STANFORD
COMPUTATIONAL
ANTITRUST

ARTICLE

Algorithmic Governance in Computational Antitrust—a Brief Outline of Alternatives for Policymakers

Marcela Mattiuzzo* & Henrique Felix Machado**

Abstract. Computational antitrust consists of empowering competition authorities with modern techniques of artificial intelligence (AI), machine learning (ML), big data and associated solutions in the hope of enhancing antitrust enforcement and equipping it to deal with the dynamics of increasingly digitized markets. However, such power may come with risks of crossing the red lines posed by constitutional and public law requirements that limit and balance State discretion, such as fundamental due process rights, equity, and personal data protection. In this article, we explore some contributions from the algorithmic governance literature to help mitigate those risks and safeguard future computational antitrust solutions.

* PhD Candidate at the University of São Paulo. Holds a Master of Laws and a Bachelor degree in Law from the same institution. Partner at VMCA Advogados, a law firm specialized in antitrust and data protection in Brazil. Former Advisor and Chief of Staff to the Office of the President of the Administrative Council for Economic Defense (CADE).

** Master of Laws and Bachelor in Law from the University of Brasília. Currently a Physics undergraduate at the University of São Paulo and an associate at VMCA Advogados. Former technician and coordinator at CADE's General-Superintendence division for competition analysis of infrastructure and regulated markets.

I. Introduction

As computation and digital technologies have developed exponentially since the latter half of the past century, economists and economic theory have tried to keep up via the production of new models and techniques both to study and incorporate such technologies into their analyses. More recently, especially in the past decade (the 2010s), these efforts reached antitrust analysis, which has largely turned to digital markets as one of the most pressing topics in the field's agenda, both in academic discussions and cases brought by authorities. A whole host of concepts and analytical tools have been developed and increasingly applied to assess competitive impacts associated with new features of digital markets, such as the idea of platforms in multiple sided markets,[1] the elucidation of disruptive innovations as a competitive entry strategy,[2] the economic relevance of data and artificial intelligence,[3] and algorithmic and blockchain forms of collusion.[4]

However, paradoxically, antitrust itself is still lagging behind in incorporating digital elements into its own practice.[5] Taking note of this situation, a number of scholars and practitioners have very recently started to devise proposals with the aim of closing the gap. In Eliot's[6] terms, the application of "antitrust to AI" is slowly helping to develop its counterpart, the application of "AI to antitrust." We will refer to this approach, following how some of its proponents have conceived it, as the "computational antitrust" proposition.[7]

Computational antitrust can be thought of as a branch of a broader (and older) strain of legal thought that sees digital technology as a potential ally to law, one that could be employed to enhance, transform, or even substitute traditional legal practice in several (if not all) areas. [8] Correspondingly, computational antitrust's proposition is to make full use of cutting-edge techniques, e.g., artificial intelligence (AI), machine learning, big data, and natural language processing in all domains of antitrust practice.

---

[1] *See* Juan Manuel Sanchez-Cartas & Gonzalo León, *Multisided Platforms and Markets: A Survey of the Theoretical Literature*, 35 J. ECON. SURV. 452 (2021) (for a review of this literature).
[2] *See* Alexandre de Streel & Pierre Larouche, *Disruptive Innovation and Competition Policy Enforcement* (Organisation for Economic Co-operation and Development [OECD], Working Paper DAF/COMP/GF(2015)7, 2015), https://ssrn.com/abstract=2678890 (for a competition policy review and discussion).
[3] *See* MAURICE STUCKE & ALLEN GRUNES, BIG DATA AND COMPETITION POLICY (2016) (seminal book in the field).
[4] *See* ARIEL EZRACHI & MAURICE STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016), stating the problem. For more nuanced approaches, *see* Thibault Schrepel, *The Fundamental Unimportance of Algorithmic Collusion for Antitrust Law*, JOLT DIGEST (Feb. 07, 2020), https://jolt.law.harvard.edu/digest/the-fundamental-unimportance-of-algorithmic-collusion-for-antitrust-law; Emilio Calvano et al. *Algorithmic Collusion: A Real Problem for Competition Policy?*, CPI (Jul. 13, 2021), https://www.competitionpolicyinternational.com/algorithmic-collusion-a-real-problem-for-competition-policy/; *Algorithms and collusion,* OECD, https://www.oecd.org/competition/algorithms-and-collusion.htm (retrieved on September 26, 2021) (the OECD 2017 roundtable on the topic).
[5] *See* Thibault Schrepel, *Computational Antitrust: An Introduction and Research Agenda*, 1 STAN. COMPUT. ANTITRUST 1 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3766960; Lance Eliot, *Antitrust and Artificial Intelligence (AAI): Antitrust Vigilance Lifecycle and AI Legal Reasoning Autonomy*, ARXIV (2020).
[6] *See* Eliot, *supra* note 5.
[7] *See* Schrepel, *supra* note 5.
[8] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2006).

Digital techniques can, of course, be used by law firms, consultancy firms, forensic specialists, and other private actors in antitrust. But the focus of this article—as well as, mostly, computational antitrust—is geared toward the instrumentation of antitrust authorities. Computational antitrust proponents point out various reasons for this, such as their potential for enhancing legal certainty, mitigating human bias, improving the efficiency of agencies, counterbalancing the capacities of digital players, and helping to deal with the sheer volume of data that agencies need to process due precisely to contemporary data-rich digital markets.[9]

In fact, over the past few years, some antitrust agencies have rolled out initiatives to start incorporating digital techniques into their toolset, with many examples ranging from Spanish Comision Nacional de los Mercados y la Competencia's use of encrypted channels to guarantee the anonymity of complaints[10] to the online price monitoring tool devised by the British Competition and Markets Authority.[11] Such a movement is poised to intensify in the coming years, which makes the study of this new field all the more urgent.

In the present article, we turn to an additional specificity that is much more applicable to authorities vis-à-vis private actors: the need to follow a series of principles, rules, and constraints that accompany the government's privileged position as an imposer of rules and binding decisions. Important constraints in this vein are, for example, the rule of law, the due process, and the need to justify decisions, and critics have already started to point this out in the context of computational antitrust.[12]

This means that authorities cannot simply adopt new ways of exerting jurisdiction without first putting in place due precautions that take into account publicly determined values and constraints. However bright the shine of a new technology may be, digital projects by authorities along the lines of computational antitrust may find themselves stranded if they cannot prove their compatibility with constitutional and public law principles and requirements. Therefore, besides the established "antitrust to AI" approach and the more recent "AI to antitrust" proposals, the third strain of investigation may be called for, along the lines of a "governance of AI to antitrust."

