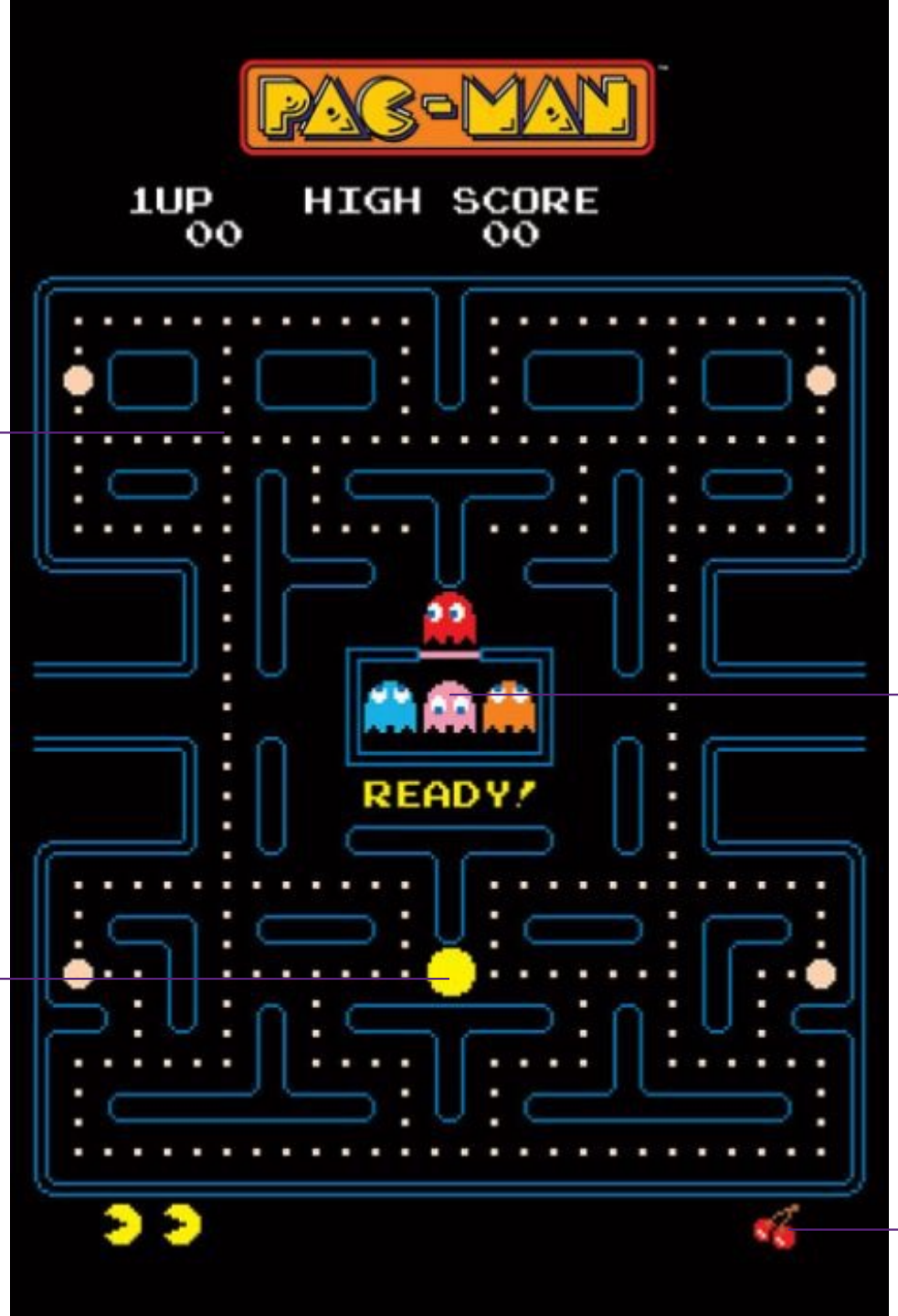
In search of the silver bullet: The impact of algorithmic screening tools on competition law proceedings and the right to a fair trial

Jerome De Cooman
jerome.decooman@uliege.be
30 September 2022, Madrid (IE University)

