

Artificial Intelligence & Detection of Anticompetitive Behaviours

Jerome De Cooman

jerome.decooman@uliege.be

30 March 2023, UCL, Louvain-la-Neuve (Belgium)



A photograph of a grand architectural archway, likely from a university building. The arch is filled with the Latin inscription 'EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE'. Above the arch is a golden coat of arms featuring a crown, a shield, and two figures. Below the arch is a relief sculpture depicting several figures in classical attire. The scene is set against a white background with a purple diagonal overlay on the left and bottom.

EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

I. Introduction

Schinkel (2014)



PAC-MAN

1UP 00 HIGH SCORE 00

Consumer surplus



(National) Competition Authorities



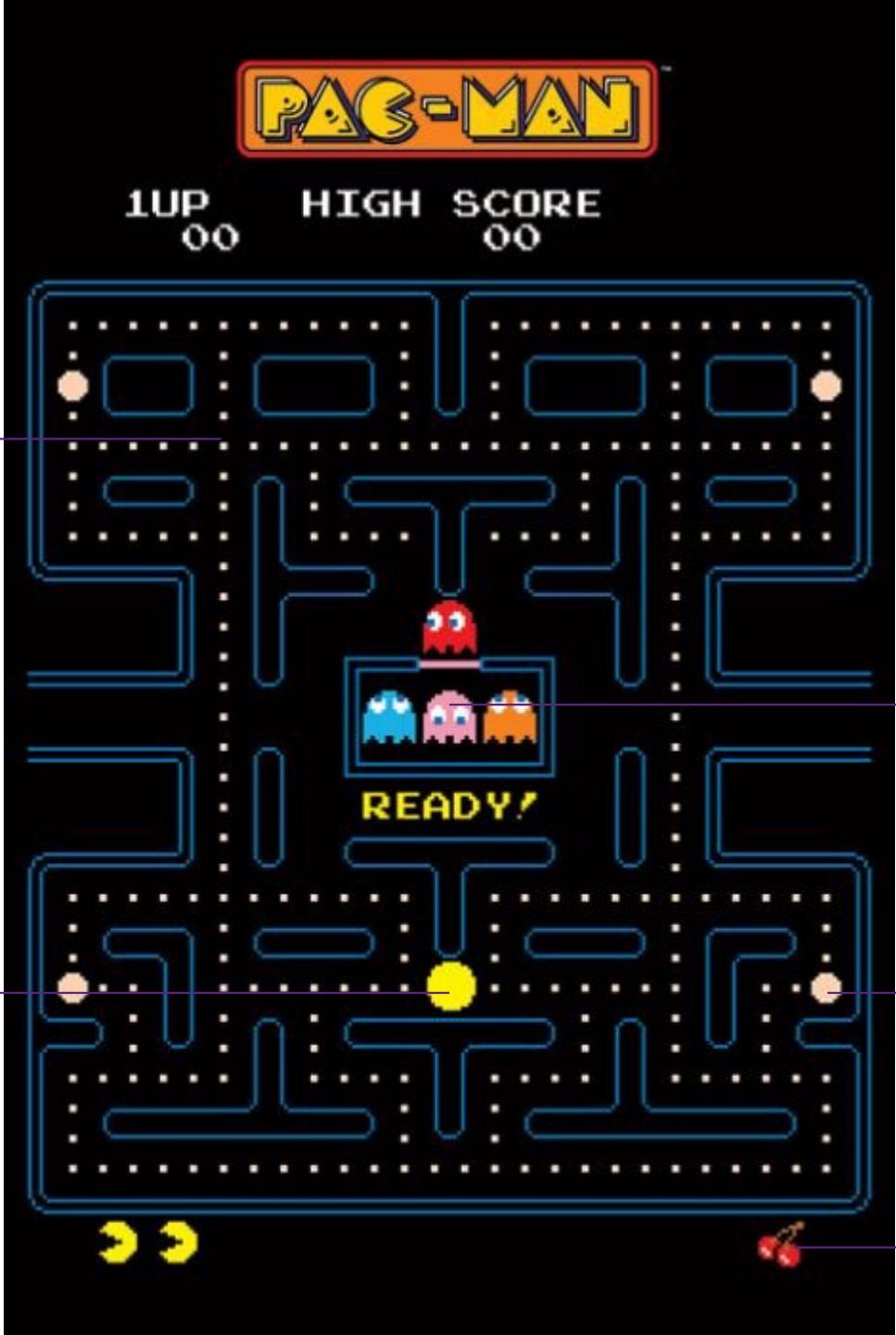
International cartel



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. The Economics of Cartelisation
- III. Soft Carrots and Hard Sticks: Sanctions and Leniency
 - A. Addressing the Participation Constraint: Sanction
 - B. Addressing the Incentive Constraint: Leniency Programme
- IV. An Alternative: Cartel Screening
 - A. Strengthening Competition Law Enforcement
 - B. Definition and Promises
- V. The Risks of Cartel Screening
 - A. Data Challenge
 - B. Algorithmic Challenge
 - C. Human Challenge
- VI. Competition law and the AI Act
- VII. Conclusion



EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

II. The Economics of Cartelisation



II. The Economics of Cartelisation

- ▶ Trust is the cement of society (Baker and Hurst 1998)
- ▶ Cartel does not escape this rule
- ▶ Analysing cartel through the lens of Morgenstern and von Neuman's game theory (1944)

		B	
		Remains silent (s_1)	Denounces A (s_2)
A	Remains silent (t_1)	(1, 1)	(3, 0)
	Denounces B (t_2)	(0, 3)	(2, 2)

II. The Economics of Cartelisation



- ▶ The prisoner's dilemma is
 - › Non-zero sum game of
 - › Complete and
 - › Imperfect information
- ▶ The lack of communication makes the strategy of denouncing the other the dominating one
 - › No Pareto optimality
 - › But Nash equilibrium
- ▶ In sequential prisoner's dilemma, risk of retaliation makes cooperation a prudent behaviour (Axelrod 1984)
 - › This leads to Axelrod's tit for tat strategy: A cooperates by default and deviate in t only if B deviates in $t-1$



II. The Economics of Cartelisation

