Market and Competition Law Review / VOLUME VI / No. 1 / APRIL 2022

Humpty Dumpty and High-Risk AI Systems: The *Ratione Materiae* Dimension of the Proposal for an EU Artificial Intelligence Act*

*Jérôme De Cooman***

ABSTRACT: On 21 April 2021, the European Commission proposed a Regulation laying down harmonised rules on artificial intelligence (hereafter, "AI"). This so-called Artificial Intelligence Act (hereafter, the "Proposal") is based on European values and fundamental rights. Far from appearing *ex nihilo*, it deeply relies on the European Ethics Guidelines proposed by the independent high-level expert group on AI set up by the European Commission. In addition, the European Commission's White Paper on AI already called for a regulatory framework that should concentrate on a risk-based approach to AI regulation that minimises potential material and immaterial harms. The Proposal, internal market oriented, sets up a risk-based approach to AI regulation that distinguishes unacceptable, high, specific and non-high-risks. First, AI systems that produce unacceptable risk are prohibited by default. Second, those that generate high risk are subject to compliance with mandatory requirements such as transparency and human oversight. Third, AI systems interacting with natural persons have to respect transparency obligations. Fourth, developers and users of non-high-risk AI systems should voluntarily endorse requirements for high-risk AI systems. Exploring the origins of the AI Act and the *ratione materiae* dimension of the Proposal, this article argues that the very choice of what is a high-risk AI system and the astounding complexity of this definition are open to criticism. Rather than a full-extent analysis of the Proposal's requirements, the article focuses on the definition of what is an unacceptable, high, specific and non-high-risk AI system. With a strong emphasis on high-risk AI systems, the Commission comes dangerously close to the

* Date of Reception: 3 December 2021. Date of Acceptance: 1 February 2022.
DOI: https://doi.org/10.34632/mclawreview.2022.11304.

** Ph.D. student, research and teaching assistant, EU Legal Studies, Liege Competition and Innovation Institute (LCII), University of Liege (ULiege). Bât. B33. Droit européen de la concurrence. Quartier Agora. Place des Orateurs, 1. 4000 Liege, Belgium. Jerome.decooman@uliege.be. ORCID ID: 0000-0001-8721-5730.

pitfall this article humorously labels as the Humpty Dumpty fallacy, to pay tribute to the nineteenth century English author Lewis Carroll. Just because the Commission exhaustively enumerates high-risk AI systems does not mean the residual category displays non-high-risk. To support this argument, this article introduces recommender systems for consumers and competition law enforcement authorities. Neither of these two examples fall under the AI Act scope of application. Yet, the issues they have raised might well be qualified as high-risk in a different context. In addition, the AI Act, although inapplicable, could have provided a solution.

KEYWORDS: Artificial Intelligence Act, risk regulation, product safety, recommender systems, EU competition law

1. Introduction

On 21 April 2021, the European Commission published a proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts (hereafter, "Proposal").[1] This Proposal, based on European Union (hereafter, "EU") values and fundamental rights, suggests a risk-based approach to artificial intelligence (hereafter, "AI") that distinguishes between unacceptable, high, specific or non-high-risks.

The origins of this multi-layered risk-based approach can be found in the 2018 EU Ethics Guidelines and the 2019 White Paper on AI. The first document left its mark with the key requirements reproduced in the Proposal, such as transparency and human oversight. The second can be said to have initiated the risk regulation approach.

The Proposal for a Regulation constitutes the European response to an intense degree of competition amongst three big players – the United States of America, the People's Republic of China and the EU – to fill the perceived regulatory void in the development of AI systems and their introduction in our societies.[2] Today's race to AI therefore drives "a race to

[1] European Commission, *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final*, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[2] The White House, *The Biden Administration Launches AI.gov Aimed at Broadening Access to Federal Artificial Intelligence Innovation Efforts, Encouraging Innovators of Tomorrow*, May 05,

AI regulation".[3] Building on the economic idea of the first mover advantage, regulators over the world aim to be the first to adopt a regulation that will shape AI development and impose compliance cost to others.[4] In this regard, it is worth noting the Proposal is a world premiere. This is good news for the EU, as AI systems constitute a colossal financial windfall, especially regarding the innovation capital.[5] However, they also raise substantial ethical and legal risks.[6] Still, since then, they have only been handled through unenforceable ethical guidelines.[7]

New risks emerge from technological evolution.[8] Our "risk society" is also "a regulatory state".[9] The combination of these two elements results in four types of risk regulations: the regulation of elements that pose risks to society (type I), the "tailoring of rules or standards to fit the particular risks to which the conduct of that particular firm gives rise" (type II), and the management of the risk that a regulatory agency does not operate properly due, on the one hand, to its own internal organization (type III), or, on the other hand, to disobedience of regulated firms (type IV).[10] The

---

2021, https://www.whitehouse.gov/ostp/news-updates/2021/05/05/the-biden-administration-launches-ai-gov-aimed-at-broadening-access-to-federal-artificial-intelligence-innovation-efforts-encouraging-innovators-of-tomorrow/. Expert committee of China's Ministry of Science and Technology (MOST), *Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence*, June 17, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/ (translation).

[3] Nathalie A. Smuha, "From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence", *Law, Innovation and Technology* 13, no. 1 (2021): 57-84.

[4] *Ibidem*, 74-75.

[5] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Policy and Investment Recommendations for Trustworthy AI*, June 26, 2019, https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence.

[6] Vincent C. Müller ed., *Risks of Artificial Intelligence* (Boca Raton: Chapman and Hall/CRC 2015). Alexey Turchin and David Denkenberger, "Classification of global catastrophic risks connected with artificial intelligence", *AI & Society* 35 (2020): 147-163.

[7] Luciano Floridi, "Establishing the rules for building trustworthy AI", *Nature Machine Intelligence* 1 (2019): 261.

[8] Aaron Wildavsky, *Searching for Safety: Social Theory and Social Policy* (Abingdon: Routledge 2017). Robert Baldwin, ed., *Law and Uncertainty: Risks and Legal Processes* (London: Kluwer Law International, 1997).

[9] Ulrich Beck, *Risk Society: Towards a New Modernity* (London: Sage, 1992). Giandomenico Majone, "The rise of the regulatory state in Europe", *West European Politics* 17, no. 3 (1994): 77-101.

[10] Julia Black, "Managing regulatory risks and defining the parameters of blame: A focus on the Australian Prudential Regulation Authority", *Law & Policy* 28, no. 1 (2006): 3-4.

Proposal belongs to the type I risk regulation. Risk is the object of regulation and its justification.[11]

The Proposal distinguishes AI systems that raise unacceptable risk (prohibited), high risk (subject to compliance with mandatory requirements), specific risk (transparency obligations for those interacting with natural persons) and non-high-risk (voluntarily endorsed codes of conduct).

Yet, the Proposal has deficiencies. Its first and foremost drawback is its complex *ratione materiae* dimension. With a strong emphasis on high-risk AI systems, the Commission comes dangerously close to the pitfall this article humorously labels as the Humpty Dumpty fallacy, to pay tribute to the nineteenth English writer Lewis Carroll.[12] The very choice of words has its importance. Just because the Commission exhaustively enumerates high-risk AI systems does not mean the residual category displays non-high-risk. This article argues some AI systems still exhibit high risks, although excluded from this qualification.

To build this argument, this article proposes a threefold structure. The first part recalls the EU background that paved the way for the Proposal (2). The second part, explanatory by nature, presents the typology of risk introduced by the Proposal and dives deeper in the definition of unacceptable, high, specific or non-high-risks (3). The third and final part discusses the Humpty Dumpty fallacy. The very choice of what is a high-risk AI system and the astounding complexity of this definition are open to criticism. Recommender systems and EU competition law enforcement provide the most striking illustrations of this pitfall (4).

2. Background

The AI Regulation Proposal does not come from nowhere. The EU reflection on AI is part of the strategy for a Digital Single Market.[13] In May 2017, the European Commission published its mid-term assessment of the implementation of this strategy.[14] At the same time, both the

[11] Julia Black, "The role of risk in regulatory processes", in *The Oxford Handbook of Regulation*, ed. Robert Baldwin *et al.* (Oxford: Oxford University Press, 2010): 304.

[12] Lewis Carroll, *Through the Looking-Glass, and What Alice Found There* (London: Macmillan, 1872).