Consumer surplus

International cartel



(National) Competition Authorities

Occasional windfall profit

II.A. Current Investigation Methods

- Cartel takes place "*behind a veil of dishonesty*" and wear a "*cloak of secrecy*" (OECD 2001)
- Upshot? Few cartels discovered (Bryant and Eckard 1991, Combe 2007, Ormosi 2020, Combe 2020)
- Solution: Leniency programmes
  - Break the omerta code among cartel member by offering amnesty to the first-in-the-door (Zingales 2008)
  - Are resource-efficient (Harrington 2008) as they provide first-hand evidence (Stephan 2009)
    - reduction of investigation and prosecution costs and reduction of the duration of the procedure (Brenner 2009)
  - Deter cartel formation as cartel "*is a game of trust*" (Leslie 2004)

II.A. Current Investigation Methods

- However:
  - Controversial effectiveness:
    - "*Success is to be measured by a small number of cartels, not a large number of leniency applications*" (Harrington and Chang 2015)
    - "*What consumers and industry ultimately need is an economy that doesn't have cartels in the first place*" (Vestager 2021)
  - Deterrence gap
    - The majority of investigations starts after a leniency application (Archimbaud 2020)
    - Low probability of detection through *ex officio* investigation (EU Court of Auditor 2021)
    - The carrot is amnesty, the stick the probability of detection: Expected value of penalty $\leq$ or $\geq$ profit driven from cartelisation? (Deschamps and Marty 2006)
  - "*While there is a recognition that a leniency program is an immensely valuable tool (…) concerns arise when it is the <u>only</u> tool*" (Harrington and Chang 2015)

II.B. Strengthening Competition Law Enforcement

- Despite leniency programmes and screening methods, the probability of cartel detection is still around 15% (Combe 2020)
- There is however an almost ten year long political initiative to update competition law enforcement in light of digital technology
  - "*We must take much better use of the great opportunities offered by digital technologies*" (Juncker 2014)
  - The Commission "*will continue to monitor the opportunities and challenges brought by artificial intelligence solutions*" (EC 2017a)
  - Consultancy tender aimed at gathering "*informed knowledge* (…) *about existing AI solutions*" for law enforcement and particularly how AI "*could potentially improve DG Competition's processes of evidence management, legal drafting and market intelligence gathering*" (EC 2017b)

II.B. Strengthening Competition Law Enforcement

- In light of priority and resources allocation, AI systems help the competition law authorities initiate the "*right investigation*" (von Bonin and Malhi 2020)
  - Refinement of Regulation 1/2003 ambition of "*freeing up resources to focus on serious infringement*" (§ 36).
  - AI systems draw the sketch of suspicious businesses by identifying cartelists' recurring characteristics or patterns (Sanchez-Graells 2019)
- "*Algorithmic shift in the fight against cartels*" (de Marcellis-Warin, Marty and Warin 2022)
  - Process data quicker and more efficiently
    - → Sooner identification of market deficiencies
    - → Shift from reactive claim to proactive investigations
    - → Increases the probability of detection that increases the efficiency of leniency programmes

II.C. Screening

- There is "*conventional wisdom on collusion*" that permits the identification of "*factors that are supposed to hinder or facilitate*" collusive behaviours (Tirole 1988)
  - Structural screens: analysis of market structure
  - Behavioural screens: analysis of the collusive methods or outcome of collusion
- The probability of cartel detection is not exogenous and depends on competition authorities' choices (Combe 2020)
  - Finite resources lead to different priority degrees (CJEU, *Automec srl v Commission* 1992)
  - The Commission is free to focus "*its enforcement resources on cases where it appears likely that an infringement may be found*" (Commission Notice 2011)

II.C Screening (and Machine Learning)

- Screens do not "*prove collusion or manipulation*" (Abrantes-Metz *et al*., 2012)
- Screens identify and flag "*unusual patterns*" (Cocciolo *et al*., 2022)
- Spotting an inconsistency does not mean proving collusion (Harrington 2008)
- Screening raises red flags that trigger the need for, *e.g.*, down raids (Harrington and Imhof 2022).