In this context, a useful contribution can be made by the fields of technological due process and algorithmic governance applied to the public sector, which have been steadily evolving in the past years to deal with the potential perils and shortcomings associated with the introduction of algorithmic processes to the

[9] Schrepel, *supra* note 5.
[10] Comisión Nacional de los Mercados y la Competencia [CNMC], *La CNMC refuerza el uso de algoritmos y del "big data" en la detección de cárteles y conductas anticompetitivas*, COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA (Mar. 1, 2021), https://www.cnmc.es/prensa/sistema-informantes-competencia-anonimos-sica-chat-cifrado-cnmc-20210301 (Mex.).
[11] *See* Simon Nichols, *Predictive coding: how technology could help to streamline cases*, COMPETITION AND MARKETS AUTHORITY: COMPETITION AND MARKETS AUTHORITY BLOG (July 24, 2020), https://competitionandmarkets.blog.gov.uk/2020/07/24/predictive-coding-how-technology-could-help-to-streamline-cases/. For a more complete overview of initiatives from several authorities, *see* Schrepel, *supra* note 5.
[12] Andreas Von Bonin & Sharon Malhi, *The Use of Artificial Intelligence in the Future of Competition Law Enforcement*, J. EUR. COMPET. LAW PRAC. 468 (2020).

public administration. In other areas of law, major topics have been studied, such as the possibility of abuse of enforcement in predictive policing, discrimination in AI decision-making arising from database quality issues, and employment policies.

It is worth noting that our main goal is to emphasize that neither can we disregard computational antitrust, nor should we ignore algorithmic governance. Both pieces of literature have valid and relevant points, and the main objective should be to find ways of making use of technology while also respecting and observing due process obligations that fall upon public authorities such as antitrust agencies.

With that in mind, after this introduction, we have organized the following pages into four other sections. Section II offers a broad and illustrative overview of computational antitrust proposals while also identifying potential risks. Section III then takes a step back to provide a context of technological due process and algorithmic governance literature, summarizing relevant concepts and ideas that can be helpful to computational antitrust. In Section IV, we try to illustrate preliminary forms of applying algorithmic governance precautions to incipient computational antitrust projects, with a special emphasis on screening techniques. Finally, Section V provides a brief conclusion.

II. Computational Antitrust

In principle, computational antitrust has potential uses in all antitrust domains. Core canonical areas are, of course, included—that is, merger control and investigation of anticompetitive practices—along with other areas of authorities' activities, such as monitoring and enforcement, economic studies, and competition advocacy, as well as policy and improvements in the administration of the authority itself.

The potential application of computational techniques can vary widely based on the problem they are meant to address. This variety in solutions and applications can correspondingly call for different algorithmic governance precautions depending on the case at hand. For example, while the use of a given AI technique to enhance authorities' productivity can be comparably safe, its employment in decision-making could pose substantial legal risks if not used with much care.

Most antitrust agencies had already undergone the first wave of digital transformation when computer technologies were first introduced to be used as writing tools, spreadsheets, websites, databases, and digitalization of proceedings (records and case files). In Eliot's[13] useful classification of the introduction of digital and AI automation technologies to antitrust agencies, this can be seen as a first level of automation, which offers simple legal assistance to authorities. From a technological standpoint, the early introduction of computer technologies paved the way for contemporary computational antitrust possibilities since it allowed for the production of digital, computable data that can now be used as input materials

[13] Eliot, *supra* note 5.

for more advanced techniques. It is worth noting that even this simplest form of automation brought the need to standardize certain procedures, with many agencies issuing new rules to guarantee a safe and transparent transition in compliance with principles and requirements applicable to public agencies.

An already ongoing application of computational antitrust is the continuation of this process to reach increasing levels of automation through the incorporation of more recent technologies that take advantage of the now-abundant volumes of digitized content routinely processed by authorities. Following Eliot's scale, this is leading to the automation of tasks with higher levels of abstraction, such as AI applied to legal reasoning, but still contained within the realm of *legal assistance*—that is, solutions with no autonomy to make decisions.

Some of the most immediate applications in this realm relate to continuous improvements in agencies' internal tasks. For example, in some cases, agencies need to review a large number of documents. Forensic tools are increasingly incorporating AI to help agencies with document review, pre-classifying potentially relevant documents, and filtering documents for later revision by a human analyst.[14] Agencies can also apply AI tools to better understand their own actions, including in administrative areas or core activities such as past cases, which could in turn help to make practices more uniform, recognize hidden patterns, identify areas of concern, evaluate biases or bottlenecks, assist with compliance and guidelines, and other avenues for improvement.[15] Other proposals involve, for example, the use of APIs and blockchain to facilitate exchanging information to and from private parties (e.g., to reply to agencies' RFIs), allowing for large database transfers and ensuring data integrity.[16]

Such efficiency-enhancing tools may still seem simple, but this does not exempt them from carrying potential legal risks. As per the examples above, while obtaining huge amounts of data via APIs may be simple, preventing unnecessary data transfers or guaranteeing anonymity to comply with data protection legislation could pose a greater challenge. Similarly, the automation of monitoring and enforcement of remedies might become technically feasible, but algorithms may need to incorporate due process and fair trial safeguards before applying penalties or allowing for remedy revisions in certain circumstances, following nuanced, internationally recognized best practices and measures.[17]

---

[14] As exemplified by FTC's use of the Relativity forensic tool, which has been incorporating big data and AI tools, and by CMA's use of AI to help filter evidence in the musical instruments probe, where the agency needed to review more than 10 million documents. Nichols, *supra* note 11.

[15] An interesting example is the study by Massarotto & Ittoo, who applied an unsupervised machine learning algorithm was applied to FTC cases from 2005 to 2019 in order to identify underlying patterns of relevant antitrust analysis variables and cluster cases with similar characteristics. *See* Giovanna Massarotto & Ashwin Ittoo, *Gleaning Insight from Antitrust Cases Using Machine Learning*, 1 STAN. COMPUT. ANTITRUST 16 (2021), https://law.stanford.edu/wp-content/uploads/2021/03/Computational-Antitrust-Article-2-Gleaning-Insight-1.pdf.

[16] Schrepel, *supra* note 5.

[17] *See, e.g.,* Int'l Competition Network [ICN], *Merger Remedies Guide* (2016), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2018/05/MWG_RemediesGuide.pdf (which demonstrates the need for custom-designed and negotiated remedy monitoring and revision procedures, due to the fact that "[c]ompetition authorities are unable to control or predict every factor capable of impacting the implementation of remedies").

A much-commented application of computational antitrust is screening, both for helping to identify potentially anticompetitive conducts and relevant mergers whose submission is not mandatory, especially as a tool to prevent killer acquisitions.[18] Many authorities have employed some sort of computational screening tool for several years, in varying degrees of automation and sophistication. Until 2019, the authorities of Brazil, Germany, Mexico, Portugal, Russia, South Korea, Spain, Switzerland, and the United Kingdom employed these tools, as per the French Autorité de la Concurrence and the German Bundeskartellamt.[19] However, traditional screening methods tend to use econometrics, while most recently, AI and machine-learning techniques have been proposed as a promising evolution. Some agencies can tap into the huge amounts of data in the hands of other government or regulatory bodies, which has enormous potential for applying contemporary data processing (even Big Data) techniques.

