Public Procurement and the Artificial Intelligence Act: Addressing Bid-Rigging Through the Back Door

PhD Conference in Public Procurement & Competition Law

Jerome De Cooman

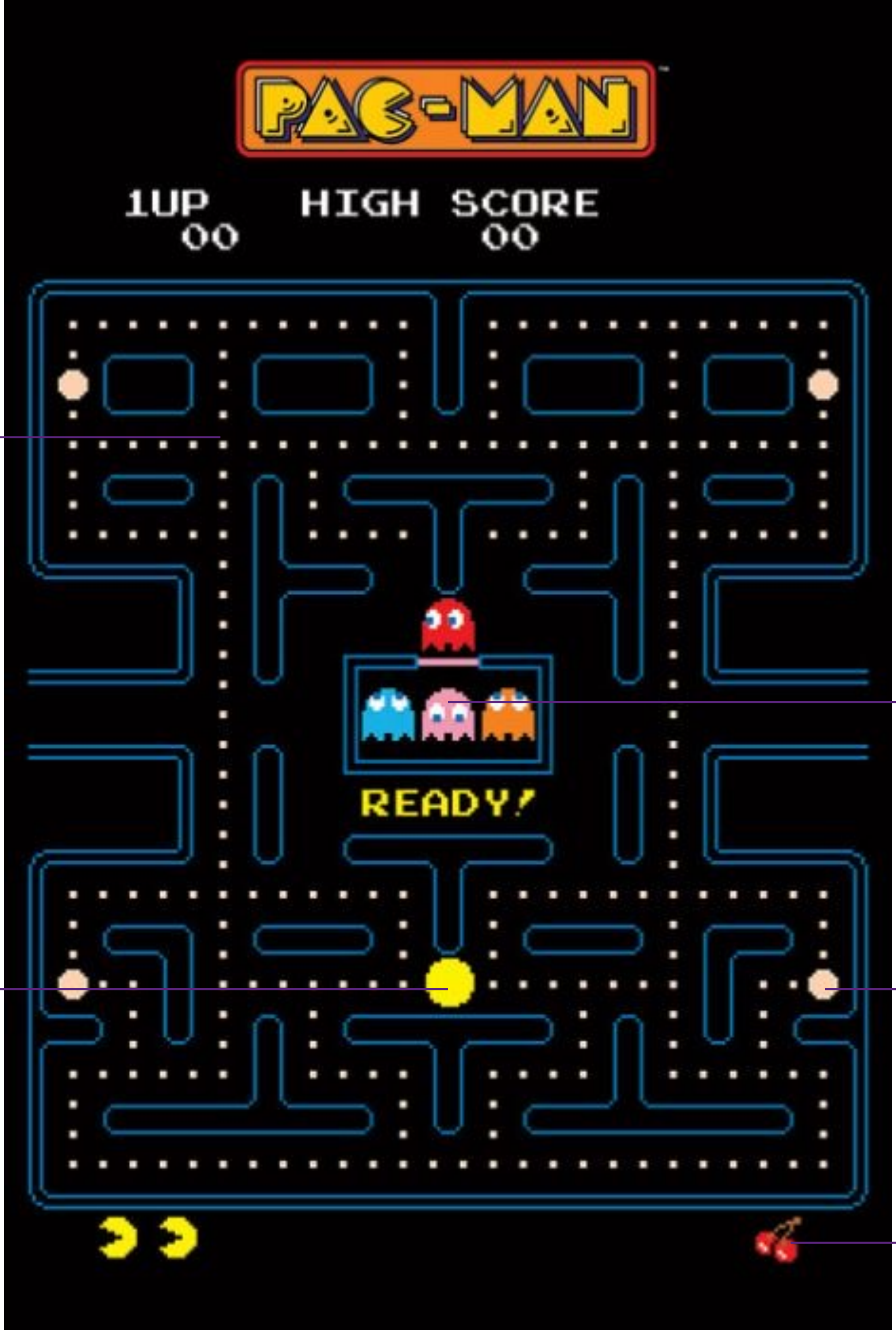
jerome.decooman@uliege.be

27 April 2023, University of Copenhagen (Denmark)

LIÈGE université
Cité

I. Introduction

Schinkel (2014)