II.C. Screening (and Machine Learning)

- Screen identifies pattern of collusion
- An AI system aims at *"discovering correlations (sometimes alternatively referred to as relationships or patterns) between variables in a dataset, often to make predictions or estimates of some outcome"* (Lehr and Ohm 2017)
- AI-driven cartel screening is an intuitive idea
- Studies demonstrate (AI-driven) cartel screening works
- However, AI-driven cartel screening faces three challenges

III. Data Challenge: availability

- All digital solutions are information-dependent and are therefore “significantly affected by problems in the *availability* (…) of the information they rely on.” (Sanchez-Graells 2021)
- Detect collusion in dataset T, trained on dataset W (same market as dataset T) or on dataset Z (comparable market) if W does not exist
- Upshot? “*no data, no fun*” (Sanchez-Graells 2021)

III. Data Challenge: Quality

- Screening is a resource and data-intensive activity
  - Data obtained from undertakings: Reliable but impossible to access them without tipping them off
  - Publicly available or aggregated data: far less trustworthy (OECD 2013)
- Upshot? It is "*neither productive nor efficient*" to "*implement screens in every market and at every moment in time*" (Abrantes-Metz 2013)
- Even if reliable data available, the extensive cost of developing and implementing screens might be burdensome for certain competition authorities (Kovacic 2013)

III. Data Challenge: Quality

- Type II error (false negative): not detecting a cartel despite its existence
- Type I Error (false positive): mistakenly identifying a cartel where there is none
- Origins?
- Misspecification of the (non-)collusive model:
  - "*Economists have developed literally dozens of oligopoly pricing theories*" (Scherer 1970)
  - "*Virtually anything can happen*" (Stigler 1964); Screening literature is a "*forest for the trees*" (Stenborg 2004)
  - "*None of the collusive markers identified are universal, and each must be used with caution*" (Harrington 2008); AI does not lead to a "*theory of everything*" (Schrepel 2021).
- Data "*originates from antitrust cases and may therefore be subject to selection bias*" (Symeonidis 2003) as collusive markers are built on discovered and successfully prosecuted cartels (Groutt and Sonderegger 2006)
- Confusion between explicit and tacit collusion (Abrantes-Metz 2013)

III. Data Challenge: Governance

- AI is not Types I and II error-proof, yet its reliability rate is above 80% (Walliman, Imhof and Rutz 2018)
- AI systems still need data and best quality data are not always publicly available (// with Casey and Niblett 2021)
- "*It is a capital mistake to theorize before one has data*" (Conan Doyle 1889)
- Insight: construct a better data architecture before developing AI-driven cartel screening
- Drawing inspiration from the AI Act: article 10

IV. Algorithmic Challenge

- The EC is entitled to discard some cases at a very early stage
- BUT all cases are subject to an initial assessment phase (EC notice on best practices)
- The EC has to respect the duty to state reason (case T-67/11, *Martinair v. EC,* 2015) as stated in Article 41 CFR
- The duty to state reason is a *sine qua non* condition for an effective judicial review (art. 47 CFR)

IV. Algorithmic challenge

- AI-driven cartel screening challenges the principle of good administration and the duty to state reasons (Pasquale 2021)
- Civil servants should provide "*human-interpretable information about the factors used in a decision and their relative weight*" (Doshi-Velez *et al.*, 2019)
- When an administrative decision is (at least partially) based on an algorithmic recommendation, then the duty to state reasons will be satisfied if the human operator is able to disclose how the different parameters were weighted and to what extent that recommendation was decisive for the final decision (Yeung 2019)

IV. Algorithmic Challenge

- This is, however, not always possible given AI system's opacity
- Public officers cannot state their reasons by taking into consideration the relevant factors and weighting them appropriately because neither the factors nor their weight are known
- In case of intrinsic opacity, the only available explanation is "*because the AI system said so*" (Fink and Finck 2022)

IV. Algorithmic Challenge

- Drawing inspiration from the AI Act: ensuring human autonomy through human agency and oversight
  - Human agency means human must be able to make informed choice
  - Human oversight means AI system does not undermine human autonomy because there is still a human-in(on)-the-loop (or in-command)
- Art. 14 AI Act: the design of AI systems has to ensure "*they can be effectively overseen by natural persons during the period in which the AI system is in use*"
- How? AI-driven cartel screenings should be designed "*in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately*" (art. 13 AI Act).