As a general rule, antitrust authorities tend to have a more reactive profile in their activities, meaning that most cases originate from complaints, leniency applications, or submissions by third parties. As noted by Schrepel,[20] screening automation could lead to authorities developing a more proactive profile in their core functions.

The antitrust authority, however, is usually not conceived as a regulatory agency, so this could merit further discussion on what role exactly antitrust should play. Since in most countries competition law tends to oversee the whole market economy of the respective jurisdiction (or almost that), antitrust agencies ultimately have the potential to concentrate and cross-analyze huge, overarching databases from many fields of an economy, which would invite discussions on their capacity as an instrument of the surveillance state. All sorts of concerns might arise from this, such as data protection issues, the legitimacy of the ontology and analytic models chosen to handle the data, and even the antitrust jurisdiction in broader economic policy issues.

An interesting example is given by Mahari et al.,[21] who propose an early warning system to identify potential killer acquisitions that fail to meet mandatory notification thresholds. Their method was extended from a previous paper by Lera et al.[22] which used data from the eToro Social Trading Platform. In that model, the market would be better conceptualized as a network, i.e., composed of agents and connections between such agents. Network analysis, which has hugely evolved

[18] *See* Rosa Abrantes-Metz & Albert Metz, *Can Machine Learning Aid in Cartel Detection?*, ANTITRUST CHRON. (2018), https://ssrn.com/abstract=3291633; Organisation for Economic Co-operation and Development [OECD], *Summary of the Workshop on Cartel Screening in the Digital Era,* DAF/COMP/M(2018)3 (Sep. 26, 2018), https://one.oecd.org/document/DAF/COMP/M(2018)3/en/pdf; Martin Huber & David Imhof, *Machine learning with screens for detecting bid-rigging cartels*, 65 INT. J. IND. ORGAN. 277 (2019); Schrepel, *supra* note 5; Daryl Lim, *Can Computational Antitrust Succeed?*, 1 STAN. COMPUT. ANTITRUST 39 (2021) https://law.stanford.edu/wp-content/uploads/2021/04/lim-computational-antitrust-project.pdf; Robert Mahari et al., *Time for a New Antitrust Era: Refocusing Antitrust Law to Invigorate Competition in the 21st Century*, 1 STAN. COMPUT. ANTITRUST 52 (2021) https://law.stanford.edu/wp-content/uploads/2021/04/pentland-computational-antitrust-project.pdf.
[19] AUTORITE DE LA CONCURRENCE & BUNDESKARTELLAMT, ALGORITHMS AND COMPETITION (2021).
[20] Schrepel, *supra* note 5.
[21] Robert Mahari et al.,*Time for a New Antitrust Era: Refocusing Antitrust Law to Invigorate Competition in the 21st Century*, 1 STAN. COMPUT. ANTITRUST (2021).
[22] Sandro Lera et al., *Prediction and Prevention of Disproportionally Dominant Agents in Complex Networks,* 117 PROC. OF THE NAT'L ACAD. SCI. 27090 (2020).

from computation, has developed highly non-linear models of network dynamics, such as preferential attachment models,[23] differing strikingly from much simpler energy-based equilibrium-system analogies that underpin the mainstream microeconomic foundations of contemporary antitrust.[24] In Mahari et al.'s[25] particular example, one can infer that network modelling would reach a different conclusion regarding the potential causal nexus between a merger when compared to more linear measures of causality such as the increase in Herfindahl-Hirschman Index (HHI) traditionally used by many jurisdictions.[26]

This example illustrates how screening algorithms can contain methods for evaluating practices and mergers that differ from traditional antitrust criteria. It is even ironic that, after a period of strong rejection of non-linear and complexity methodologies in favor of mainstream marginalist modelling (which have also benefited from econometric computer simulations), antitrust may now be faced with the need to open its theoretical horizons and embrace multidisciplinary perspectives in order to realize the potential of computational solutions successfully.[27] The problem, however, is that for such a change to happen, the new theoretical perspectives must be put to the test and agreed upon by legitimate instances. In some jurisdictions, this could mean the publication of new guideline documents; in others, it could call for changes in case law, internal regulations, or even legislation.

This shows how the boundary between *mere efficiency-enhancing solutions* and *actual decisions* can be tricky. Some productivity tools can bear profound consequences related to the merits of a case and even slip into decision-making territory. In the case of screening algorithms, von Bonin & Malhi[28] illustrate this by making a relevant case for the need to observe minimum legal criteria in the EU for the Commission to initiate complaints. They also note the possibility of an "enforcement bias" effect, that is, an overenforcement "*in certain industries or practices for which data may be more readily available and/or in industries in which a sufficiently broad or deep dataset is not available*" von Bonin & Malhi.[29] A similar argument was developed at length by Sanchez-Graells'[30] analysis of CMA's former

[23] Réka Albert & Albert-László Barabási, *Statistical Mechanics of Complex Networks*, 74 REV. MOD. PHYS. (2002).
[24] PHILIP MIROWSKI, MORE HEAT THAN LIGHT: ECONOMICS AS SOCIAL PHYSICS, PHYSICS AS NATURE'S ECONOMICS (1989).
[25] Mahari et al., *supra* note 21.
[26] Though the HHI is not linear (sum of squares), the increase in HHI – or, more generally, the difference between a pre-merger HHI and a post-merger HHI – can be reduced to a linear formula. *See* Benjamin Dryden, *Quickly Calculate HHI Deltas Using this 1 Weird Trick*, LAW360 (March 4, 2016), https://www.foley.com/en/insights/publications/2016/03/quickly-calculate-hhi-deltas-using-this-1-weird-tr.
[27] To take Mahari et al.'s, *supra* note 21, example once again, contemporary network science, hailed as one of the ingredients of computational antitrust, *see* Schrepel *supra* note 5, is a descendant (of sorts) from the much older "social network analysis" tradition, *see* Linton Freeman, THE DEVELOPMENT OF SOCIAL NETWORK ANALYSIS: A STUDY IN THE SOCIOLOGY OF SCIENCE (2004), a school of structuralist sociological thought whose adoption would be unfathomable to most traditionally-trained neoclassical antitrust economists, but which has already been pursued by non-mainstream economists (thus outside of antitrust) for some decades now. *See, e.g.,* Ronald Burt, STRUCTURAL HOLES: THE SOCIAL STRUCTURE OF COMPETITION (1992).
[28] Andreas Von Bonin & Sharon Malhi, *The Use of Artificial Intelligence in the Future of Competition Law Enforcement*, 11 J. EUR. COMPET. LAW PRAC. 468 (2020).
[29] *Id.*
[30] Albert Sanchez-Graells, *'Screening for Cartels' in Public Procurement: Cheating at Solitaire to Sell Fool's Gold?,* 10 J. EUR. COMPET. LAW PRACT. 199 (2019).