- ▶ Cartel is an iterative prisoner's dilemma
 - › Cheating is the dominant strategy
 - › Cartel is an inherently unstable organisation
 - › Like mafia, cartel is a game of trust (Leslie 2004)
 - › Trust and retaliation solves the prisoner's dilemma

		B	
		Does not deviate (s_1)	Deviate (s_2)
A	Does not deviate (t_1)	(2, 2)	(0, 3)
	Deviate (t_2)	(3, 0)	(1, 1)



EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

III. Soft Carrots and Hard Sticks

- A. Addressing the Participation Constraint: Sanction
- B. Addressing the Incentive Constraint: Leniency Programme

III. Soft Carrots and Hard Sticks: Sanctions and Leniency



- ▶ Undertakings are (supposed to be) rational utility maximisers
 - › Participation constraint: cartelisation gain $>$ sanction
 - › Incentive constraint: cartelisation gain $>$ deviating gain
- ▶ Two ways to destabilise a cartel
 - › Increasing sanction (A)
 - › Increasing the gain driven from deviation (B)



A. Addressing the Participation Constraint: Sanction

- ▶ “the value of the punishment must not be less in any case than what is sufficient to outweigh that of the profit of the offence” (Bentham)
- ▶ Sanction > cartel gain → deter cartel formation
- ▶ However:
 - › This is true if detection probability = 100 % (Yeung 2004)
 - › Enforcement has a cost
 - › Undertakings may be risk averse, risk preferer or risk neutral

Expected Sanction

$$= \left(\frac{\text{Expected gain from cartelisation}}{\text{Probability of detection}} + \text{Enforcement Costs} \right) * \text{risk aversion factor}$$



A. Addressing the Participation Constraint: Sanction

- ▶ Upshot? The detection rate is of utmost importance
- ▶ Detection rate = approximately 15 % (Combe 2020)
- ▶ The tip of the iceberg (Ormosi 2013)
- ▶ Given a probability of cartel detection of approximately 15 per cent, this model is likely to propose high fine.
 - › Expected gain of cartelisation is, e.g., 10
 - › Probability of detection is 0,15
 - › Sanction is 66,67
- ▶ Does this model hold true in practice?



A. Addressing the Participation Constraint: Sanction

- ▶ Severe sanction is impracticable
 - › Is exemplary sentences legitimate? (Joshua and Harding 2003)
 - › Does sanction ultimately lead to an increase of prices or bankruptcy? (Werden and Simon 1987)
 - › Is harsh sanction proportionate? (Yeung 2004)
- ▶ Are undertakings rational economic actors?