V. Human Challenge

- Explicability goes beyond the algorithmic challenge.
- The duty to state reasons requires an explanation of the algorithmic operation and an explanation of "*the influence that algorithm results have on (constraining) human decision-making*" (Busuioc 2022).
- The weight of the recommendation should not be underestimated
- Going against the recommendation would require a well written reasoned decision that renders "*the exercise of discretion costlier*" (Petit 2018)
  - "*A hearing officer's belief that computer decisions are error-resistant increases the likelihood of inaccurate outcomes*" (Citron 2008)
  - "*Computers also benefits from their traditional reputation of being intelligent and fair, making them seem credible sources of information and advice*" (Fogg 2003)

V. Human Challenge

- This is due to the automation bias, *i.e.* the irrational tendency to rely on automated decision even when the operator suspect malfunction (Goddard *et al*. 2012).
- The automation bias is the digital update of:
  - Search satisfaction: stop searching once a first plausible explanation is found
  - Anchoring: premature decision-making based on limited information initially available
  - Confirmation bias: tendency to interpret information to fit the preconceived opinion
- The algorithmic recommendation is:
  - A first plausible explanation…
  - … that tempts the officials to cease the scrutiny…
  - … and even if further investigation were to be conducted, the recommendation would serve as an anchor as any new information gathered would be interpreted as strengthening the preconceived opinion.

V. Beyond Oblivion: Policy Recommendation

- Drawing inspiration from the AI Act
- Users must "*remain aware of the possible tendency of automatically relying or over-relying on the output produced (automation bias)*" (art. 14(4)(b)), to choose when not use the AIS or discard the recommendation (art. 14(4)(d)).
- This is not enough: the absence of overreliance on the recommendation "*must be transparently demonstrated and ensured*" through non-technical measures (Smuha *et al*., 2021)
- *E.g.*: four-eyes principle: mandating a second human officer to approve both the decision and underlying reasoning proposed by a first officer

VI. Conclusion

- This paper is not a pamphlet against algorithmic screening
- The counterfactual scenario of not using these tools is full reliance on competition authorities' officials
- There is no evidence human decision is "*significantly more accountable than AI*" (Lim 2021)
- Both individual (Coglianese 2022) and groups (Callon and Latour 2006) are black boxes

- The question is therefore not whether algorithmic screening is perfect, but rather what will work better
- AI-driven cartel screening may play a role in strengthening competition law proceedings
- BUT it is not a silver bullet (data, algorithmic, and human challenges)
- The AI Act provides useful solutions, but is not applicable to competition law
- Voluntary endorsement to avoid any challenges of EC's decision based on violation of the duty to state reasons?

LIÈGE université
Cité

III. Algorithmic Decision-Making under the AI Act

- Do algorithmic screening tools fall within the scope of application of the AI Act?
  - "*Without any prejudice to the application of Union competition law*" (Explanatory Memorandum)
  - This is not a dead-end
  - AI system is a software that generates either content, predictions or recommendations given a set of human-defined objectives (art. 3(1) AI Act)
  - High-risk AI system is
    - Either covered by sectorial product legislation listed in Annex II and used as a product or a safety component (art. 6(1)(a) AI Act) for which a third-party conformity assessment is required (art. 6(1)(b) AI Act)
    - Or not covered by sectorial product legislation but still considered as high-risk and as such listed in Annex III (arts. 6(2) and 7 AI Act).