[13] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final*, May 6, 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

[14] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the*

Parliament[15] and the European Council[16] recommended the Commission to present an EU approach to AI. This was done with the Communication on Artificial Intelligence for Europe on 25 April 2018.[17] Its ambition was, in particular, to guarantee an appropriate ethical and legal framework based on EU values and fundamental rights. It is worth noting this did not leave aside Member States. They signed a declaration of cooperation on 10 April 2018,[18] and a new coordinated plan on AI was published on 21 April 2021.[19] Upshot? The Commission set up an independent high-level expert group on AI (hereafter, "HLEG").[20] The HLEG published the Draft Ethics Guidelines on 18 December 2018.[21] After a public consultation, whose results were published on 12 February 2019,[22] the Ethics Guidelines were published on 8 April 2019[23] and endorsed the same day

---

Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, COM(2017) 288 final, May 10, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0228.

[15] European Parliament, *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051.

[16] General Secretariat of the Council, *European Council Meeting – Conclusions, EUCO 14/17*, October 19, 2017, http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf.

[17] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, COM(2018) 237 final*, April 25, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.

[18] *EU Declaration on Cooperation on Artificial Intelligence*, April 10, 2018, https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence.

[19] European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Fostering a European approach to Artificial Intelligence, COM(2021) 205 Final*, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:205:FIN.

[20] European Commission, *AI HLEG – Steering group of the European AI Alliance*, https://ec.europa.eu/futurium/en/european-ai-alliance/ai-hleg-steering-group-european-ai-alliance.

[21] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Draft Ethics Guidelines for Trustworthy AI: Working Document for stakeholders' consultation*, December 18, 2018, https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai.

[22] European Commission, *Stakeholder Consultation on Guidelines' first draft*, February 19, 2019, https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/stakeholder-consultation-guidelines-first-draft.

[23] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, April 8, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

by the Commission in its plan to build trust in human-centric AI.[24] On 26 June 2019, the HLEG published their policy and investment recommendations for trustworthy AI[25] and opened an evaluation phase of the Ethics Guidelines.[26] This ended on 1 December 2019.[27] The HLEG then published a revised (and final) version of the assessment list for trustworthy AI (ALTAI) on 17 July 2020.[28] Meanwhile, the President of the European Commission, Ursula von der Leyen, promised to put forward a legislative proposal for AI.[29] This was followed by the publication of a White Paper on AI to propose a European approach to excellence and trust on 19 February 2020.[30] Capitalizing on the seven requirements developed by the HLEG,[31] the Commission warned in its White Paper that AI can cause both material[32] and immaterial harms[33] and therefore calls for a regulatory framework that "should concentrate on how

---

[24] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence, COM(2019)168 final*, April 8, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0168.

[25] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Policy and Investment Recommendations for Trustworthy AI*, June 26, 2019, https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence.

[26] European Commission, *EU artificial intelligence ethics checklist ready for testing as new policy recommendations are published*, June 26, 2019, https://ec.europa.eu/digital-single-market/en/news/eu-artificial-intelligence-ethics-checklist-ready-testing-new-policy-recommendations-are.

[27] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Trustworthy AI Assessment List*, June 26, 2019, https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/register-piloting-process-0.

[28] Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, July 17, 2020, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

[29] Ursula von der Leyen, *A Union that strives for more: My agenda for Europe*, July 16, 2019, https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf.

[30] European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final*, February 19, 2020, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[31] These seven requirements are human agency and oversight (1), technical robustness and safety (2), privacy and data governance (3), transparency (4), diversity, non-discrimination and fairness (5), societal and environmental well-being (6), and accountability (7). HLEG, *ALTAI*, 2020.

[32] EC, *White Paper*, 2020: 10 ("safety and health of individuals, including loss of life, damage to property").

[33] *Ibidem* ("loss of privacy, limitations to the right of freedom of expression, human dignity, discrimination for instance in access to employment").

to minimize the various risk of potential harm".[34] A year later, the Commission re-emphasised in its 2030 Digital Compass its ambition to make the EU a leader in ethical AI.[35] Seven weeks after this communication, the risk-based approach to AI regulation proposed in the White Paper was fully fleshed out in the Proposal, taking into account the comments from public consultation on the White Paper that ran from 19 February to 14 June 2020.[36]

The proposal has not been made in isolation. Indeed, numerous other (mostly non-binding) initiatives had been undertaken in this context. After the adoption of Civil Rules on Robotics,[37] the European Parliament also adopted non-binding Resolutions on AI ethics,[38] liability,[39] copyright,[40] criminal law,[41] education, culture and the audio-visual sector.[42] In addition, and to state the obvious, the Proposal has to respect the EU Charter of Fundamental Rights (hereafter, "EU Charter") and EU secondary laws, including the General Data Protection Regulation,[43] the Law Enforcement

---

[34] *Ibidem*.

[35] European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions – 2030 Digital Compass: The European way for the Digital Decade, COM(2021) 118 final*, March 9, 2021, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

[36] European Commission, *Public consultation on the AI White Paper: Final Report*, November 2020, https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence.

[37] EP, *Civil Law Rules on Robotics*, 2017.

[38] European Parliament, *European Parliament resolution of 20 October 2020 on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL)*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html.

[39] European Parliament, *European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence, 2020/2014(INL)*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

[40] European Parliament, *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI)*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html.

[41] European Parliament, *European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI)*, https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf.

[42] European Parliament, *European Parliament Draft Report, Artificial intelligence in education, culture and the audio-visual sector, 2020/2017(INI)*, https://www.europarl.europa.eu/doceo/document/A-9-2021-0127_EN.html.

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJEU L 119/1, May 4, 2016.

Directive,[44] Regulation 2019/1020 on Market Surveillance,[45] and the New Legislative Framework (hereafter, "NLF").

3. EU Risk-Based Approach to AI Regulation

The public consultations that occurred after the release of the EU Draft Ethics Guidelines for Trustworthy AI, and the White Paper made clear that a precise definition of AI and a risk ladder were required.[46] The European Commission had therefore no choice but to propose a sectoral and case-by-case approach, rather than a one-size-fits all or blanket regulation. The Proposal distinguishes AI systems that create unacceptable risk (1), high risk (2), specific risk (3) and non-high-risk (4). The concept of risk itself is however not defined in the Proposal, except incidentally, when the Commission explains peril comes from "a high risk of harm to the health and safety or the fundamental rights of persons" (recital 32).

a. Unacceptable Risks

AI systems that create unacceptable risk are prohibited (art. 5). Importantly, military applications are excluded from this qualification (art. 2(3)). With this exception in mind, AI systems that either use subliminal manipulation of natural persons' consciousness (art. 5(1)(a)) or exploit vulnerabilities of a specific group of persons due to their characteristics, *e.g.*, age, physical or psychological disability (art. 5(1)(b)), are prohibited because they are deemed to raise unacceptable risks by distorting people's behaviour in a way that is likely to cause physical or psychological harm.

The ban also covers the use by public authorities of AI systems that score natural persons based on their personal and social behaviour, known or predicted (art. 5(1)(c)), that lead to detrimental or unfavourable treatment of certain natural persons or whole groups either "in social contexts which are unrelated to the contexts in which the data was originally generated or

---

[44] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89.

[45] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No. 305/2011, OJ L 169, 1-44.

[46] Jerome De Cooman, "Éthique et intelligence artificielle: l'exemple européen", *Revue de la Faculté de Droit de l'Université de Liège* 1 (2020): 79-123.

collected" (art. 5(1)(c)(i)), or that is "unjustified or disproportionate to their social behaviour or its gravity" (art. 5(1)(c)(ii)).

Finally, the use of 'real-time' remote biometric identification systems in public physical spaces for the purpose of law enforcement is a prohibited practice (art. 5(1)(d)) – *i.e.*, an AI system that aims at identifying without significant delay "natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge of the user of the AI system whether the person will be present and can be identified" (art. 3(36)). Such systems are exceptionally authorised when strictly necessary to search for specific potential victims of crime, including missing children (art. 5(1)(d)(i)); prevent specific, substantial and imminent threat to natural persons' physical safety, including terrorist attacks (art. 5(1)(d)(ii)); or one of the thirty-two criminal offences referred to in article 2(2) of the Council Framework Decision and punishable by a custodial sentence or a detention order for a maximum period of at least three years (art. 5(1)(d)(iii)).[47] In case they are exceptionally authorised, law enforcement authorities will carry out a cost-benefit analysis (art. 5(2)(a) and (b)) and will need an *ex ante* authorisation granted by either a judicial or an independent administrative authority (art. 5(3)).

[47] Art. 2(2) of Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States – Statements made by certain Member States on the adoption of the Framework Decision (2002/584/JH A), OJ L190/1 ("the following offences, if they are punishable in the issuing Member State by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined by the law of the issuing Member State, shall, under the terms of this Framework Decision and without verification of the double criminality of the act, give rise to surrender pursuant to a European arrest warrant: 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").

b. High Risks

High-risk AI systems are those that threaten either health and safety or fundamental rights of natural persons. They are not prohibited, but subject to compliance with mandatory requirements such as high quality data governance (art. 10), documentation and traceability (arts. 11 and 12), transparency (art. 13), human oversight (art. 14), and accuracy and robustness (art. 15), among others.