"Screening for Cartels" tool, used in public procurement markets. Such questions bear direct relation to "quality of data" discussions from the algorithmic governance literature as well.

Also, a more general implication of this discussion is that the ontology used in AI classification algorithms—a very frequent use-case—may have an inherent decision-making anticipation component. The issue ironically goes full circle and returns to a "human problem"—which, as Schrepel[31] correctly points out, should continue to pose a significant challenge in the future of computational antitrust despite the latter aiming to pull human intervention out of the equation.

At this point, we are starting to discuss the role of computational antitrust not only as a legal assistant, but also as a *legal advisor* (to borrow Eliot's[32] vocabulary once more), meaning that the AI starts to act at higher levels of autonomy in legal reasoning and decision-making. Though autonomous AI agents are generally understood to be far from becoming concrete and attainable in computational antitrust in the short-run, it is important to understand that pinpointed steps in an automated AI system might already embed autonomous decision-making instances, or at least autonomous legal reasoning.

Earlier than expected, computational antitrust could be met with algorithmic governance challenges such as database adequacy and the need for transparency of programs, algorithms, and systems for the sake of fair trial claims (as pointed out by von Bonin[33]). Of course, the more autonomous computational antitrust legal advisor capabilities become, the more valid will general decision-related claims from the algorithmic governance research community be. This includes, for example, bias and discrimination debates, the possibility of human review, issues regarding transparency of decision-making, and others. It is possible to infer, then, that such discussions will become ever more present as computational antitrust capabilities unfold.

Finally, even if the computational outputs are subject to human review, one might wonder about the effect they will have when considered within their broader human-populated environment. For example, legal assistance tools that prepare pre-filled template decisions and documents, already commercially available in some areas of law, may induce decision patterns even if subjected to review. Just as human-assisted self-driving vehicles may need to comply with standards regarding working conditions and requirements for "drivers,"[34] critics may target antitrust agencies for not providing "safe" or adequate human review environments.

[31] Schrepel, *supra* note 5.
[32] Eliot, *supra* note 5.
[33] Von Bonin & Malhi, *supra* note 28.
[34] *See, e.g.,* controversies sparked by accidents involving supervised semi-autonomous vehicles, such as reported by Chaim Gartenberg, *Safety driver of fatal self-driving Uber crash was reportedly watching Hulu at time of accident*, THE VERGE (June 22, 2018), https://www.theverge.com/2018/6/22/17492320/safety-driver-self-driving-uber-crash-hulu-police-report.

III. Algorithmic Governance and Technological Due Process

It is worth taking a step back from computational antitrust debates in order to look more broadly to the algorithmic governance discussions, for they may be of use to antitrust and to the challenges that could arise as a result of digitization of decision-making in regards to competition law. Algorithmic governance is largely developed on the idea that, precisely because technology is evolving and automation has become more prevalent, if decisions are taken by non-human actors, they should, to some extent, still be accountable. How much accountability will be demanded and to what extent that will influence the building of algorithmic systems itself is an issue open for debate, but the literature on this topic tends to agree that we cannot completely let go of the need for accountability simply because of automation, that is, automation does not equate absolute accuracy nor is it completely devoid of many of the "failures" that are common in human-made decisions, such as discrimination, prejudice, lack of causality, etc.[35] It is true that technology can help us overcome some of these issues, but it is not true that the mere use of technological solutions will automatically erase those problems.

Authors such as Nissenbaum—in what is perhaps one of the first articles written on this topic—have called attention to the fact that it is particularly difficult to ensure accountability of computation, particularly given four characteristics of computer systems, namely:

i. "the problem of many hands," or collective responsibility, which is common because computer systems are usually built by groups rather than individuals, and assigning blame to a group has historically been a challenge;
ii. bugs, or software errors in general, which are characterized as endemic to any complex computerized system, and as such compound the assessment of responsibility;
iii. treating the machine as a scapegoat in order to remove any human responsibility or error; and
iv. the controversy over software ownership, which, if resolved could provide a clearer individual target for accountability debates.[36]

In light of these characteristics, Nissenbaum makes some recommendations to rehabilitate accountability. She understands that "we should hold on to the assumption that someone is accountable unless after careful investigation, we conclude that the malfunction in question is, indeed, no one's fault." Her first suggestion is to separate accountability from liability, since the latter usually equates to determining who should pay whom and how much, whereas the former is centered on the action.

---

[35] Sandra Wachter, et al., *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Nondiscrimination Law and AI,* 41 COMPUT. L. & SEC. REV. (2021) explain what the unique challenge of algorithmic discrimination entails, and also conclude that automating fairness, at least according to the European understanding of what fairness entails, may in fact be impossible.
[36] Helen Nissenbaum, *Computing and accountability,* 37 COMMC'N. ASS'N. COMPUTATIONAL MACH., Jan. 1994, at 73, 72-80.

She further clarifies that, even in the case of collective actions, each individual involved shares in the responsibility for the offense—that one is not directly liable does not make her any less accountable for the outcome, and the author believes that preserving this capacity to identify those who were behind the offensive outcome is paramount. Her second observation addresses the need for a "standard-of-care," or, in other words, "a call for simpler design, a modular approach to system building, formal analysis of modules as well as the whole, meaningful quality assurance, independent auditing, built-in redundancy, and excellent documentation." Her view is that this approach would both incentivize better system design and set high standards for system engineers while simultaneously differentiating between preventable and unpreventable bugs. Lastly, Nissenbaum calls for strict liability for consumer-oriented or large-scale software, which would shift the burden of proof to producers, and require extraordinary measures on their part whenever the system under construction is developed for widespread use.

Following that line, keeping pace with the technological development (which was significant ever since Nissenbaum first offered her insights) and, in order to bring a greater level of concreteness to the debate, groups of scholars have come up with principles that could govern algorithmic decision-making. The Fairness, Accountability and Transparency in Machine Learning Organization (FAT-ML) is one such institution. It has compiled a list of what it believes to be the key principles that should be observed by companies and governments when dealing with algorithms: responsibility, explainability, accuracy, auditability, and fairness.[37] In the United States, the Association for Computing Machinery (ACM) followed a similar path and devised its own principles, adding awareness, access and redress, data provenance, and validation and testing to the list.[38] The OECD has also quite famously proposed its own set of five principles, specifically focused on AI.[39]

Responsibility, according to FAT-ML, relates to the idea that one, in designing algorithmic systems, must consider the people that will be impacted by the decision-making process and as such should to some extent provide mechanisms for redress—both at the individual and societal levels. This idea connects to two other ACM principles: *awareness* and *access and redress*. ACM's principles of *awareness* is mostly focused on raising the algorithm's builders' and users' awareness of the possible consequences of its use, especially regarding the biases that can arise from it. *Access and redress* claims regulators should adopt mechanisms that allow individuals impacted by the decisions made by algorithms to question and repair potential harms. Likewise, the OECD proposes a principle of *accountability* for AI that follows a similar path.

