analysis-of-previously-unusable-dna-evidence.html>. Access on: Apr. 9, 2019.

UNITED STATES OF AMERICA. THE NEW YORK CITY COUNCIL. A Local Law in relation to automated decision systems used by agencies. *Legislative Research Center*, New York, Int. No. 1696-A, 2017. Available at: <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0>. Access on: May 7, 2019.

UNITED STATES OF AMERICA. *The United States Department of Justice. U.S. v. David Topkins*. Washington, DC: Department of Justice, 2015. Available at: <https://www.justice.gov/atr/case-document/file/513586/download>. Access on: Apr. 9, 2019.

USACM - ASSOCIATION FOR COMPUTING MACHINERY US PUBLIC POLICY COUNCIL. *Statement on Algorithmic Transparency and Accountability*. ACM, 2017. Available at: <https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf>. Access on: Apr. 9, 2019.

VIJAYAKUMAR, S. Algorithmic decision-making. *Harvard Politics*, June 28, 2017. Available at: <http://harvardpolitics.com/covers/algorithmic-decision-making-to-what-extent-should-computers-make-decisions-for-society/>. Access on: May 9, 2019.

WISCONSIN. SUPREME COURT OF THE UNITED STATES. *On petition for a writ of certiorari to the Supreme Court of Wisconsin*. 881 N.W.2d 749 (Wis. 2016). Eric L. Loomis v. State of Wisconsin. Jeffrey B. Wall, Acting Solicitor General Counsel of Record. Washington, DC: Department of Justice, May 2017. Available at: <https://www.scotusblog.com/wp-content/uploads/2017/05/16-6387-CVSG-Loomis-AC-Pet.pdf>. Access on: May 9, 2019.

WORLD WIDE WEB FOUNDATION. *Algorithmic accountability*: applying the concept to different country contexts. Washington, DC: WWWF, 2017.