There are two categories of high-risk AI systems. The first one comprises "AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment".[48] AI systems raise high risks due to the sectors' particular characteristics in which they are used and – cumulatively – the particular way they are used. The second category includes "other stand-alone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III".[49] This acknowledges that, notwithstanding the particular sector concerned, "there may also be exceptional instances where, due to the risk at stake, the use of AI applications for certain purposes is to be considered as high-risk as such".[50]

i. High-Risk AI Systems Not Covered by Sectorial Product Legislation

Annex III lists eight categories in which an AI system shall be qualified as high-risk. The first area is biometric identification and categorisation of natural persons (1). Such systems are, in principle, forbidden when used for the purpose of law enforcement. It deserves to be questioned, therefore, whether they will be used in other fields as well. To the extent that this is the case, high-risk AI systems regulatory obligations would apply to them. The second is management of operation of critical infrastructure such as road traffic or energy supply (2). The third is education and vocational training, including assessment required for admission to educational institutions (3). The fourth is workers recruitment, such as screening and filtering applications (4.a), as well as task allocation and performance monitoring (4.b). The fifth is access to essential public and private services, *e.g.*, eligibility for public assistance assessment (5.a), credit scoring (5.b), and

[48] EC, *Proposal*, 13.

[49] *Ibidem*. European Commission, *Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM2021) 206 final*, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:206:FIN.

[50] EC, *White Paper*, 2020: 18.

dispatching of first aid services (5.c). The sixth concerns law enforcement and encompasses individual risk assessment (6.a), emotion (6.b) or deep fake detection tool (6.c), evaluation of evidence reliability assessment tool (6.d), predictive policing (6.e), profiling (6.f), and data analysis allowing the discovering of hidden patterns and information (6.g). The latter category is quite broad. The seventh is similar to the previous one, although in a migration, asylum and border control context, and includes emotion (7.a) risk assessment (7.b), verification of authenticity of documents (7.c) and eligibility to asylum and other procedures (7.d) tools. Finally, the eighth refers to factual and legal research and interpretation tools used by judicial authorities (8.a). It is worth noting that the European Commission will be empowered to amend this list (art. 7).

To label some AI systems that are not covered by a sectorial product legislation as high-risk, the Commission has applied a risk assessment methodology, described as the evaluation "whether the AI system and its intended use generates a high-risk to the health and safety and/or the fundamental rights and freedom of persons" based on criteria set up in the Proposal.[51] These are especially the intended purposes of the AI system (art. 7(2)(a)), the extent to which the use of an AI system has already caused harm to the health and safety or adverse impact on the fundamental rights (art. 7(2)(c)), or the extent to which potentially harmed or adversely impacted persons are in a vulnerable position (art. 7(2)(f)).

ii. High-Risk AI Systems Covered by Sectorial Product Legislation

The first category of high-risk AI systems is much more complex to define, as it relies on numerous other EU secondary legislation instruments. There are two cumulative conditions to consider an AI system as high-risk.

The first condition is twofold. On the one hand, the AI system must be used as a product or a safety component of it (art. 6(1)(a)), *i.e.*, a component that fulfils a safety function whose failure or malfunction endangers the health and safety of persons or property (art. 3(14)).

On the other hand, the aforementioned product must be covered by one of the EU harmonisation instruments listed in Annex II. The twelve first instruments are part of the NLF, *i.e.*, machinery (II.A.1), toys safety

[51] European Commission, *Commission Staff Working Document Impact Assessment Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, SWD(2021) 84 Final, Part 1/2, 50.

(II.A.2), recreational craft and personal watercraft (II.A.3), lifts (II.A.4), equipment and protective systems intended for use in potentially explosive atmospheres (ATEX) (II.A.5), radio equipment (II.A.6), pressure equipment (II.A.7), cableway installations (II.A.8), personal protective equipment (II.A.9), gas appliances (II.A.10), medical devices (II.A.11) and in vitro diagnostic medical devices (II.A.12). Annex II adds seven other instruments of EU secondary legislation that belongs to the so-called old approach. They consist of approval and market surveillance of two- or three-wheel vehicles and quadricycles (II.B.2), of agricultural and forestry vehicles (II.B.3), and motors vehicles and their trailers, including systems, components and technical units, with an emphasis on protection of vehicle occupants and vulnerable road users (II.B.6). They also refer to marine equipment (II.B.4), rail system interoperability (II.B.5), and civil aviation security (II.B.1), including unmanned aircrafts and their engines, propellers, parts and remote-control equipment (II.B.7).

Per the second condition, an AI system will be qualified as a high-risk one when this system, either a safety component or a product, must be assessed by a third-party whose role is to evaluate the product's conformity with the EU harmonisation legislation listed in Annex II (art. 6(1)(b)). This is only common sense. Some sectors were harmonised before AI, so the horizontal framework created by the AI Act should merely actualise safety legislation. AI systems listed in Annex II are considered high-risk because products regulated under the NLF or the old approach are subject to a third-party conformity assessment that "already presupposes a risk assessment on the safety risks posed by the products covered by that instrument".[52]

c. Specific Risks

Title IV of the Proposal imposes transparency obligations for AI systems that interact with natural persons, such as chatbots (art. 52(1)). Emotion recognition systems[53] and biometric categorisation systems[54] (art. 52(2))

---

[52] European Commission, *Commission Staff Working Document Impact Assessment, Annexes Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, SWD(2021) 84 Final*, Part 2/2, 38.

[53] Art. 3(34) Proposal defines "emotion recognition system" as "an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data".

[54] Art. 3(35) Proposal defines "emotion recognition system" as "an AI system for the purpose of assigning natural persons to specific categories, such as sex, age, hair colour, eye colour, tattoos, ethnic origin or sexual or political orientation, on the basis of their biometric data".

are similarly targeted. Such systems must be designed in a way that natural persons know they interact with or are exposed to an AI system.[55] In the same vein, users of deepfake technology – *i.e.*, "hyper-realistic videos using face swaps that leave little trace of manipulation"[56] – have to disclose that the content has been manipulated or artificially generated (art. 52(3)).

d. Non-high-risks

Except for Title IV, which targets certain AI systems raising specific risks and imposes transparency obligations, the Proposal dichotomises high risk and non-high-risk AI systems. While the former are exhaustively enumerated, the latter constitute a residual (and the largest) category.[57] The Commission does not make mandatory for non-high-risk AI systems to comply with requirements imposed to high-risk AI systems. Developers and users of non-high-risk AI systems are however encouraged to voluntarily endorse these requirements through codes of conduct (art. 69). Such mechanism is reminiscent of the Draft Ethics Guidelines, which initially aimed to be voluntary endorsed by stakeholders.[58] However, this solution was deeply criticised in the feedback received during the open consultation, and therefore abandoned in the final report.[59]

4. Discussion: The Humpty Dumpty Fallacy

The particularity of risk regulation is to propose *ex ante* solutions. It is a truism to say that the purpose of risk regulations is to prevent risk by reducing at the lowest possible level the probability of its occurrence using statistical prediction tools while assessing calculable risks.[60] That said, it is difficult, if not impossible, to measure the results of the adopted regulation, as the purpose of such approach is risk avoidance. Julia Black and Robert Baldwin astutely note that "if a risk does not crystallize, it can be

---

[55] Pauline Bégasse de Dhaem and Denis Philippe, "La digitalisation du secteur bancaire: analyse du projet de règlement européen en matière d'intelligence artificielle", in *Actualités en Droit Économique: L'entreprise Face au Numérique*, CUP Vol. 208, ed. Gabriela de Pierpont and Enguerrand Marique (Brussels: Anthemis, 2021): 237.

[56] Mika Westerlund, "The emergence of deepfake technology: A review", *Technology Innovation Management Review* 9, no. 11 (2019): 40-53.

[57] Bégasse de Dhaem and Philippe, "La digitalisation du secteur bancaire", 234.

[58] HLEG, *Draft Ethics Guidelines*, 2.

[59] HLEG, *Ethics Guidelines*.

[60] David Wright and John Copas, "Prediction scores for risk assessment", in *Law and Uncertainty: Risks and Legal Processes*, ed. Robert Baldwin (London: Kluwer International Law, 1997): 21-38.

difficult, if not impossible, to show that was the result of the regulator's actions".[61] This drawback is, however, more procedural than substantive.