[37] Nicholas Diakopoulos et. al., *Principles for Accountable Algorithms and a Social Impact Statement for Algorithms,* FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY IN MACHINE LEARNING (2021), https://www.fatml.org/resources/principles-for-accountable-algorithms.
[38] Association for Computing Machinery US Public Policy Council [ACM], *Statement on Algorithmic Transparency and Accountability* (Jan. 12, 2017), https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf.
[39] OECD, *Recommendation of the Council on Artificial Intelligence* (2019), https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

As Doshi-Velez et al. put it, the idea of *explanation* (or explainability as the FAT-ML calls it), when applied to decision-making, refers to "the reasons or justifications for that particular outcome, rather than a description of the decision-making process in general."[40] Therefore, what they consider to be an explanation is a "human-interpretable description of the process by which a decision-maker took a particular set of inputs and reached a particular conclusion." It is important to note that explanation is not identical to transparency, for understanding the process by which a decision was made is not the same as knowing every step taken to reach it. The OECD seems to be particularly aware of that difference, for it proposes a principle of *transparency and explainability*, aimed at

i. fostering a general understanding of AI systems,
ii. making stakeholders aware of their interaction with AI systems,
iii. enabling those affected by decision-making to understand the outcomes, and
iv. allowing anyone negatively impacted by AI-systems decisions to challenge such outcomes.[41]

The principle of *accuracy*, according to Diakopoulos and Friedler, means that the "sources of error and uncertainty throughout an algorithm and its data sources need to be identified, logged, and benchmarked."[42] Put bluntly, it is only by understanding the origins and causes of mistakes that one can hope to mitigate them. The ACM expresses a similar notion through the principle of *data provenance*, which states that "a description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process."[43]

The principle of *auditability* is another constant in discussions of algorithmic governance. It entails requiring a third-party review of the method used by the algorithm to reach its conclusions.[44] How this disclosure should be undertaken, and whether it should take place at all in certain circumstances, especially where commercial secrets are involved, is a subject of much debate.

Fairness may be the most obvious if least clear of all the principles proposed. The idea behind fairness is preventing algorithms from reaching discriminatory outcomes. However, determining what constitutes a discriminatory outcome is often challenging. The ACM, without expressly subscribing to the principle of fairness, puts forward the *validation and testing* standard, according to which "[institutions] should routinely perform tests to assess and determine whether the model generates discriminatory harm."[45] The OECD, on the other hand, says that

[40] Finale Doshi-Velez & Mason Kortz, *Accountability of AI Under the Law: The Role of Explanation* (2017) (Berkman Klein Center for Internet & Society working paper on file with Berkman Klein Center Working Group on Explanation and the Law), http://nrs.harvard.edu/urn-3:HUL.InstRepos:34372584.
[41] OECD, *supra* note 39.
[42] Nicholas Diakopoulos & Sorelle Friedler, *How to Hold Algorithms Accountable,* MIT TECH. REV. (2016).
[43] ACM, *supra* note 38.
[44] Christian Sandvig et. al., *Auditing algorithms: Research methods for detecting discrimination on internet platforms* (May 22, 2014), *in* DATA AND DISCRIMINATION: CONVERTING CRITICAL CONCERNS INTO PRODUCTIVE INQUIRY.
[45] ACM, *supra* note 38.

fairness should be coupled with *human-centered values*. The organization also adds a different principle, that of *inclusive growth, sustainable development, and well-being*, which focuses on pursuing beneficial outcomes with the use of AI.[46]

Some authors have tried to bring more clarity to this particular debate when it comes to governmental use of computational tools. Citron's proposal, for instance, is primarily concerned with making sure agencies are equipped with decision-making processes and guarantees that suffice in the world of automation. Her suggestions for technological due process reflect in many ways what other authors claim algorithmic accountability would require in the context of governmental use of machine learning and algorithms in general. She argues that government agencies should adopt the following three practices:

i. maintaining audit trails, which would help comply with notice requirements;
ii. holding hearings to clarify automated systems' fallibility and afford justification from officers for automated decisions on a case-by-case basis;
iii. ensuring transparency and accountability by, specifically (a) making systems' source code public, (b) conducting testing and monitoring by independent agents, (c) involving public participation in the building of systems as much as possible, and (d) refraining from automating policies which have not undergone formal or informal rulemaking.[47]

One should note that Citron's concern with the use of algorithms by the State resonates with criteria put forth by constitutional regimes in many jurisdictions. It is generally true that, in most (if not all) democratic countries, the government has a special need to justify its decision-making, notably if the decision at stake in some way limits or hinders individual rights and freedoms. If that is true, the argument goes, then the Administration cannot hide behind algorithms to avoid that obligation, meaning it cannot let go of its need for justification merely because of the use of computational tools. And here is where the fields of computational antitrust and algorithmic governance converge—in discussing how one can ensure that the technological developments of the first do not disregard the accountability concerns of the second.

[46] OECD, *supra* note 39.
[47] *See* Danielle Citron, *Technological Due Process,* 85 WASH. U. L. REV. 1249, 1305 (2008) ("Audit trails should include a comprehensive history of decisions made in a case, including the identity of the individuals who recorded the facts and their assessment of those facts. Audit trails should detail the actual rules applied in every mini-decision that the system makes. With audit trails, agencies would have the means to provide individuals with the reasons supporting an automated system's adjudication of their important rights.")

IV. Governance in Computational Antitrust—A Way Forward

As mentioned in the previous sections, we have already clarified why we consider both computational antitrust and algorithmic governance relevant and why both fields encompass inevitable choices that must be tackled by policymakers, the private sector, and academia alike.

But in order to concretely combine these two areas, one can envision some strategies. Our focus here will be on encapsulating important algorithmic governance variables into three dichotomies that help to provide general guidelines for computational antitrust solutions—and it is worth emphasizing that we absolutely do not intend these categories to be exhaustive or sufficient to describe the complexity of the debate, merely that we understand they can be useful in drafting initial proposals to bringing these two areas closer together and starting to conceive of solutions. To make the discussion more concrete, we add comments regarding the case of screening algorithms. Given that screening solutions are perhaps the most famous and advanced proposals in computational antitrust, as mentioned above, they offer an ideal exploratory case to demonstrate the relevance and potential applications of algorithmic governance precautions to computational antitrust.