Expected Sanction

$$= \left(\frac{\text{Expected gain from cartelisation}}{\text{Probability of detection}} + \text{Enforcement Costs} \right) * \text{risk aversion factor}$$

B. Addressing the Incentive Constraint: Leniency Programme



- ▶ Leniency is a way to give cartelists another (prisoner's) dilemma
- ▶ Break the omerta code amongst cartel offering amnesty to the first-in-the-door undertaking that provides evidence (Zingales 2008)

Position	Reduction	Reduction after investigation start
1st	Immunity	30-100%
2nd	30-50% of the fine	20-30%
3rd	20-30%	Up to 20%
Subsequent	Up to 20%	

B. Addressing the Incentive Constraint: Leniency Programme



- ▶ Benefits of leniency programme:
 - › Detection effect: detection of otherwise undetected cartel
 - › Savings effect: resource-efficiency
 - › Deterrence effect: harder to reach an agreement
 - › Discontinuation effect: harder to not deviate from the agreement
 - › Redress effect: compensation damages

B. Addressing the Incentive Constraint: Leniency Programme



► 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)
- › Incentive effect: if detection, then negotiation
- › Stabilisation effect: if deviation, then application for leniency as retaliation
- › Non-disclosure effect: without application for leniency, probability of detection very low
- › Savings side effect: affects *ex officio* investigation
- › Discouraging effect: downside of private enforcement



C. Interim Conclusion

- ▶ Questionable effectiveness of carrot-and-stick policy
 - › Sanction is a function of detection
 - › Yet, probability of detection is low
 - › Leniency is a way to increase the probability of detection
 - › Yet, probability of detection decreases the effectiveness of leniency
- ▶ “While there is a recognition that a leniency program is an immensely valuable tool (...) concerns arise when it is the only tool” (Harrington and Chang 2015)
- ▶ Another tool to increase the probability of detection?



EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

IV. Alternative: Cartel Screening

- A. Strengthening Competition Law Enforcement
- B. Definition and promises

A. 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
 - › 2014: “*We must take much better use of the great opportunities offered by digital technologies*” (Juncker)
 - › 2017: The Commission “*will continue to monitor the opportunities and challenges brought by artificial intelligence solutions*”
 - › 2017: 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*”

A. Strengthening Competition Law Enforcement



- › 2019: von der Leyen asked Vestager to make sure that “competition policy are fit for the modern economy”
- › 2020: White Paper on AI: how to equip law enforcement authorities, including competition law authorities
- › 2020: European Court of Auditors: scissors effect: reduction of market surveillance capacity and increasing of case’s complexity
- › 2021: the Single Market Programme proposed to improve competition enforcement (art. 3(2)(a)(i)) for instance with data-gathering and analysis tools (att. 8(2)(d)(i))

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 work?
- ▶ 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	<p>Low variance</p> <p>Sharp increase in high price-cost margin</p> <p>Sharp decline of price followed by sharp increase</p>
	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



- ▶ What about AI-driven cartel screening?
 - › 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
 - › AI-driven cartel screening draws the sketch of suspicious businesses by identifying the recurring characteristics (patterns) of cartels to improve the proactive detection of anticompetitive behaviours.



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



EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

V. Pitfalls

- A. Data Challenge
- B. Algorithmic Challenge
- C. Human Challenge



A. Data Challenge

Availability – Quality – Governance

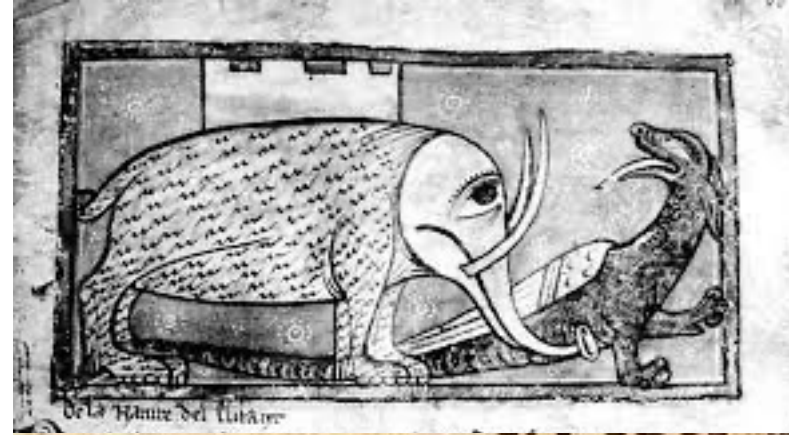


A. Data Challenge – Availability

- ▶ 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)
- ▶ *Caveat*: Problems may still arise with available large dataset (e.g., UK Screening for Cartels Tools:
 - › Training on 100 tenders involving 500 bids
 - › Distributed model