Despite the statistical nature of risk regulation, rationality and scientific evidence are not the only drivers of the level of risk acceptability. Cultural and psychological dimensions also play a role.[62] This explains why smoking or alcoholic drinking "tends to be less heavily regulated than vehicle emissions although it is normally assumed to be a much bigger killer".[63] Similarly, no American has ever been killed by a commercial nuclear power plant accident in the United States despite the events of Three Mile Island. Yet, as American historian Melvin Kranzberg noted, "although antinuclear protestors picket nuclear power plants under construction, we never see any demonstrators bearing signs saying 'Ban the Buick!'" despite the high number of car fatalities.[64] The same goes for AI. Lawmakers should take into account cultural and psychological dimensions. The Frankenstein complex, *i.e.*, the fear that the creature (AI or robots) will one day outcompete and destroy its creator (humanity),[65] is strongly rooted in Western culture.[66] In EU countries, AI systems follow a "plug and pray" model, rather than the Asian "plug and play".[67]

The combination of scientific and non-scientific factors – statistical studies and general public risk appetite – leads to an "archipelago of risk domains isolated from one another, with different policy stances across

---

[61] Julia Black and Robert Baldwin, "Really responsive risk-based regulation", *Law & Policy* 32, no. 2 (2010): 200 ("Was the lack of an outbreak of salmonella in the last year, for example, due to the local authority's excellent monitoring, or to improvements in food processing demanded by retailers, or to food producers' own efforts independently of the supply chain, or simply to luck?").

[62] Lukasz Gruszczynski, *Regulating Health and Environmental Risks under WTO Law: A Critical Analysis of the SPS Agreement* (Oxford: Oxford University Press, 2010): 20.

[63] Christopher Hood, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford: Oxford University Press, 2001): 8; Boy Heyman, "Values and health risks" in *Risk, Safety and Clinical Practice: Health Care Through the Lens of Risk*, ed. Bob Heyman *et al.* (Oxford: Oxford University Press, 2008).

[64] Melvin Kranzberg, "Technology and history: 'Kranzberg's laws'", *Technology and Culture* 27, no. 3 (1986): 552.

[65] Sam N. Lehman-Wilzig, "Frankenstein unbound: Towards a legal definition of artificial intelligence", *Futures* 13, no. 6 (1981): 442-457. Gorman Beauchamp, "The Frankenstein complex and Asimov's robots", *Mosaic* 13, no. 3-4 (1980): 85.

[66] Giovanni Sartor, "Human rights in the information society: Utopias, dystopias and human values", in *Philosophical Dimensions of Human Rights*, ed. Claudio Corradetti (London: Springer 2012): 297.

[67] Mireille Buydens, "L'intelligence artificielle et le droit: vertiges en terre inconnue", *Revue Internationale des Services Financiers*, no. 3-4 (2019): 49.

the various domains",[68] resulting in a more than vast range of regulatory responses.[69] This explains why tailoring the regulatory response to the type of risk at stake is crucial.[70] Risk regulators analyse the "total surplus of benefits over costs and thereby rank the available options".[71] When this cost-benefit analysis leads to unsustainable risks, precaution must prevail,[72] as "even a risk with a very low probability becomes unacceptable when it affects all of us".[73] With a risk-based approach, the regulatory response will therefore depend on the frequency and gravity of the risk.[74] Such a tailored or sectorial approach fits technology.[75] As a scientific discipline, AI encompasses so many techniques and applications[76] that a one-size-fits-all solution is obviously not a viable option.[77] Unsustainable risk should be prohibited, severe risk should be handled through *ex ante* transparency and human oversights requirements, medium risk through a weaker version of these safety requirements, and low risk could be mitigated *ex post*.[78] This brings us to the key issue of the Proposal. By merely distinguishing high-risk and non-high-risk AI systems, the European Commission does not cover the full spectrum of AI risks. It only focuses on the two extremes,

---

[68] Hood, Rothstein and Baldwin, *The Government of Risk*, 7.

[69] Jan Bohanes, "Risk regulation in WTO Law: A procedure-based approach to the precautionary principle", *Columbia Journal of Transnational Law* 40 (2002): 338-339.

[70] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008): 118.

[71] Martin Peterson, *The Ethics of Technology: A Geometric Analysis of Five Moral Principles* (Oxford: Oxford University Press 2017): 88.

[72] Laurence Boisson de Chazournes, "New technologies, the precautionary principle, and public participation", in *New Technologies and Human Rights*, ed. Thérèse Murphy (Oxford: Oxford University Press, 2009): 162.

[73] Joseph Norman *et al.*, "Climate models and precautionary measures", *Issues in Science and Technology* 31, no. 4 (2015): 15-16. Mike Feintuck, "Precautionary maybe, but what's the principle? The precautionary principle, the regulation of risk and the public domain", *Journal of Law and Society* 32, no. 3 (2005): 371.

[74] Datenethickommission, *Opinion of the Data Ethics Commission*, December 2019 https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/datenethikkommission-abschlussgutachten-lang.pdf?__blob=publicationFile&v=4.

[75] Aaron Wildavsky, *Searching for Safety: Social Theory and Social Policy.*

[76] Stuart Russel and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Upper Saddle River: Pearson, 2010). Keith Frankish and William M. Ramsey eds., *The Cambridge Handbook of Artificial Intelligence* (Cambridge: Cambridge University Press, 2014).

[77] Gregory N. Mandell, "Regulating emerging technologies", *Law Innovation and Technology* 1, no. 1 (2009): 75-92.

[78] Nicolas Petit and Jerome De Cooman, "Models of law and regulation for AI", in *The Routledge Social Science Handbook of AI*, ed. Anthony Elliott (Abingdon: Routledge, 2021): 199-221.

i.e., unacceptable or high risks on the one hand, non-high-risks on the other. True, transparency obligation pertaining to certain AI systems temper this pitfall. But this only constitutes a specific response to some specific risks that does not address potential risks raised by alleged non-high-risk AI systems.

Concerning non-high-risk AI systems, the voluntary endorsement mechanism raises our scepticism. On the one hand, the shift of the burden of protection from regulation to codes of conduct might allow organisations to portray themselves in a more autonomy-friendly light than what is factually justified.[79] This phenomenon is known as the *bluewashing* strategy, as it is similar to environmental greenwashing.[80] On the other hand, it is uncertain whether developers will truly adhere to such frameworks.[81] It has been shown – albeit regarding ethical statements – that they have little or no impact on developers' daily practices.[82] This pitfall fuels the need for regulation devised at a superior level, as "AI cannot and will not serve the public good without strong rules in place".[83] Policymakers should "do

[79] For a similar argument, although on privacy by design, see Niels van Dijk *et al.*, "Right engineering? The redesign of privacy and personal data protection", *International Review of Law, Computers & Technology* 32, no. 2-3 (2018): 251. Ira S. Rubinstein and Nathaniel Good, "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents", *Berkeley Technology Law Journal* 28, no. 2 (2011): 1409.

[80] Ben Wagner, "Ethics as an escape from Regulation: From ethics-washing to ethics shopping?", in *Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen*, ed. Emre Bayamlioglu *et al.* (Amsterdam: Amsterdam University Press, 2018). Luciano Floridi, "Translating principles into practices of digital ethics: Five risks of being unethical", *Philosophy & Technology* 32, no. 2 (2019): 185-193. Nathalie A. Smuha, "The EU approach to ethics guidelines for trustworthy Artificial Intelligence", *Computer Law Review International* 4 (2019): 97-106, De Cooman, "Éthique et intelligence artificielle", 79-121. Petit and De Cooman, "Models of law and regulation for AI", 199-221.

[81] Awanthika Senerath, Marthie Grobler and Nalin Asanka Gamagedara Archchilage, "Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies", *ACM Transactions on Privacy and Security* 22, no. 4 (2019): 1-30. Bill C. Hardgrave, Fred D. Davis and Cynthia K. Riemenschneider, "Investigating determinants of software developers' intention to follow methodologies", *Journal of Management Information Systems* 20, no. 1 (2003): 123-151.

[82] Andrew McNamara, Justin Smith and Emerson Murphy-Hill, "Does ACM's code of ethics change ethical decision making in software development?", *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (2018): 729-733. Brent Mittelstadt, "Principles alone cannot guarantee ethical AI", *Nature Machine Intelligence* 1 (2019): 504. Thilo Hagendorff, "The ethics of AI ethics – An evaluation of guidelines", *arXiv*, February 28, 2019, https://arxiv.org/abs/1903.03425.

[83] Paul Nemitz, "Constitutional democracy and technology in the age of artificial intelligence", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 7.

more than merely recommend the adoption and implementation" of some requirements to achieve the Holy Grail of a trustworthy AI system.[84] In its current form, the Proposal is unfit for dealing with alleged non-high-risk AI systems.