Consumer surplus

(National) Competition Authorities

International cartel

Leniency

Occasional windfall profit

I. Introduction

- AI reshuffles the deck of this pursuit and evasion scenario
- On the one hand, AI allows the development of new strategy that favours Pac-Man
  - "algorithm-based technological solutions" = "structural competition problem" (Vestager 2020)
- On the other hand, AI allows the development of new strategy that favours the Ghosts

I. Introduction

- Amongst these tools lies AI-driven cartel screening (Huber and Imhof 2019)
  - Flags unusual patterns that triggers the need for further investigation
- AI-driven cartel screening works
- Yet, there are at least three challenges to overcome:
  - Data challenge: availability and quality
  - Algorithmic challenge: explicability
  - Human challenge: cognitive biases
- AI is a *pharmakon*.

Structure of the presentation

I. Introduction

II. An Alternative: Cartel Screening

- A. Strengthening Competition Law Enforcement
- B. Definition and Promises
- C. Pitfalls
  1. Data Challenge
  2. Algorithmic Challenge
  3. Human Challenge

III. Competition law and the AI Act

- A. Scope of application
- B. AI-driven cartel screening
- C. Criminalisation of competition law
- D. Peripheral and Hard Core Criminal Law
- E. Peripheral Criminal Law under the AI Act?

IV. Conclusion

LIÈGE université
Cité

II. Cartel Screening

A. Strengthening Competition Law Enforcement

B. Definition and promises

C. Pitfalls

A. Strengthening Competition Law Enforcement

- The probability of cartel detection is not exogenous and depends on competition authorities' choices (Combe 2020)
  - The EC has finite resources
    - The EC is entitled to give different priority degrees to complaints received (*Automec*)
    - The EC is free to focus "its enforcement resources on cases where it appears likely that an infringement may be found." (EC Best Notice 2011)

A. 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

B. Cartel Screening: Definition and Promises

- How does it works?
- 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

Structural screens

Structural screens		High probability of cartelisation
Structural factors	Number of firms (concentration)	Low (high)
	Entry barriers	High
	Undertakings’ interaction	Frequent
	Transparency	Low demand side, high supply side
Supply-side factors	Vertical product differentiation	Homogeneous product
	Innovation	Low-innovative markets
	Advertisement	Low-advertising industries
Demand-side factors	Demand	Stable
	Buyer bargaining power	Low
	Horizontal product differentiation	Low differentiation

Behavioural screens

Collusive markers		Collusive behaviour
Price	Price evolution	Low variance Sharp increase in high price-cost margin Sharp decline of price followed by sharp increase
	Product price and quality	Homogenisation through increased product standardisation and pricing formula
	Prices across customers	Decrease of customer-specific prices
Market shares	Sales quotas	Distribution of market shares seems more stable under collusion
	Exclusive territories	Price increase in the home-market, export decreases
	Customer allocation	Stable customer base
Enforcement	Buy-back	In time t a firm A sells above its historical market share while a firm B sells below its historical market share; in t+1, A buys products from B
	Compensation	In time t a firm A sells above its historical market share while a firm B sells below its historical market share; in t+1 the sale levels are inverted