A. Data Challenge - Quality

- The Elephant Tale (Sanchez-Graells 2019)





A. Data Challenge – Quality

- ▶ The Elephant Tale (Sanchez-Graells 2019)
- ▶ Implications for AI:
 - › Training on the “entire universe of data” or on statistically representative data
 - › The quality of training dataset is critical: ”dirty data, bad predictions” (Richardson et al 2019)
 - › The elephant tale warns against the “distortionary effects likely to result from policy developed on the basis of poor data that misrepresents reality.” (Sanchez-Graells 2019)

A. Data Challenge – Quality



- ▶ Risk of Type II error – non detection of cartel
 - › “With oligopoly, everything is possible” (Stiegler 1964)
 - » *Animal Feed Phosphate Cartel*
 - » “None of the collusive markers identified are universal, and each must be used with caution” (Harrington 2008)
 - » “One target, one rule” (Tinbergen 1952)
 - › Interaction between collusive markers
 - » In principle, demand fluctuations hinder collusion
 - » But an increase in demand fosters collusion when entry barriers are sufficiently high
 - › Selection bias
 - » Are discovered cartel statistically representative of the whole population of cartel?



A. Data Challenge – Quality

- ▶ Risk of Type I error – mistakenly detecting a cartel
 - › Erroneously condemn competitive behaviour
 - › Waste of time and resources
 - › Structural screens are particularly at risk (Harrington 2008)
 - » This is not because the market presents the structural characteristics of collusion that there is collusion
 - › Screening does not distinguish between parallelism and anticompetitive behaviour
- ▶ // with an ultrasound of the thyroid that triggers the need for a biopsy?
(Abrantes-Metz 2013)



A. 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)



A. Data Challenge – Governance

- ▶ Competition authorities do not want to lag behind (e.g., UK CMA)
- ▶ “*It is a capital mistake to theorize before one has data*” (Conan Doyle 1889)
- ▶ Insight:
 - › The algorithmic cart should not be put before the data horse
 - › Construct a better data architecture before developing AI-driven cartel screening
 - » But the probability of detection is merely 15%
 - » Some competitive case *might* be undiscovered collusion
 - » Is reassessing past data even feasible?



A. Data Challenge – Governance

- ▶ Drawing inspiration from the AI Act: article 10
- ▶ AI system must respect “appropriate data governance” and management practices regarding training, validation, and testing datasets (art. 10(2))
- ▶ The training dataset has to be “complete” and “free of errors” (art. 10(3))
 - › Is this even possible?
 - › Is this require an *appropriate* level of completeness? If so, what is appropriate?



B. Algorithmic Challenge

Good Administration – Duty to state reasons – Explicability – Human oversight –
Transparency

B. Algorithmic Challenge – Good administration



- ▶ “Every person has the right to have his or her affairs handled impartially, fairly and within a reasonable time by the institutions and bodies of the Union.” (art. 41 EUCFR)
- ▶ This applies to administrative body that has to “gather, in a diligent manner, the factual elements necessary for the exercise of its broad discretion” (*Claire Staelen v European Ombudsman*)
- ▶ “the official shall take into consideration the relevant factors and give each of them its proper weight in the decision.” (art. 9 CGAB)
- ▶ The duty of care “although not explicitly listed in Article 41 CFR, is generally understood as a key component of good administration” (Forrester 2009)



B. Algorithmic Challenge – Duty to state reasons

- ▶ “The obligation of the administration to give reasons for its decisions.” (art. 41(2)(c) CFR based on art. 296 TFEU)
- ▶ No decision can be made on brief or vague grounds; or without an individual reasoning
- ▶ A decision should contain the facts, the law, and the facts-to-law leap (Fink and Finck 2022)
- ▶ Rationale
 - › Protect against arbitrariness (Nehl 2009)
 - › Ensure effective judicial review (art. 47 CFR)



B. Algorithmic Challenge – Duty to state reasons

- ▶ The EC has to respect the duty to state reason (*Martinair*)
 - › During preliminary investigations (e.g., *Hoechts*, *Roquette 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”?