This is where the nineteenth century English author Lewis Carroll enters the game. In his book *Through the Looking Glass*, one of his characters – Humpty Dumpty – has a delightful exchange on semantics.[85]

> *"When I use a word," Humpty Dumpty said in rather a scornful tone, "it means just what I choose it to mean – neither more nor less".*
>
> *"The question is," said Alice, "whether you can make words mean so many different things".*
>
> *"The question is," said Humpty Dumpty, "which is to be master – that's all".*

The dichotomy between high-risk and non-high-risk AI systems "means just what [the Commission] choose[s] it to mean – neither more nor less". Although the Proposal and its underlying risk-based approach are praiseworthy, a mere analysis of its scope *ratione materiae* shows its inherent deficiencies. Just because the Proposal argues some AI systems are non-high-risk does not mean the risk is actually low. This is the essence of what this article humorously labels as the Humpty Dumpty fallacy.

Far from trivial, it is highly impacted by the fact that, as previously hinted, rationality is not the only driver to risk regulation. Sometimes, general public risk appetite and popular outcry force policymakers to adopt knee-jerk regulation in a misleading application of the precautionary principle. This consists in adopting inefficient over-regulation in response to risks, incidents and accidents.[86] The Fukushima nuclear disaster gives us the perfect example.[87] Its response combines the radioactivity risk, the (rare, although disastrous) event itself and the public opinion.[88] Rather than blaming Japanese seismic activity, some have blamed nuclear

---

[84] Rubinstein and Good, "Privacy by design", 1408 (although discussing privacy by design).

[85] Carroll, *Through the Looking-Glass*, 124.

[86] David Haven, "Ocean pollution", *Marine Technology Society Journal* 34, no. 2 (2000): 59-61. Elisabeth Staksrud, "Online grooming legislation: Knee-jerk regulation?", *European Journal of Communication* 28, no. 2 (2013): 152-167.

[87] Petit and De Cooman, "Models of law and regulation for AI", 199-221.

[88] Emily Hammond, "Nuclear power, risk, and retroactivity", *Vanderbilt Journal of Transnational Law* 48 (2015): 1059-1082.

technology.[89] Upshot? Countries geographically less exposed to earthquakes have introduced nuclear exit policies in favour of fossil fuel energies.

AI constitutes a fertile breeding ground for the seed of knee-jerk or over-regulation. For instance, there is evidence that human air pilots are more open to mistake than their AI counterparts.[90] Behavioural economy broadens the argument to all decision-making disciplines.[91] Psychologist and economist Daniel Kahneman summarises that "whenever we can replace human judgement by a formula, we should at least consider it".[92]

Notwithstanding human error is the greatest and "ever-present source of uncertainty,"[93] a knee-jerk regulation will lead to a ban of AI-assisted planes rather than increasing human-machine synergies, assuming that "society displays a lower tolerance threshold for accidents caused by machines".[94]

Overregulation sometimes leads to underregulation. The overregulation of situations that present many casualties (*e.g.*, nuclear safety) could induce forgetfulness of those, which cumulatively have an impact at least as severe as the first ones (*e.g.*, traffic deaths).[95] One could argue that this is because the former is socially intolerable, while the latter is more acceptable.[96] This phenomenon is reinforced when "low probability risk receives media coverage".[97] This could lead to a *selection bias*. In the Commission's own words, "AI is a highly dynamic and rapidly evolving industry so that not a lot of currently valid evidence is available".[98] The Commission later recog-

---

[89] William J. Kinsella, "Being "post-Fukushima": Divergent understandings of sociotechnical risk", *Fukushima Global Communication Programme Working Paper Series*, 2015, https://i.unu.edu/media/ias.unu.edu-en/news/12850/FGC-WP-18-FINAL.pdf.

[90] David A. Mindell, *Our Robots, Ourselves: Robotics and the Myths of Autonomy* (New York: Viking Adult, 2015).

[91] Daniel Kahneman, Olivier Sibony and Cass R. Sunstein, *Noise: A Flaw in Human Judgement* (New York: Little, Brown and Company, 2021).

[92] Daniel Kahneman, *Thinking Fast and Slow* (New York: Farrar, Straus and Giroux, 2011): 226.

[93] Tony Muschara, *Risk-Based Thinking: Managing the Uncertainty of Human Error in Operations* (Abingdon: Routledge, 2018): 22.

[94] Petit and De Cooman, "Models of law and regulation for AI", 199-221.

[95] Black and Baldwin, "Really responsive risk-based regulation", 209.

[96] Henry Rothstein *et al.*, "The risks of risk-based regulation: Insights from the environmental policy domain", *Environmental International* 32 (2006): 1062.

[97] Bohanes, "Risk regulation in WTO law", 359.

[98] European Commission, *Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence: Inception Impact Assessment, ARES(2020)3896535*, July 23, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal-requirements_en.

nised that "although evidence for individual legal challenges and breaches of fundamental rights is growing, robust and representative evidence for harms inflicted by the use of AI is scarce due to the lack of data and mechanisms to monitor AI as a set of emerging technology".[99]

Even with available valid evidence, the idiosyncratic definition of what is high-risk leads the AI Act to exclude some AI systems that are nevertheless usually identified as harmful, as if the most-discussed algorithmic harm examples had blinded the Commission. The two next sections highlight the most striking illustrations of the Humpty Dumpty fallacy, *i.e.*, recommender systems for consumers (a) and competition law enforcement authorities (b).

a. Recommender Systems for Consumers

The Commission emphasises in the Proposal that consumers' "exploitative profiling and micro-targeting" are "considered as potential candidates for prohibition".[100] In the end, however, they were discarded, not because they were considered harmless, but as "these problems [were] specifically examined and targeted by the recent proposal for the Digital Service Act" (hereafter, "DSA").[101]

A recommender system is defined as "a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed" (art. 2(O) DSA). They are a form of *hypernudge*, a digital architecture that alters individuals' behaviour "by configuring and thereby personalising the user's informational choice context, typically through algorithmic analysis of data streams from multiple sources claiming to offer predictive insights concerning the habits, preferences and interests of targeted individuals".[102] It is therefore all the more surprising to exclude recommender systems from the Proposal. It has been shown that some recommendations induce visceral reactions that

---

[99] EC, *SWD accompanying the AI Act*, part 1/2.

[100] EC, *SWD accompanying the AI Act*, Part 2/2, 47.

[101] *Ibidem*. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) amending Directive 2000/31/EC, 15.12.2020, COM(2020) 825 final*, December 15, 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN.

[102] Karen Yeung, "'Hypernudge': Big Data as a mode of regulation by design", *Information, Communication & Society* 20, no. 1 (2017): 119.

purely inhibit the mere possibility of not following the suggestion.[103] This is, in a way, quite close to the subliminal manipulation prohibited by the Proposal.

The DSA explains recommender systems "can have a significant impact on the ability of recipients to retrieve and interact with information online" and "play an important role in the amplification of certain messages, the viral dissemination of information and the stimulation of online behaviour" (Recital 62 DSA). As such, the DSA requires very large platforms to "set out in their terms and conditions, in a clear, accessible and easily comprehensible manner, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main parameters" (art. 29 DSA).

This raises two observations. First, the transparency requirement mitigates the eventual adverse effects of hypernudge, which "typically works better in the dark".[104] The intention of the DSA is laudable. The effectiveness of merely requiring understandable terms and conditions is, however, questionable, since it has long been proved that users neither read, nor understand such disclosures.[105]

Second, this requirement only applies to "very large online platforms," *i.e.*, those that provide their services to at least 45 million average monthly active users in the EU (art. 25 DSA). It goes beyond the scope of this article to discuss the relevance of this criterion regarding the DSA objective of proportionate compliance costs. Yet, it would probably have been better to follow a neutral approach *à la* GDPR. Under that regulation, data subjects' rights do not depend on the size of the data controller or processor.[106]

Perhaps the weakness of this requirement is precisely that the DSA is only intended to ensure a "responsible and diligent behaviour by providers of

---

[103] Robert Baldwin, "From regulation to behaviour change: Giving nudge the third degree", *The Modern Law Review* 77, no. 6 (2014): 831-857.

[104] Luc Bovens, "The ethics of nudge", in Till-Grüne-Yanoff and Sven Ove Hansson (eds), *Preference Change: Approaches from Philosophy, Economics and Psychology* (Springer 2009): 210.

[105] Aleecia M. McDonald and Lorrie Faith Cranor, "The cost of reading privacy policies", *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (2008): 543-568. Helen Nissenbaum, "A contextual approach to privacy online", *Daedalus* 140, no. 4 (2011): 32-48. Daniel J. Solove, "Introduction: Privacy self-management and the consent dilemma", *Harvard Law Review* 126, no. 7 (2013): 1880-1903. Solon Barocas and Helen Nissenbaum, "Big Data's end run around anonymity and consent", in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, ed. Julia Lane *et al.* (Cambridge: Cambridge University Press 2014): 44-75.