B. Cartel Screening: Definition and Promises

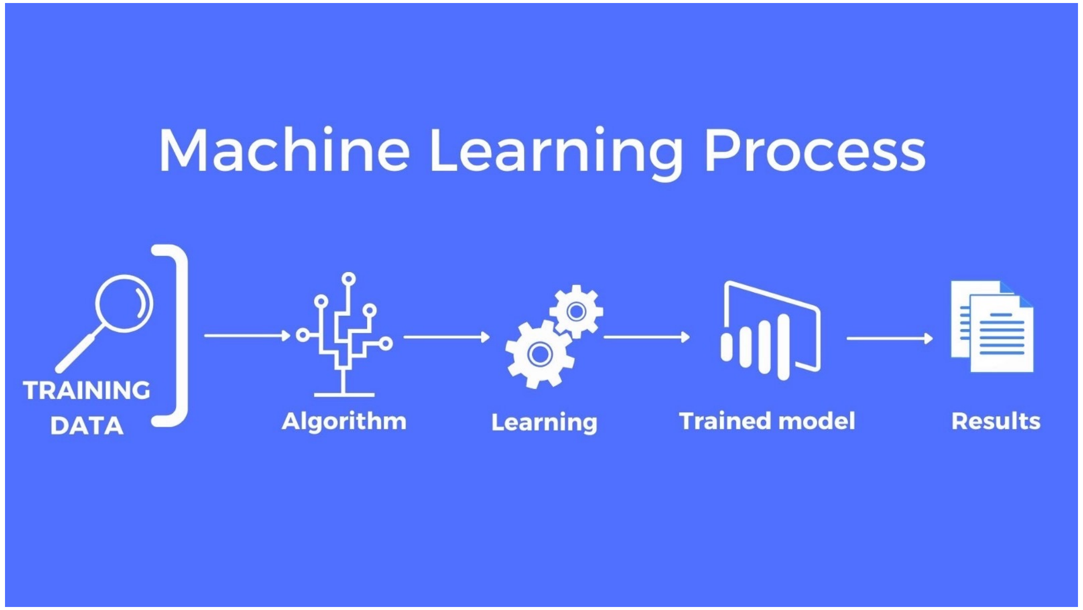
- Screens identify and flag "*unusual patterns*" (Cocciolo *et al.*, 2022)
- Screens do not "*prove collusion or manipulation*" (Abrantes-Metz *et al.*, 2012)
- Screening raises red flags that trigger the need for, *e.g.*, dawn raids (Harrington and Imhof 2022).
- From a procedural perspective, competition law is a three-stages process
  - Triage to identify cases worthy of close scrutiny
  - Verification through investigation
  - Sanction

B. Cartel Screening: Definition and Promises

- Studies demonstrate (AI-driven) cartel screening works
  - Detection of illegal agreements (Coglianese and Lai 2022)
  - Detection of corruption (e.g., in bid-rigging)
  - Faster assessment of merger control (Casey and Niblett 2021)
- However, AI-driven cartel screening “still has sceptics” (Abrantes-Metz 2014)
- This algorithmic solution faces three challenges

C. Pitfall – Data challenge

Data availability: no data, no fun



Data quality: dirty data, bad prediction

Ilcophans ſiue elephante.
qd arabicé alchy.

C. Pitfall – Algorithmic Challenge

- The EC has to respect the duty to state reason (*Martinair*)
  - During preliminary investigations (e.g., *Hoechts*, *Roquètte Frères*, *Deutsche Ban*)
  - And administrative procedures (*Shell International*; *Cimentaries*; *Schindler*)
- What about cartel screening?
  - Useful to trigger dawn raid
  - The duty to state reasons applies to dawn raid – *to some extent*
  - To be in possession of "information and evidence providing *reasonable grounds* for suspecting infringement of the competition rules by the undertaking concerned" (*Roquette Frères*)
  - Is the cartel screening's recommendation a "reasonable ground"?
  - Is the statement of reasons "excessively succinct, vague and generic"? (*Heidelberger Cement*)

C. Pitfall – Human Challenge

- Debates on black box and explicability is paradoxical
  - Algorithms are criticised because opaque
  - But both human beings (Thaler and Sunstein 2008) and administration are similar black boxes (Callon and Latour 2006)
- 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 had on (constraining) human decision-making* (Busuioc 2022).
- Going against the recommendation would require a well written reasoned decision that renders "*the exercise of discretion costlier*" (Petit 2018)
  - Automation bias

III. The AI Act and The Competition Law Proceedings

Scope of application – AI-driven cartel screening – Criminalisation of competition law – Peripheral and Hard Core Criminal Law