B. Algorithmic Challenge – Duty to state specific reasons



- ▶ Duty to state specific reasons (art. 20(4) Reg. 1/2003)
 - › Describe the features and nature of the suspected infringements
 - › Describe the presumed facts the EC intends to investigate
 - › Indicate the sectors and market allegedly concerned
- ▶ Rationale
 - › Undertakings has to assess the scope of their duty to cooperate
 - › Safeguarding their rights of the defence (*Hoescht*)
- ▶ In practice, “very general terms” might still contain “the essential indications” required (*Dow Benelux; Nexans; Prysmian*)



B. Algorithmic Challenge – Duty to state reasons

- ▶ Is red flags raised by cartel screening a reasonable grounds for suspicion? (*Roquette frères*)
- ▶ Is the statement of reasons “excessively succinct, vague and generic”? (*Heidelberger Cement*)
- ▶ It depends:
 - › Hypo 1: “The AI system said so” is definitely “excessively succinct, vague and generic” (Fink and Finck 2022)
 - › Hypo 2: if human officer is able to disclose how the different parameters were weighted and to what extent the recommendation was decisive in the final decision, then the duty to state reasons will not be infringed (Yeung 2019)



B. Algorithmic Challenge – Duty to state reasons

- ▶ Hypo 1 or hypo 2 depends on the AI system's opacity
 - › Public officer's illiteracy (Fink and Finck 2022)
 - › Intrinsic opacity (Pasquale 2019)
- ▶ When neither the factors nor their weight are known, then a reference to the AI system's recommendation
 - › cannot fulfil the duty to state reasons
 - › Cannot ensure an effective judicial review of the administrative decision



B. Algorithmic Challenge – Explicability (?)

- ▶ “the degree to which explicability is needed is highly dependent on the context and the severity of the consequences if that output is erroneous or otherwise inaccurate.” (HLEG 2019)
- ▶ Dawn raid are:
 - › Highly intrusive and traumatic for staff (Aslam and Ramsden 2008)
 - › Sometimes conducted without judicial warrant
- ▶ The degree of explicability is expected to be high

B. Algorithmic Challenge – Human Oversight



- ▶ 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)

- ▶ 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*” (art. 14(1) AIA)
 - › to “fully understand the capacities and limitations” of the AI systems (art. 14(4)(a))
 - › to be able to interpret the system’s output (art. 14(4)(c) and 13(1)),
 - › to be able to choose when (not) to use the AI system and when to disregard its output (14(4)(d)).



B. Algorithmic Challenge – Transparency

- ▶ 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 AIA).
- ▶ This requires public officers to receive “appropriate knowledge and tools to comprehend and interact with AI systems to a satisfactory degree and, where possible, be enabled to reasonably self-assess or challenge the system.” (HLEG 2019)
- ▶ Users should receive “instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users” (art. 13(2) AIA)

B. Algorithmic Challenge – Effective Human Oversight



- ▶ “Public enforcers have the ability to exercise oversight in line with their mandate” (HLEG 2019)
 - › Cf. Art. 41 CFR
 - › human control on decision-making process has to remain effective (EGE 2018)
- ▶ AI systems should not “become the primary decision makers” that “take human decision making out of the process.”
- ▶ Concrete human oversight prevents “the mindless rubberstamping of AI-generated proposed decision” (Sanchez Graells 2021)



C. Human Challenge

Bias and noises – Discretion – Automation bias – Four-eyes principle

C. Human Challenge – Biases and Noises



- ▶ 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)



C. Human Challenge – Biases and Noises

- ▶ To err is human; but human also predictably err (Thaler and Sunstein 2008)
- ▶ Bias: “any systemic error that inclines people’s judgements in a particular direction” (Sunstein 2022)
- ▶ 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 preconceived opinion
 - › Diagnostic momentum or hindsight bias: the pursuit of an action previously instigated by someone else without considering any new information and changing plan accordingly (*a fortiori* if hierarchical superior)