[106] Even if the GDPR emphasised several times that "the specific needs of micro, small and medium-sized enterprises" should be taken into account.

intermediary services (which) is essential for safe, predictable and online environment".[107] It would have been up to the Proposal to regulate this kind of system, as the distinction between digital nudging and AI-powered recommender systems is blurred.[108] Indeed, the inferential capacity of machine-learning systems allows the development of astonishing recommender systems able to "unearth patterns".[109] Challenges they raise will be more and more acute with the development of descriptive models based on unsupervised learning. This technique is indeed quite useful for customers' clustering and segmentation, which in turn allows for the establishment of a correlation between type of customer and products bought – customers who purchase this product could purchase this other product as well.[110]

The conspicuous absence of requirements for recommender systems in the AI Act illustrates the Humpty Dumpty fallacy well. The fact that the Commission exhaustively enumerates high-risk AI systems does not mean others are non-high-risk. Excluding recommender systems from the Proposal because they are targeted in the DSA if used by very large online platforms only induces a gap that will have to be filled.

b. The AI Act (In)Applicability to EU Competition Law

i. The Problem with (Algorithmic) Cartel Screening

In the AI White Paper, the European Commission announced that it will assess how to equip "law enforcement authorities with appropriate tools", *i.e.*, AI systems.[111] In her mission letter, Commission President Ursula von der Leyen asked Margrethe Vestager to strengthen "competition enforcement in all sectors".[112] This ambition does not come out of the blue. First, it is argued that the probability of cartel detection is around 15 percent in both the EU and the United States.[113] Second, the vast majority of cartel

[107] EC, *Digital Services Act*, Recital 3.

[108] Mathias Jesse and Dietmar Jannack, "Digital nudging with recommender systems: Survey and future directions", *Computers in Human Behavior Report* 3 (2021): 1-14.

[109] John Zerilli and Adrian Weller, "The technology", in *The Law of Artificial Intelligence*, ed. Matt Hervey *et al.* (London: Sweet & Maxwell, 2021): 12.

[110] Ronald Ashri, *The AI-Powered Workplace: How Artificial Intelligence, Data, and Messaging Platforms Are Defining the Future of Work* (New York: Apress, 2020): 52.

[111] EC, *White Paper*, 2.

[112] Ursula von der Leyen, *Mission letter to Margrethe Vestager, Executive Vice-President for a Europe fit for the Digital Age*, December 1, 2019, https://ec.europa.eu/commission/commissioners/sites/default/files/commissioner_mission_letters/mission-letter-margrethe-vestager_2019_en.pdf.

[113] Emmanuel Combe, *Economie et Politique de la Concurrence*, 2nd ed. (Paris: Dalloz, 2020): 181.

detections come from an application for leniency.[114] Leniency programmes are, however, not a panacea.[115] The amnesty is the carrot for whistleblowing undertakings. The stick is the Commission's proactive detection of anticompetitive behaviours. Few cartelists apply for leniency when the probability of such Sword of Damocles is low.[116] Structural and behavioural screens have therefore been developed to solve this issue.[117] Cartel screening raises empirical red flags and identifies markets and undertakings worthy of further investigations.[118]

It is argued that AI systems have a role to play in EU competition law proceedings.[119] Screening is a data- and resource-intensive activity.[120] AI systems can identify market deficiencies sooner and help the Commission open the "right" investigation by processing extensive data sets quicker and more efficiently.[121]

These tools are however no panacea either.[122] Excessive or undue reliance upon such tools as the basis to pursue investigation or conversely discard the case would probably infringe Article 41 of the EU Charter, which clearly states that "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". It has been suggested that an excessive automation

---

[114] Nicolas Petit, *Droit Européen de la Concurrence* (Paris: Domat, 2013): 529.

[115] Massimo Motta and Michele Polo, "Leniency programs and cartel prosecution", *International Journal of Industrial Organization* 21, no. 3 (2003): 347-379.

[116] Joseph E. Harrington, Jr. and Myong-Hun Chang, "When can we expect a corporate leniency program to result in fewer cartels?", *The Journal of Law & Economics* 58, no. 2 (2015): 417-449.

[117] Paul A. Groutt and Silvia Sonderegger, "Structural approaches to cartel detection", in *European Competition Law Annual 2006: Enforcement of Prohibition of Cartels*, ed. Claus-Dieter Ehlermann and Isabela Atanasiu (Oxford: Hart Publishing, 2007): 83-103. Joseph E. Harrington, Jr, "How do cartels operate?", *Foundation and Trends in Microeconomics* 2, no. 1 (2006): 1-105.

[118] Rosa M. Abrantes-Metz, "Recent successes of screens for conspiracies and manipulations: Why are there still sceptics?", *Antitrust Chronicle* 10, no. 2 (2014): 1-17.

[119] Thibault Schrepel, "Computational antitrust: An introduction and research agenda", *Stanford Computational Antitrust* 1 (2021): 1-15.

[120] Directorate for financial and enterprise affairs – Competition committee, "Ex Officio cartel investigations and the use of screens to detect cartels", *OECD Competition Law & Policy Roundtables*, DAF/COMP(2013)27, 7 July 2014, https://www.fne.gob.cl/wp-content/uploads/2014/07/2013-Ex-officio-cartels-investigation-3569-KB1.pdf.

[121] Andreas von Bonin and Sharon Malhi, "The use of Artificial Intelligence in the future of competition law enforcement", *Journal of European Competition Law & Practice* 11, no. 8 (2020): 468-471.

[122] Albert Sanchez-Graells, "'Screening for cartels' in public procurement: Cheating at solitaire to sell fool's gold?", *Journal of European Competition Law & Practice* 10, no. 4 (2019): 199-211.

could lead to complacency on the part of officials.[123] This is partly due to the automation bias, *i.e.*, the irrational tendency to rely on automated decision even when the operator suspects malfunction.[124] This is the digital update of search-satisfying, anchoring, and confirmation biases. *Search satisfaction* induces the idea to stop searching once a first plausible explanation is found. *Anchoring* means a premature decision-making based on limited information initially available. The anchor effect suggests the officials will fail to adjust their decision when new information becomes available.[125] The anchoring bias is strengthened by the *confirmation bias*, *i.e.*, the tendency to interpret information to fit their preconceived opinion. The anchoring bias is reinforced by the diagnostic momentum or hindsight bias, *i.e.*, the continuing of an action previously instigated by someone else without considering any new information and changing plan accordingly, particularly if the plan was commenced by a senior expert or hierarchical supervisor.[126] Using algorithmic recommendations based on market screening might strengthen these biases. The recommendation constitutes the first plausible explanation (search satisfaction) coming from an alleged superior authority (hindsight bias). After all, when it comes to persuasion, "computers also benefit from their traditional reputation of being intelligent and fair, making them seem credible sources of information and advice".[127] The officials will therefore be tempted to cease the scrutiny. 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 (anchoring and confirmation).

Another potential infringement of Article 41 of the EU Charter is to be found regarding the Commission's duty to state reasons for administrative decisions. It should be borne in mind that going against the recommendation would require a well-written reasoned decision rendering "the

[123] Christopher. D. Wickens *et al.*, "Complacency and automation bias in the use of imperfect automation", *Human Factors and Ergonomics Society* 57, no. 5 (2015): 728-739.

[124] Kate Goddard, Abdul Roudsari and Jeremy C. Wyatt, "Automation bias: A systemic review of frequency, effect mediators, and mitigators", *Journal of the American Medical Informatics Association: JAMIA* 19, no. 1 (2012): 121-127.

[125] Amos Tversky and Daniel Kahneman, "Judgement under uncertainty: Heuristics and biases", *Science* 185, no. 4157 (1974): 1124-1131.

[126] Ian S. Forrester, "From Regulation 17/62 to Article 52 of the Charter of Fundamental Rights", in *General Principles of EU Law and European Private Law*, ed. Ulf Bernitz, Xavier Groussot and Felix Schulyok (Alphen aan den Rijn: Kluwer Law International, 2013): 343-371.