A. The AI Act Scope of Application

- The AI Act applies… to AI systems (art. 3 AIA, in combination with Annex I)
  - “software that is developed with machine learning, logic- and knowledge-based, or statistical approaches”
  - That can “for a given set of human defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with”
- AI-driven cartel screening fits the definition
  - It relies on machine learning
  - It generates predictions that then lead to recommendation to pursue further investigations

A. The AI Act Scope of Application

- The AIA is risk-based approach (Recital 14):
  - Unacceptable risk: prohibited
    - Subliminal manipulation, exploitation of vulnerabilities in order to distort people's behaviour, social scoring by public authorities, or (unless limited exceptions) real-time remote biometric identification in publicly accessible physical space for the purpose of law enforcement (art 5)
  - High-risk: mandatory requirements (*see* next slide)
  - Limited risk: limited transparency requirements
    - AI system designed to interact with natural person (art. 52) – include deepfakes
  - Non-high-risk
    - Residual category – everything that is not high-risk (art. 69)

A. The AI Act Scope of Application

- High-risk AI systems: submitted to *ex ante* safety requirements (art. 8)
  - Either those that are used as a product of a safety component of product covered by sectorial product legislation (Annex II) for which a third party conformity assessment is required (art. 6(1))
  - Or those that are explicitly listed in Annex III because deemed posing risk of harm to the health and safety, or a risk of adverse impact on fundamental rights (art. 6(2))

B. AI-driven Cartel Screening under the AI Act

- Is there a room for AI-driven cartel screening in this risk pyramid?
  - 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).
- What is the legal regime applicable to law enforcement authorities using AI system?
  - Unacceptable risk in case of real-time remote biometric identification systems in public accessible spaces → irrelevant regarding cartel screening
  - High-risk under the stand-alone systems of Annex III

B. AI-driven Cartel Screening under the AI Act

- Annex III(6) lists seven types of AI systems intended to be used by law enforcement authorities
  - (III.6.a) making risk assessment of natural persons for (re)offending,
  - (III.6.b) polygraphs and other similar tools,
  - (III.6.c) deep fake detection tool,
  - (III.6.d) evaluating the reliability of evidence in the course of investigation or prosecution of criminal offences,
  - (III.6.e) predicting the (re)occurrence of an actual or potential criminal offence based on profiling of natural person or assessing personality traits and characteristics or past criminal behaviour of natural persons or groups,
  - (III.6.f) profiling of natural persons in the course of detection, investigation or prosecution of criminal offences, and
  - (III.6.g) makings crimes analytics regarding natural persons, allowing law enforcement authorities to search complex related and unrelated large data sets available in different data sources or in different data formats in order to identify unknown patterns or discover hidden relationships in the data.

B. AI-driven Cartel Screening under the AI Act

- Conclusion (?): Annex III focuses on criminal law; *ergo*, AI-driven cartel screening is not high-risk AI system
- Word count and conceptual analysis of “competition”
- Appears only six times in four different contexts
  - Removal of distortions of competition by creating a regulatory level playing field preventing the proliferation of nationally fragmented regimes (2)
  - International competition between undertakings developing AI systems (1)
  - communications between the market surveillance authorities (2)
  - The AI Act is “without prejudice to the application of Union competition law.” (1)