C. Human Challenge – Biases and Noises

- ▶ Within EU competition law proceedings: Combination of investigative and decision-making powers
- ▶ **Prosecutorial bias:** “investigatory teams that have dedicated months to finding enough evidence to support an infringement might suffer from the dreaded ‘tunnel vision’, which could cause them to adopt an unfair or biased decision.” (Lachnit 2016)
 - › biased investigation favouring information concluding to a collusive behaviour (**confirmation bias**) and discarding the others (**hindsight bias and diagnosis momentum**) (Wils 2004)
 - › **Commitment bias:** the unwillingness to adopt a decision that contradict what officials have done in the past due to the involvement of “both the Commission’s human resources and reputation capital” (Teleki 2021)
 - › **Policy bias:** high level of enforcement to keep-up with the statistics (Wils 2004) and because “promotion flow from taking decision” (Forrester 2013)

C. Human Challenge – Biases and Noises



- ▶ Bias is systematic; noise is an “unwanted variability in judgements” (Sunstein 2022)
 - › Occasion noise: noise personal to a human: fatigue, blood sugar, local news or weather
 - › Level noise: a decision depends on the decisionmaker (lenient or severe)
 - › Pattern noise: leniency or severity depends on patterns of the decisionmaker

		Grounds			
		W	X	Y	Z
Decision-maker	A	receptive	receptive	indifferent	indifferent
	B	receptive	receptive	indifferent	indifferent
	C	indifferent	indifferent	receptive	receptive
	D	indifferent	indifferent	receptive	receptive

C. Human Challenge – The Exercise of Discretion



- ▶ 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).
- ▶ 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)



C. Human Challenge – Automation bias

- ▶ Automation bias (or algorithmic dumbfounding), *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.



C. Human Challenge – Automation bias

- ▶ Risk of self-fulfilling prophecies
 - › Recommendation in $t+1$ is based on recommendation given in t
 - › Feedback loop
 - › Path-dependency
 - › Critical given scarce resources of Authorities → systematic exclusion of some cases
 - › Solution: reduce weight of recommendation t when used as input in $t+1$

C. Human Challenge – The Need for a Four-Eyes Principle



- ▶ This has been forecasted by the EU legislator
- ▶ “remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (‘automation bias’), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons” (art. 14(4)(b) AI Act)
- ▶ Effective human oversight
- ▶ With this formulation, the AIA is not sufficient
- ▶ Proposal: four-eyes principle

C. Human Challenge – The Need for a Four-Eyes Principle



- ▶ Four-eyes principle: A approves both the decision and statement of reasons of B
- ▶ Not alien to competition law
 - › Woodrow Wilson
 - › French Competition Authorities
 - » The Investigation Service (*Le Service d'Instruction*): opens investigation, gathers evidence
 - » The Board (*Le Collège*): takes the decision
 - › Belgian Competition Authorities
 - » The Investigation service (*Auditorat*)
 - » The Board (*Le Collège de la concurrence*)

C. Human Challenge – The Need for a Four-Eyes Principle



- ▶ The bicephalic structure enhances procedural fairness (Lasserre 2009)
- ▶ The Authority is no more “the ‘judge, jury, and executioner’ of its own cases.” (Lachnit 2016)
- ▶ Unbiasing decisionmaking: solve the commitment bias
- ▶ AI-driven cartel screening raises similar issue; calls for similar solution
- ▶ An independent team scrutinise the AI and its use: this mitigate the automation bias

C. Human Challenge – The Need for a Four-Eyes Principle



- ▶ Easy to implement in France, Belgium, and other bicephalic institutions
 - › This will prolong the duration of case
 - › But that extra-time might not be wasted
- ▶ Complex to implement in “all-in-one” competition authority (e.g., EC):
 - › No need to split DG Comp
 - › Extension of the Hearing Officer’s role
 - » Already ensures the effective exercise of procedural rights
 - » Already an independent arbiter
 - › The Hearing Officer might well be the proper public overseer of AI-driven cartel screening.



EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

VI. 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

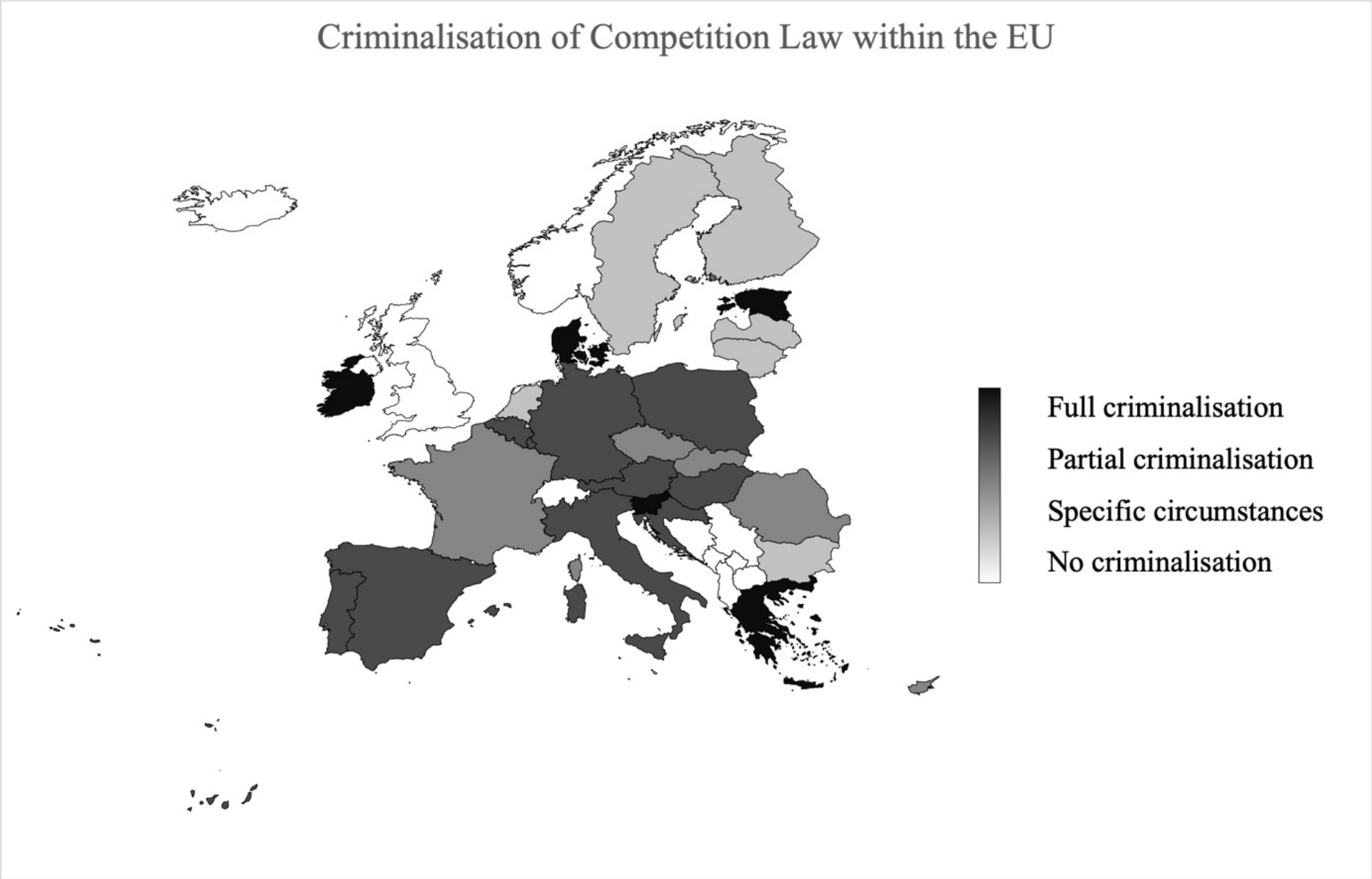
- ▶ Law enforcement activity mentioned in Annex III
 - › Annex III submits to mandatory requirements AI systems used by law enforcement authorities “AI systems intended to be used by law enforcement authorities for predicting the occurrence or reoccurrence of an actual or potential criminal offence based 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 backdoor 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

A photograph of a classical building facade, likely the University of Liège. The image shows a large archway with a Latin inscription. Above the arch is a golden coat of arms featuring a crown, a shield, and two figures. Below the arch is a relief sculpture depicting several figures in classical attire. The image is partially overlaid by a purple geometric shape in the bottom-left corner and a white geometric shape in the bottom-right corner.

EN DVLCIS PATRIÆ SPEM LAVRV CINGAT VT IPSE

VII. Conclusion

VII. 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



VII. 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