A – Automation v. AI and Machine Learning

The first dichotomy relates to a difference one can make between general *automation* and, more specifically, *AI and machine-learning* algorithms. Domingos makes a similar distinction when he explains that, in traditional automation, "the only way to get a computer to do something—adding two numbers to flying an airplane—was to write down an algorithm explaining how in painstaking detail."[48] However, "machine-learning algorithms, also known as learners, are different: they figure out on their own by making inferences from data. And the more data they have, the better they get."[49]

A real-life example of straightforward automation is the algorithm used by the Brazilian Supreme Court (or STF for its Portuguese acronym) in order to distribute cases for reporting Justices. The algorithm is designed to follow the exact prescription of the Internal Regulations of the court, which already determine how distribution should take place. After allegations of potential issues with the system that could in practice lead to faulty distribution,[50] the court decided to issue a bid to select scholars to audit the algorithm[51] which was ultimately carried out by a group from the University of Brasília. The researchers concluded that there were

[48] PEDRO DOMINGOS, MASTER ALGORITHM: HOW THE QUESTION FOR THE ULTIMATE LEARNING MACHINE WILL REMAKE OUR WORLD (Basic Books 2015).
[49] Domingos, *supra* note 48.
[50] *See* Daniel Chada & Ivar Hartmann, *Distribuição dos processos no STF é realmente aleatória?* [*Is the distribution of processes in the Brazilian Supreme Court really random?],* JOTA (July 25, 2016), https://www.jota.info/stf/supra/distribuicao-dos-processos-no-supremo-e-realmente-aleatoria-25072016.
[51] *See* André Richter, *STF fará auditoria no sistema eletrônico de distribuição de processos* [*STF will audit the electronic process distribution system*], AGÊNCIA BRASIL (May 16, 2018), https://agenciabrasil.ebc.com.br/justica/noticia/2018-05/stf-fara-auditoria-no-sistema-eletronico-de-distribuicao-de-processos.

no substantial problems or failures with the algorithm, though they also recommended that the STF be more transparent and also extensively document the workings of the system.[52]

A different example, which effectively relies on AI, is that adopted by the algorithm Radar, used by the Superior Court of Minas Gerais (TJMG for its Portuguese acronym), a state in Brazil.[53] The system is responsible for identifying and selecting appeals that have "identical requests."[54] In other words, the AI algorithm is effectively responsible for determining what similar appeals are. Notably, this selection is not based on criteria entirely and exhaustively set forth by the court, but rather on how the algorithm understands similarity. The TJMG never revealed how the AI was trained or what are the variables it uses to determine such likeness of the requests, but even if it did, as Domingos mentions, this process is malleable and changes over time because the system "learns" from new data.[55]

As these examples help to demonstrate, it tends to be easier to achieve accountability in traditional automation efforts vis-à-vis AI and ML techniques. For public administrators who need to provide transparency of motivation when making decisions, this difference is paramount. As the principles laid out in section III above clarify and as some authors emphasize,[56] whereas full transparency would be achievable in the former (even if not always desirable), the same cannot be said for the latter, such that the idea of explainability *in lieu* of full transparency would be better suited for AI and ML systems.

Lawrence Lessig had famously presented such a view with respect to government transparency when he claimed that turning the panopticon to focus on the authorities, thus creating civic omniscience, was problematic. He built his argument upon the ideas expressed by Brandeis in *Other People's Money*, namely the argument that full disclosure of the information would help the public judge the quality of goods and services and, as such, allow the people to regulate markets. As Lessig warns, "not all data satisfies the simple requirement that they be information that consumers can use, presented in a way they can use it."[57]

Ananny & Crawford, for their turn, dealing more specifically with algorithms, clarify that the ideal of transparency rests on the belief that:

> the more facts revealed, the more the truth can be known through a logic of accumulation. Observation is understood as a diagnostic for ethical action, as observers with more access to the facts describing a system will be better able

[52] *See* Gustavo Rodrigues, *Por dentro da distribuição de processos do STF* [*Inside the STF process distribution*], INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (Sep. 20, 2018), https://irisbh.com.br/por-dentro-da-distribuicao-de-processos-do-stf/ (interview with Henrique Araújo Costa, one of the researchers from the University of Brasília, detailing their findings) .

[53] TRIBUNAL DE JUSTIÇA DE MINAS GERAIS [TJMG], *TJMG utiliza inteligência artificial em julgamento virtual* [*Minas Gerais State Court of Justice uses artificial intelligence in virtual judgment*] (Nov. 7, 2018).

[54] TJMG, *supra* note 53, second paragraph.

[55] Domingos, *supra* note 48.

[56] *See, e.g.,* Domingos, *supra* note 48; Alejandro Barredo Arrieta et. al., *Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI*, ARXIV (Dec. 26, 2019), https://arxiv.org/abs/1910.10045.

[57] Lawrence Lessig, *Against Transparency*, THE NEW REPUBLIC (Oct 9, 2009), https://newrepublic.com/article/70097/against-transparency.

> to judge whether a system is working as intended and what changes are required.[58]

As the authors emphasize, however, this assumption only holds true if one assumes that "knowing is possible by seeing,"[59] an affirmation that they contest on ten different fronts:

1. Transparency can be disconnected from power, meaning that transparency as a means of accountability will only work inasmuch as those subjected to it are somewhat vulnerable to its consequences, a condition that does not always hold.
2. Transparency may expose information about individuals or groups without any clear benefit, damaging privacy.
3. If transparency is made an overarching obligation, actors subjected to it may decide to reveal information strategically; in other words, they may do so in a way that hinders rather than facilitates understanding.
4. Transparency requirements may create "false binaries,"[60] as well as the false perception that the only options available are full disclosure or total secrecy, which is not true.
5. The ideal of transparency rests upon other assumptions, such as perfect information and fully rational decision-making – the premise being that once individuals are able to examine a system, they will be fully capable of understanding it, and, more importantly, of making completely rational decisions based on the information provided. Ananny & Crawford emphasize the "persistent fiction"[61] of these assumptions.
6. Transparency does not always build trust.
7. Transparency usually involves some level of professional expertise, in the sense that "professionals have a history of policing their boundaries . . . It may be impossible to really see professional practices without understanding that they are situated within contexts."[62]
8. The call for transparency assumes that to see is to know, something educational observation over time has proven untrue.[63]
9. Transparency requirements are sometimes made infeasible or technically cumbersome by advances or developments in computer science technology whereas as will be seen in section 4.1.1 below – machine learning poses additional challenges.
10. The timing of disclosure of algorithmic systems can affect results, in that revealing the inner working of a system before, during or after the system

[58] Mike Ananny & Kate Crawford, *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability,* 20 NEW MEDIA & SOC'Y 973, 973-89 (2016).
[59] *Id*. at 977.
[60] *Id.* at 979.
[61] *Id.* at 980.
[62] *Id.*
[63] "Learning about complex systems means not simply being able to look inside systems or take them apart. Rather, it means dynamically interacting with them in order to understand how they behave in relation to their environments (Resnick et al., 2000). This kind of complex learning intertwines epistemological claim-making with material design, social contexts, and self-reflexivity—making sure that a system is not only *visible* but also debated and changeable by observers who are able to consider how they know what they know about it." *Id.* at 981.

becomes operational has distinct consequences, which is compounded by the fact that the system itself is likely to change over time.