III. Algorithmic Decision-Making Under the AI Act

- Law enforcement activity mentioned in Annex III
  - The AI Act defines law enforcement authority as any public authority competent for law enforcement activities, *i.e.*, the prevention, investigation, detection, or prosecution of criminal offences (arts. 3(40) and 3(41) AI Act).
  - Annex III submits to mandatory requirements AI systems used by law enforcement authorities "AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680 *or assessing personality traits and characteristics* or past criminal behaviour *of natural persons or groups*" (Annex III(6)(e) AI Act)
- This definition is quite close to the purpose of behavioural cartel screenings, and yet it is restricted to criminal offences

III. Algorithmic Decision-Making Under the AI Act

- Reference to criminal offences is problematic, as competition law is qualified as criminal in some but not all Member States
  - Full criminalisation: Ireland, Estonia, Denmark, Greece and Slovenia
  - Criminalisation of specific competition law infringements in Luxembourg, Germany, Poland, Hungary, Austria, Italy, Belgium, Portugal and Croatia
  - Criminalisation of competition law infringement in specific circumstances in France, Romania, Czechia and Slovakia (*caveat* Cyprus)
  - No criminalisation in Bulgaria, Finland, Netherlands, Sweden, Malta, Lithuania, Latvia and EU competition law
- Upshot: The AI Act will only apply to competition law proceedings in legal orders that criminalise competition law
- How does this fit the objective of harmonisation?

III. Algorithmic Decision-Making Under the AI Act

- Applying the AI Act to competition law through the backdoor? Criminal law if (ECtHR *Engel*)
  - Classification in domestic law as a starting point (ECtHR, *Weber v. Switzerland* 1990)
  - Nature of the offence
    - Does the rule concern all citizens? (ECtHR, *Bendenoun v. France* 1994)
    - Does the rule have a deterrent or punitive purpose or does it merely impose pecuniary compensation? (*Ibid*)
    - Were the proceedings brought by a public authority under statutory powers of enforcement? (ECtHR, *Benham v. The United Kingdom* 1996)
    - Does the rule at stake seek to protect general interests of society? (ECtHR, *Produkcija Plus Storitveni Podjetje D.O.O. v. Slovenia* 2018)
    - Is the imposition of a penalty upon a finding of guilt? (ECtHR, *Benham v. The United Kingdom* 1996)
    - Is the misconduct at stake classified as part of the criminal law in the vast majority of the Contracting States (ECtHR, *Öztürk v. Germany* 1984)
  - Severity of the penalty (ECtHR, *Campbell and Fell v. The United Kingdom* 1984)
- Upshot? Competition law belongs to the criminal sphere (ECtHR, *Société Stenuit v. France* 1992; ECtHR, *Lilly France S.A. v. France* 2002; ECtHR, *A. Menarini Diagnostic S.R.L. v. Italy* 2011)

III. Algorithmic Decision-Making Under the AI Act

- Within the EU
  - Competition law offences "*shall not be of criminal nature*" (Council Regulation 1/2003)
  - ECtHR *Jussila*: hard core vs peripheral criminal law
  - EU competition law is not hard core criminal law but belongs to its periphery (Bot 2010, Sharpston 2011, Kokott 2013, Wahl 2018, Bobek 2021)
  - Confirmed by the ECJ (recently, *bpost* 2022)
  - Competition law is "*criministrative*" law (Bailleux 2014)

III. Algorithmic Decision-Making Under the AI Act

- RQ: Could the criministrative nature of competition law serve as a back-door to apply the AI Act to all competition law proceedings regardless of the domestic qualification?
- No
  - Contextual approach: the AI Act and SWD refer to “criminal matters” in a context of hard core criminal law
  - Coherence: “AI systems specifically intended to be used for administrative proceedings by tax and customs authorities should not be considered high-risk AI systems used by law enforcement authorities for the purposes of prevention, detection, investigation and prosecution of criminal offences” (Recital 38, *in fine*, AI Act)

IV. Conclusion: Without Any Prejudice?

- Annex III suggests AI systems intended to be used by law enforcement authorities in the course of detection, investigation and prosecution of criminal offences raise high-risk and are subject to mandatory requirements
  - In legal orders that qualify competition law as criminal: algorithmic screening tools would have to comply with the AI Act
  - In legal orders that do not qualify competition law as criminal: the AI Act does not apply
  - The AI Act closes the door to an extension of its scope of application through peripheral criminal law
- As the AI Act is a harmonising regulation, keeping different standards of protection depending on national qualification makes no sense