[127] Brian J. Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (San Francisco: Morgan Kaufmann Publishers, 2003): 215.

exercise of discretion costlier".[128] This is because the Commission officials should not only explain why they took a particular decision, but also why they did not follow the recommendation. On the contrary, following that recommendation will facilitate the duty to state the ground of the decision, as public servants will dispose the conclusions of the algorithm. The officials' fear to make a mistake – the AI system being statistically more often right than wrong – and the illusion that computers are error-proof both increase "the likelihood of inaccurate outcomes".[129]

This bias is all the more dangerous as recommender systems are prone to type I and type II errors. Type I errors, or false positives, correspond to mistakenly identifying a cartel where there is none, namely a false alarm. This raises important issues, since overcompliance may lead the operators to search for a solution for a non-existent problem.[130] As the Commission has limited resources, this is the "worst kind of prediction error", as it triggers costly unjustified investigation.[131] Upon confirmation of absence of collusive behaviour, operators' loss of confidence in the system might lead them to disregard subsequent recommendations, even if they are actually positive (disregarded true positives).[132] Whilst these observations were first made about automated alarm systems, they have been generalised to decision-support systems.[133] As such, it is argued that using a structural approach to help competition authorities trigger investigations in then-qualified archetypal markets for collusion would probably result in a high-rate of type I errors. Many markets have indeed the structural characteristics of collusion without being subject to collusive practices.[134] It is of paramount importance to understand that "the *propensity* for collusion

---

[128] Nicolas Petit, "Artificial Intelligence and automated law enforcement: A review paper", *SSRN*, March 21, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3145133.

[129] Danielle Keats Citron, "Technological due process", *Washington University Law* 85, no. 6 (2008): 1254.

[130] Stephen R. Dixon and Christopher D. Wickens, "Automation reliability in unmanned aerial vehicle flight control: A reliance compliance model of automation dependence in high workload", *Human Factors* 48, no. 3 (2006): 474-486.

[131] Martin Huber and David Imhof, "Machine learning with screens for detecting bid-rigging cartels", *International Journal of Industrial Organization* 65 (2019): 278.

[132] Stephen R. Dixon, Christopher D. Wickens and Jason S. McCarley, "On the independence of compliance and reliance: Are automation false alarms worse than misses?", *Human Factors* 49, no. 4 (2007): 564-572.

[133] Raja Parasuraman and Dietrich Manzey, "Complacency and bias in human use of automation: An attentional integration", *Human Factors* 52, no. 3 (2010): 381-410.

[134] Combe, *Economie et Politique de la Concurrence*, 182-183.

is not an indication that an anti-competitive behaviour has *actually* taken place".[135] It has been hypothesised – albeit solely based on discovered cartels – that very low fractions of such ideal market for cartels are actually cartelised. Bayesian statistical inference helps understand why "the likelihood of *false positives* with a structural approach is quite high".[136] Given a low prior probability of collusion, the posterior probability is still supposed to be quite low.

Type II errors, or false negatives, involve the non-detection of a cartel despite its existence. The absence of evidence is not the evidence of absence. This error usually comes from data availability.[137] Machine-learning systems are not preprogramed to respond in a certain way whenever they face certain conditions. They "learn" the appropriate response (hence their name).[138] Learning requires examples.[139] Data used by AI recommender systems "originates from antitrust cases, and may therefore be subject to *selection bias*".[140] The case studies on which scholarship draws collusive markers are indeed exclusively composed of *discovered and successfully prosecuted* cartels.[141] This sample might not be representative of the population of cartels.

In addition, recommender systems present a perverse effect of self-fulfilling prophecies. The recommendations followed at time *t* become data on which the AI system bases its recommendations at time *t+1*. This reinforcement of the feedback loop can lead to dramatic consequences.[142] When suggesting where to allocate the scarce resources of competition

---

[135] Directorate for Financial and Enterprise Affairs – Competition Committee, "Ex Officio cartel investigations and the use of screens to detect cartels", 39 (we do not emphasise).

[136] Joseph E. Harrington, Jr, "Detecting cartels", in *Handbook of Antitrust Economics*, ed. Paolo Buccirossi (Cambridge: The MIT Press, 2008): 214.

[137] Matthias Leese, "The new profiling: Algorithms, black boxes, and the failure of antidiscriminatory safeguards in the European Union", *Security Dialogue* 45, no. 5 (2014): 494-511. Brent Mittelstadt *et al.*, "The ethics of algorithms: Mapping the debate", *Big Data & Society* 3, no. 2 (2016): 1-21.

[138] John Zerilli and Adrian Weller, "The technology", in *The Law of Artificial Intelligence*, ed. Matt Hervey and Matthew Lavy (London: Sweet & Maxwell, 2021): 9.

[139] Ira S. Rubinstein, "Big Data: The end of privacy or a new beginning?" *International Data Privacy Law* 3, no. 2 (2013): 74-87.

[140] Georges Symeonidis, "In which industries is collusion more likely? Evidence from the UK", *The Journal of Industrial Economics* 51, no. 1 (2003): 45.

[141] Paul A. Groutt and Silvia Sonderegger, "Structural approaches to cartel detection", 83-103.

[142] Marjolein Lanzing, "'Strongly recommended' revisiting decisional privacy to judge hypernudging in self-tracking technologies", *Philosophy & Technology* 32, no. 3 (2019): 562. Leese, "The new profiling: Algorithms, black boxes, and the failure of antidiscriminatory safeguards in the European Union". Brent Mittelstadt *et al.*, "The ethics of algorithms: Mapping the debate".

authorities, officials are already required to evaluate the "profile" of the case to retain only those of high importance. While such considerations are justified by the scarcity of public resources, they may however lead to self-fulfilling prophecies if AI systems conclude the aforementioned evaluation is synonymous of systematic exclusion of some cases. This would create a free-competition zone where some cartels would remain undisclosed because they were initially excluded from investigation by the AI system, notwithstanding a potential "significant impact on the functioning of competition in the internal market and risk of consumer harm".[143]

ii. A Proposed Solution

The HLEG's Ethics Guidelines define the principle of respect for human autonomy as the capacity "to keep full and effective self-determination" and "leave meaningful opportunity for human choice".[144] This principle leads to two requirements.

The first is human oversight. It follows a threefold scenario whereby strengthening human autonomy should be guaranteed as soon as a human being intervenes in the process (human-in-the-loop), supervises the process (human-on-the-loop) or stays in command (human-in-command).[145] This means AI systems should not "become the primary decision makers" that "take human decision making out of the process".[146] Father of jurimetrics Lee Loevinger explains that "it is not the invention of tools, however subtle, complex, or powerful, that constitutes man's greatest achievement, but the skill in using the tools that man has developed in himself".[147]

The second requirement is human agency, *i.e.*, the capacity for operators to make informed autonomous decisions. This implies they should be given "the knowledge and tools to comprehend and interact with AI

---

[143] European Commission, *Commission notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU*, OJ C 308, 20 October 2011, 6-31, paragraph 13.

[144] HLEG, "Ethics guidelines for trustworthy AI", 12.

[145] *Ibidem*, 18. European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, March 2018, https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1/language-en/format-PDF/source-78120382.

[146] Danielle Keats Citron, "Technological due process", 1252.

[147] Jurimetrics is the discipline that uses probability and statistics to answer legal questions. Lee Loevinger, "Jurimetrics: Science and prediction in the field of law", *Minnesota Law Review* 46, no. 1 (1961): 275.

systems to a satisfactory degree and, where possible, be enabled to reasonably self-assess or challenge the system".[148]

Good news is that requirements for human agency and oversight are crystallised in the Proposal. The document, however, preliminary notes that it is "without prejudice to the application of Union competition law".[149] It seems AI recommender systems used in the context of competition law proceedings are beyond the Proposal's scope of application. The use of AI systems by public authorities is forbidden when oriented towards the evaluation and classification of the "trustworthiness of *natural persons* (…) based on their social behaviour or known or predicted personal or personality characteristics" (art. 5(1)(a)). Such description difficultly copes with the yet broad definition of undertakings under EU competition law.

A similar conclusion goes for law enforcement activities listed in Annex III – and therefore considered as high-risk – that focus on *criminal offences* of natural persons. True, there is currently a criminalisation of EU competition law enforcement.[150] But, as Advocate General Kokott highlighted, "competition is similar to criminal law, but is no part of [its] core area".[151] Commission Staff Working Document accompanying the Proposal makes it crystal clear that one of the elements that triggered the qualification of AI systems used by law enforcement authorities as high risk was *Loomis v. Wisconsin*.[152] This US criminal law case discussed the use of algorithmic risk assessment in sentencing.[153] This seems to indicate that what the Proposal targets is the "hard core" criminal law.

The application of the Proposal to competition law enforcement, *quod non*, would have solved the principal pitfalls enumerated above. AI recommender systems 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(1)). This could be operationalised by sending operators "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)).

---

[148] HLEG, "Ethics guidelines for trustworthy AI", 16.

[149] EC, *Proposal*, 4.

[150] Peter Whelan, *The Criminalization of European Cartel Enforcement: Theoretical, Legal, and Practical Challenges* (Oxford: Oxford University Press, 2014).