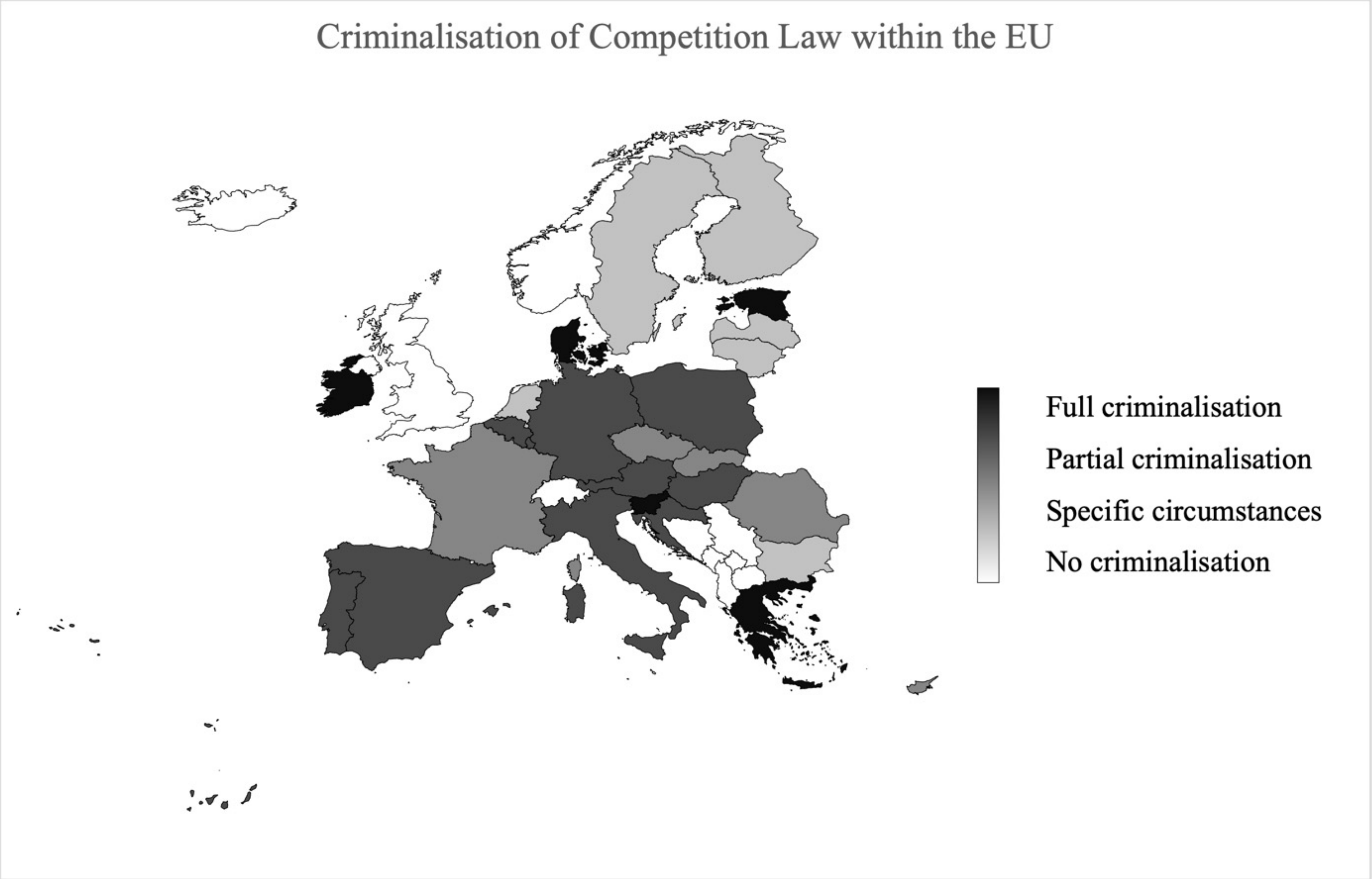
B. AI-driven Cartel Screening under the AI Act

- Law enforcement activity mentioned in Annex III
  - 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.

C. Criminalisation of Competition Law

- Shift in competition law proceedings from traditional firm-focused enforcement towards individual-focused punishment (Whelan 2014)
  - Sanction must have “a real deterrent effect” (ECJ Case 14/83)
  - “Prison is the inferno” (Harding and Joshua 2003)
- Cartelisation has been vilified
  - “Cancers on the open market economy” (Monti 2000)
  - “The most fundamental threat to competition” (Vestager 2021)
  - “The most egregious violations of competition law” (OECD 2002)
  - “The market’s most dangerous competitive vice” (Kovacic 2013)
  - “The supreme evil of antitrust” (*Verizon Communication*)
  - “The mafia in legitimate industries” (Gambetta and Reuter 1995)

C. Criminalisation of Competition Law



C. Criminalisation of 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?

D. Hard Core and Peripheral Criminal Law

- 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)