This means that, although a fully transparent causal account of the algorithm's output may be impossible, the reasoning behind such output may at least be understandable to a satisfactory degree. At the same time, there is evidence to support the claim that the more complex the system, the more accurate it can be[64]—offering a real challenge to policymakers, which to some extent will likely have to trade-off between how much explainability they can provide and how precise their tools will be.

While in traditional automation, some simpler solutions would suffice to provide broad transparency (such as open-source coding, open data formats, and extensive documentation), additional layers of care must be in place for trying to explain and understand AI and ML systems. A field of growing interest to algorithmic governance is that of explainable AI, or XAI, which has been intensively studying how AI and ML systems may be designed to offer better explainability and accountability in high-risk, critical applications.[65]

In this context, special care should be taken when we are considering connectionist AI algorithms, where notions such as correlation and pattern recognition are much more applicable than notions such as function, structure and logical causality between input and output. Because of this, symbolic AI techniques are experiencing a revival in applications where explainability is a priority.

It is understandable that the computational law community is often enthusiastic about the potential of connectionist AI such as deep neural networks, given their widespread recent success in many areas and the availability of so-called "raw data" to work with, as well as the trade-off between explainability and accuracy or computational efficiency.[66] But it is worth adopting a general caution directive and trying to employ symbolic or hybrid techniques whenever possible, at least in the early stages and first attempts at computational antitrust by authorities.

Additionally, some useful precautions can be embedded in AI and ML systems to aid public decision-makers in meeting motivation and transparency requirements. In this respect, Citron[67] recommends extensive production of logs and trails when running algorithms, as a form of clearly defining and producing notes on the scope, implementation, and execution session of an algorithm or system. Another interesting possibility for public officers is the production of customized explanations as an output or side-effect of the system itself, to serve as motivation criteria of a decision taken with the assistance of such a system.

Relating to this particular aspect, screening algorithms are an interesting sandbox experience because they already have a precursor traditional-automation form

[64] Jon Kleinberg & Sendhil Mullainathan, *Simplicity Creates Inequity: Implications for Fairness, Stereotypes, and Interpretability*, ARXIV (June 2, 2019), https://arxiv.org/abs/1809.04578.
[65] Alejandro Barredo Arrieta et. al., *supra* note 56.
[66] Kleinberg & Sendhil, *supra* note 64.
[67] Citron, *supra* note 47.

based on econometric computer modelling, where variables are elected and/or derived from structured economic theory logic (which is usually standard and even statutory in some jurisdictions). This provides an opportunity for computational antitrust projects to try their hand with more structured ML solutions and show compliance with XAI practices. As a general rule, XAI may provide useful ways of safeguarding both the authority's public law requirements and due process guarantees of defendants.

B – Assistance v. Decision-making

A second dichotomy worth noting is the role of mere *assistance* as opposed to *decision-making*. We have already emphasized the distinction between legal assistance and legal advisor systems, as well as some of their perils for computational antitrust. First, algorithms that are capable of issuing decisions are considerably riskier and more onerous to the public administration because of several constraints related to due process guarantees in contemporary democracies. Secondly, the notion of "decision" here must be stressed since it can mean a broad range of steps in a legal case, even very minor, compartmentalized steps.

Let us turn once more into the case of screening algorithms. In many jurisdictions, a procedure must be initiated (even if very simply or preliminary) in order for screening and scrutinizing practices by a given number of companies to be possible. To initiate such a procedure is a decision in itself, so it is important that the algorithm is only used after the due process requirements applicable for such decision-making are met. If a screening algorithm is started or applied without the previous decision-making step, this would mean that such a decision is being taken outside of legal requirements. The same can be said for the moment after the algorithm is started if, as part of its normal functioning, output, or side effects, the algorithm is able to proceed to opening a probe (i.e., making a decision that may need to meet further legal requirements).

An additional example is the potential use and processing of personal data in screening algorithms. In several jurisdictions, there are requirements for such activities. Algorithms may be designed to ignore or be completely oblivious to such constraints, often projected by technical teams who may not be fully aware of the entire spectrum of legal implications of a computer program. Although this example is not a decision falling within the realm of core antitrust law, it is nonetheless a form of decision-making that is being inadvertently taken by the competition authority and must meet legal requirements.

Many such decisions may be hidden within all sorts of algorithms. It is important that, when devising a computational antitrust solution, technical and legal teams can translate to each other every step, input, and output, to the extent this is possible, to produce a clear techno-legal flowchart of the solution put in place. Of course, the challenge here is also an organizational one and should involve building the capacity for legal and technical teams to be mutually intelligible, as well as ensuring adequate room for this interchange to happen

during planning, amidst organizational routines, and within the dynamics of internal hierarchies and divisions.

Another peril related to the assistance vs. decision-making duality is the tendency of limits between the two getting blurred under the pressure of efficiency and convenience. Algorithmic governance literature provides us with notable instances where this happened at the expense of public law guarantees, such as is the case regarding COMPAS, a tool originally designed as a jail monitoring mechanism and then extended, for the sake of convenience, to act as a recidivism risk assessment tool,[68] where its unreflected use ended up reproducing criminal justice's racial bias and resulted in longer sentences for black individuals when compared to white individuals.[69]

In a nutshell, what must be highlighted is that if human supervisors do not have working conditions and protocols that guarantee sufficient time and resources for a critical, substantial supervision work, they may find it tempting to adopt algorithm's recommendations indiscriminately, in practice leading mere assistance tools to take the role of decision-making. Again, this was precisely the discussion in the most famous legal battle involving COMPAS.

COMPAS was used for recidivism risk assessment (rather than jail monitoring) in the case of Eric Loomis in the state of Wisconsin. In 2013, Loomis was accused of eluding the police in the city of La Crosse, after driving a car used in a shooting. He had been previously convicted of third-degree sexual assault and, after an assessment by COMPAS, was ruled to be of high risk of committing another crime, thus sentenced to a six-year sentence. Loomis' lawyers appealed the sentence, claiming that the defense had no access to the risk assessment carried out by COMPAS, given its proprietary nature, even though such a result was expressly taken into consideration by the judge in his sentencing. The case reached the Supreme Court of Wisconsin, which maintained the judge's decision, stating that COMPAS was not the only reason the decision was based upon—precisely stating, therefore, that because the tool was merely assisting the decision, and was not the main or the only legal ground for conviction, the ruling was valid.

---

[68] *Criminal Law - Sentencing Guidelines - Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessments in Sentencing* - State vs. Loomis, *881 N.W.2d 749 (Wis. 2016)*, 130 HARV. L. REV. 1530 (2017).