D. Hard Core and Peripheral Criminal Law

- Upshot? Competition law belongs to the criminal sphere for the ECtHR
  - Bid-rigging is criminal (*Société Stenuit v. France* 1992; *SA-Capital v Finland* 2019)
  - Abuse of dominance is criminal (*Lilly France S.A. v. France* 2002)
  - Price-fixing and market sharing are criminal (*A. Menarini Diagnostic S.R.L. v. Italy* 2011)
  - Prevention of parallel imports is criminal (*M. & Co v. Germany* 1990)
  - Obstruction during a dawn raid is criminal (*Produkcija v Slovenia* 2018)

D. Hard Core and Peripheral Criminal Law

- 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)

E. Peripheral Criminal Law under the AI Act?

- Question: 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?
- Answer: use a contextual approach
  - “the meaning of words lies in their use” (Wittgenstein 1958)
  - “the complete meaning of a word is always contextual, and no study of meaning apart from context can be taken seriously” (Firth 1935)
  - “You shall know a word by the company it keeps” (Firth 1957)
  - Considering the occurrences of word “criminal” and its cognates, derivatives, synonyms, singular and plural

	Word count	Contextualisation
Crime	13	Missing children; terrorism; arrest warrant; organised crime; predictive policing; malicious use and abuse of AI; See offence
Crimes	1	Terrorism
Criminal	54	Police; Detention; custodial sentence; recidivism (of children and young people); domestic violence, criminal record; See Crime
Criminals	1	Burglary; petty theft
Criminality	3	Recidivism, domestic violence; predictive policing
Offence	5	Those referred to in Council Framework Decision 2002/584/JHA, i.e., Participation in a criminal organisation; terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; corruption; fraud, including that affecting the financial interests of the European Communities within the meaning of the Convention of 26 July 1995 on the protection of the European Communities' financial interests; laundering of the proceeds of crime; counterfeiting currency, including of the euro; computer-related crime; environmental crime, including illicit trafficking in endangered animal species and in endangered plant species and varieties; facilitation of unauthorised entry and residence; murder, grievous bodily injury; illicit trade in human organs and tissue; kidnapping, illegal restraint and hostage-taking; racism and xenophobia; organised or armed robbery; illicit trafficking in cultural goods, including antiques and works of art; swindling; racketeering and extortion; counterfeiting and piracy of products; forgery of administrative documents and trafficking therein; forgery of means of payment; illicit trafficking in hormonal substances and other growth promoters; illicit trafficking in nuclear or radioactive materials; trafficking in stolen vehicles; rape; arson; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; sabotage.
Offences	21	Threat to public security; See offence
Offender	3	Penalties (Art. 71 AI Act)
Offenders	1	Terrorism; serious crimes
Infringement	9	Penalties (Art. 71), administrative fine for AI Act breach (Art. 72), Fundamental rights
Infringements	16	See infringement

E. Peripheral Criminal Law under the AI Act?

- Argument driven from the 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)
  - Yet tax and customs law are peripheral criminal law
    - Tax surcharge proceedings (ECtHR, *Jussila v. Finland*, 2006)
    - Tax poll (ECtHR, *Bendenoun v. France* 1994; ECtHR, *Benham v. The United Kingdom*, 1996)
    - Customs law (ECtHR, *Salabiaku v. France*, 1988)
    - VAT (ECJ, *Åklagaren v Hans Åkerberg Fransson*, 2013; ECJ, *Luca Menci, 2018*)

E. Peripheral Criminal Law under the AI Act?

- 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

IV. Conclusion

IV. Conclusion

- “*When all possibilities (…) become probabilities, every possibility is the next thing to a certainty*” (Melville, *Moby Dick*, 1851)
- Screening raises possibilities of collusion, nothing more (but also nothing less)
- Competition authorities have to remain aware of AIS’ limitation.
  - Data challenge
  - Algorithmic challenge
  - Human challenge
- If not, they might well be doomed to embody Ahab’s fate, equating probabilities and certainties

LIÈGE université
Cité