[69] According to Julia Angwin and her team at ProPublica who revealed the use of algorithms in criminal sentencing and its legal and moral implications, COMPAS "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 Black defendants were falsely flagged as high risk and potential re-offenders at twice the rate as white defendants, whites were more frequently deemed as low risk than Black defendants. *See* Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks*, PROPUBLICA (23 May 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing ("We also turned up significant racial disparities, just as Holder feared. 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. The formula was particularly likely to falsely flag black defendants as future criminals, wrongly labeling them this way at almost twice the rate as white defendants. White defendants were mislabeled as low risk more often than black defendants. Could this disparity be explained by defendants' prior crimes or the type of crimes they were arrested for? No. We ran a statistical test that isolated the effect of race from criminal history and recidivism, as well as from defendants' age and gender. Black defendants were still 77 percent more likely to be pegged as at higher risk of committing a future violent crime and 45 percent more likely to be predicted to commit a future crime of any kind.").

As this case illustrates, assistance tools such as screening algorithms also need to be considered as potential decision-makers when they can be used as legal proof for taking further decisions down the line. If the proof of a case hinges on algorithmic results, and these are accepted without corroboration from alternative proof sources (e.g., dawn raids), then the "assistance" character of the tool can approach decision-making, which is a serious vulnerability in jurisdictions where a judicial review can scrutinize proof standards of competition authorities' decisions. Computational antitrust should take due organizational and legal precautions to impede the undue erosion of the lines that separate assistance from decision-making.

The screening example is once again insightful when we consider the principles of data provenance, accuracy, and overall quality-of-database recommendations from algorithmic governance studies. Proponents of the use of big data in antitrust are often optimistic about the huge amounts of "raw data" available in procurement and digital markets. However, there has still been little reflection on the problems associated with the "raw data" assumption. As noted by Davies & Frank (2013), "There is no such thing as raw data."[70] They correctly make the point that "open datasets are constructed data, potentially brought together from many flows of data inside government, and that much of what goes into an open datasets construction remains opaque in current practices."[71] Data from government bodies are often designed with diverse purposes in mind, and their collection and production may be plagued with biases, criteria, and interpretational assumptions suited for sectoral policies, contextual concerns, and other factors. Data scraped from the Web may also be tricky to control since contemporary websites, especially marketplaces or price-setting sites, are frequently non-reproducible and context-dependent. For example, if an authority's client machine changes its geographic location or cookie history, it may get widely different results. Authorities will need to devote time and resources to qualitatively and quantitatively understand data sources and their potential shortcomings and hidden "decisions" or biases.

C – Concrete adjudications v. *ex ante* measures

This leads us to a third useful dichotomy, the complementary relationship between adjudication in concrete cases and *ex ante* measures. As we mentioned, because of constitutional and public law principles, it will often be the case that competition authorities cannot simply put a computational solution to use without first providing for it *ex ante*. A long list of governance-related measures can be rolled out in this regard to help structure and protect computational antitrust solutions.

The most elementary precaution along this vein is for authorities to make rules before automating a policy, providing for the definition and use of a new system .[72]

[70] Tim Davies & Mark Frank, *There's no such thing as raw data': exploring the socio-technical life of a government dataset*, PROCEEDINGS OF THE 5TH ANNUAL ACM WEB SCIENCE CONFERENCE, ASSOC. COMPUT. MACHIN. (2013).
[71] *See* "RAW DATA" IS AN OXYMORON (Lisa Gitelman ed., 2013) (arguing that the transformation of reality into data is a constructive and interpretive process, not a biunivocal correspondence. "Interpretation," then, is not the final isolated step in the pipeline of data processing, rather a constant unavoidable feature of dealing with digital data.).
[72] Citron, *supra* note 47.

Evidently, this should be accompanied by the usual good-governance measures before and after the rule is made, which in the case of antitrust agencies usually include making guidelines, issuing studies, calling the public to participate, and advancing new theoretical discussions on the rationale underpinning new computational solutions.[73] Such measures can help authorities comply with a broad class of requirements, such as the general legality principle, legal certainty, due process, among others, offering a framework for the use of a tool.

Another measure that can be included in *ex ante* rulemaking is the allocation of accountability to persons and departments for potential mistakes and problems with the tool, as well as protocols to address these situations.[74] It is unavoidable to run into problems along the way, and to have clear responsibilities is key in order to prevent a series of challenges, such as the tendency to blame abstract systems as scapegoats, the risk of unfair or disproportionate liability allocation, and the lack of expertise-inducing organizational specialization.

In this regard, some agencies have already taken the promising good-governance measure of creating a dedicated technology department.[75] Of course, each agency is uniquely structured and not all of them will need to carve a "computational antitrust" department in their respective organizational charts, especially because many agencies already have technological expertise in forensics, IT and econometrics departments. This also does not mean that such specialized entities would be automatically liable for problems with AI and ML tools. On the contrary, the designation of specific personnel dedicated to some tasks and functions related to a given tool can help determine whether or not such a unit or position is indeed responsible for a certain issue. In the absence of clear allocation, technical personnel can end up receiving the blame even if this is unfair or inadequate. In any case, investment in qualification and mutual comprehensibility between legal and technical teams would also be risk-mitigating measures.

A final recommendation on this front is to incorporate best practices from software engineering. Therefore, agencies should extensively test, log, and benchmark the tools, their errors and bugs, data sources, performance, objectives, and accomplishments ahead of launch, and open these steps to public participation whenever possible. Agencies should also adopt and maintain adequate version control and database infrastructures, logging and record-keeping, encryption and cybersecurity when necessary, anonymization and destruction protocols for data protection measures, quality-of-data processing, among others. All of this should be obvious to many professional technicians, but it is not yet commonplace in law or antitrust.

---

[73] Such as in the example from Mahari et al., *supra* note 21, where traditional "delta HHI" causal nexus techniques were being replaced by computational antitrust's networked relevant market approach.
[74] Citron, *supra* note 47.
[75] *See* Matthew Holehouse, *Competition Regulators Need AI and Behavior Experts, UK Official Says,* Mlex (June 2019); Simon Zekaria, *UK Antitrust Agency's Chief Data Officer Will Be "First in Europe,"* Mlex (Dec. 2017); and Toko Sekiguchi & Sachiko Sakamaki, *Regulator's One-of-Kind Digital Team Looks to Set Japan's Online Antitrust Agenda*, Mlex (Nov. 2020).

V. Conclusion

As we have hopefully demonstrated throughout this brief article, the need for convergence in computational antitrust and algorithmic governance is paramount and will grow the more antitrust authorities make use of technological solutions, be they automation or more complex AI and ML systems. Precisely because the adoption of such solutions is still in its early stages, there is ample room for this discussion to develop, as well as for its relevance to expand.

Our main goal here has been to present the debate, show the interplay between the two areas, and offer some alternatives that could help frame the discussion, especially thinking of ways for antitrust policymakers to face the challenge of complying with the high standards of public decision-making and make the best out of the many opportunities technology presents. Further discussion on this matter is absolutely needed, and in particular, we understand that agencies' engagement in the debate could help both in identifying challenges more clearly and in devising concrete solutions.