[151] Opinion of Advocate General Kokott of 18 April 2013, *Schindler Holding Ltd and Others v. European Commission and Others*, C-501/11P, EU:C:2013:248, paragraph 25.

[152] EC, *SWD accompanying the AI Act*, Part 2/2, 46.

[153] *Loomis v. Wisconsin*, 881 N.W.2d 749 (Wis 2016).

This transparency requirement is quite close to the HLEG's human agency. Regarding human oversight, AI systems should, by design, "be effectively overseen by natural persons during the period in which the AI system is in use" (art. 14(1)). Upshot? Human operators have to "fully understand the capacities and limitations" of the AI systems (art. 14(4)(a)). One could draw a parallel between this situation and basic mathematical education at school. All students learn how to read a graph, "and graphs were the way that information was presented to us".[154] Albeit AI systems are much more complicated than graphs, the explicability intuition remains correct. What is critical here is not simply to explain how to read a recommendation, but, above all, to understand and be able to overcome it in the same way teachers "always taught students how to go behind what information a graph is trying to present".[155]

To mitigate the automation bias, recommender systems should reveal to operators the degree or probability of certainty.[156] Such solutions are already implemented by some algorithmic models whose objective is to reduce the risk of false positives (type I errors).[157] Beyond such technological solution, the Proposal requires that users of recommender systems "remain aware of the possible tendency of automatically relying or over-relying on the output produced" by an AI system, in particular those "used to provide information or recommendations for decisions to be taken by natural persons" (art. 14(4)(b)). This is an avowed reference to the automation bias. Human operators should similarly be able to correctly interpret the AI system's output and to decide when it should not be used, or when the output should be disregarded, overridden or reversed (arts. 14(4)(c) and (d)). This last requirement brings a solution for type I and type II errors. Finally, the risk of self-fulfilling prophecies is mitigated through the accuracy and resilience of AI systems that continue to learn after being put into service, which should be designed "in such a way to ensure that possibly biased outputs due to outputs used as an input for future operations

---

[154] Lyria Bennett Moses, "Edspresso episode 3: The ethical implications of AI decision-making, with Lyria Bennett Moses", *NSW Department of Education*, 4 February 2021, https://education.nsw.gov.au/teaching-and-learning/education-for-a-changing-world/resource-library/lyria-bennett-moses.

[155] *Ibidem*.

[156] Christopher D. Wickens *et al.*, "Complacency and automation bias in the use of imperfect automation".

[157] Martin Huber and David Imhof, "Machine learning with screens for detecting bid-rigging cartels".

('feedback loops') are duly addressed with appropriate mitigation measures" (art. 15(3)).

As a result, the Proposal is quite satisfactory. It solves major drawbacks raised by recommender systems. Yet, its limited scope of application reduces the effectiveness of these solutions. This is another consequence of the Humpty Dumpty fallacy. As statistician and essayist Nassim Taleb astutely notes, "learning to learn" is of paramount importance.[158] Policymakers place too much emphasis on specificities rather than on generalities in the decision-making process. The AI Act seems to be no exception. In this case, the specificity was *Loomis v. Wisconsin*; the generality, the risk raised by algorithmic recommendation outside the scope of hard-core criminal law.

Conclusion

This article has presented the background of the proposal for an EU Regulation laying down harmonised rules on AI, discussing the *ratione materiae* dimension of the Proposal, *i.e.*, the definition of so-called high-risk AI systems.

The Proposal is a risk regulation that is internal market oriented. Due to its inherent complexity, we foresee many practical problems at the time of its implementation, if accepted by the European Parliament and the Council. Despite a full spectrum of risk related to AI systems, the European Commission only focuses on the two extremes, *i.e.*, unacceptable and high risks on the one hand, and non-high risks on the other hand (with the limited exception of transparency for certain AI systems). In this regard, the Proposal is open to criticism. The idea of mere codes of conduct for non-high-risk AI systems is questionable. It has been demonstrated that they have little or no impact on developers' practices.

Notwithstanding its deficiencies, the Proposal constitutes another step on the way to trustworthy AI. It builds on two years of ethical efforts and takes into account many feedbacks received during numerous public consultations. The requirements of transparency, human agency and oversight are praiseworthy. Conversely, the underlying complexity of the Proposal's *ratione materiae* dimension – excluding, for instance, recommender systems for consumers and competition law enforcement authorities

[158] Nassim N. Taleb, *The Black Swan. The Impact of the Highly Improbable* (New York: Random House, 2007): xxi.

– constitutes an ill-starred decision. The Commission should avoid what this article humorously labels as the Humpty Dumpty fallacy. Just because the Proposal dichotomises high-risk and non-high-risk AI systems does not mean the latter are not worthy of discussion.

Bibliography

Abrantes-Metz, Rosa M. "Recent successes of screens for conspiracies and manipulations: Why are there still sceptics?". *Antitrust Chronicle* 10, no. 2 (2014): 1-17.

Ashri, Ronald. *The AI-Powered Workplace: How Artificial Intelligence, Data, and Messaging Platforms Are Defining the Future of Work*. New York: Apress, 2020.

Baldwin, Robert (ed.). *Law and Uncertainty: Risks and Legal Processes*. London: Kluwer Law International, 1997.

Barocas, Solon and Helen Nissenbaum. "Big Data's end run around anonymity and consent". In *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, edited by Julia Lane, Victoria Stodden, Stefan Bender and Helen Nissenbaum, 44-75. Cambridge: Cambridge University Press, 2014.

Beauchamp, Gorman. "The Frankenstein complex and Asimov's robots". *Mosaic* 13, no. 3-4 (1980): 83-94.

Beck, Ulrich. *Risk Society: Towards a New Modernity*. London: Sage, 1992.

Bégasse de Dhaem, Pauline and Denis Philippe. "La digitalisation du secteur bancaire: Analyse du projet de règlement européen en matière d'intelligence artificielle". In *Actualités en Droit Économique: L'entreprise Face au Numérique*, CUP Vol. 208, edited by Gabriela de Pierpont and Enguerrand Marique, 211-242. Brussels: Anthémis, 2021.

Bennett Moses, Lyria. "Edspresso episode 3: The ethical implications of AI decision-making, with Lyria Bennett Moses", *NSW Department of Education*, 4 February 2021, https://education.nsw.gov.au/teaching-and-learning/education-for-a-changing-world/resource-library/lyria-bennett-moses.

Black, Julia. "Managing regulatory risks and defining the parameters of blame: A focus on the Australian Prudential Regulation Authority". *Law & Policy* 28, no. 1 (2006): 1-30.

Black, Julia. "The role of risk in regulatory processes". In *The Oxford Handbook of Regulation*, edited by Robert Baldwin, Martin Cave, and Martin Lodge, 302-348. Oxford: Oxford University Press, 2010.

Black, Julia and Robert Baldwin. "Really responsive risk-based regulation". *Law & Policy* 32, no. 2 (2010): 181-213.

Bohanes, Jan. "Risk regulation in WTO Law: A procedure-based approach to the precautionary principle". *Columbia Journal of Transnational Law* 40 (2002): 323-390.

Boisson de Chazournes, Laurence. "New technologies, the precautionary principle, and public participation". In *New Technologies and Human Rights*, edited by Thérèse Murphy, 161-194. Oxford: Oxford University Press, 2009.

Brownsword, Roger. *Rights, Regulation, and the Technological Revolution*. Oxford: Oxford University Press, 2008.

Buydens, Mireille. "L'intelligence artificielle et le droit: Vertiges en terre inconnue". *Revue Internationale des Services Financiers* no. 3-4 (2019): 47-59.

Carroll, Lewis. *Through the Looking-Glass, and What Alice Found There*. London: Macmillan, 1871.

Citron, Danielle K. "Technological due process". *Washington University Law* 85, no. 6 (2008): 1249-1313.

Combe, Emmanuel. *Economie et Politique de la Concurrence*. 2nd ed. Paris: Dalloz, 2013.

Datenethikkommission, *Opinion of the Data Ethics Commission*, December 2019 https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/datenethik-kommission-abschlussgutachten-lang.pdf?__blob=publicationFile&v=4.

De Cooman, Jerome. "Éthique et intelligence artificielle: L'exemple européen". *Revue de la Faculté de Droit de l'Université de Liège* 1 (2020): 79-123.

Directorate for Financial and Enterprise Affairs – Competition Committee, "Ex Officio cartel investigations and the use of screens to detect cartels", *OECD Competition Law & Policy Roundtables*, DAF/COMP(2013)27, 7 July 2014, https://www.fne.gob.cl/wp-content/uploads/2014/07/2013-Ex-officio-cartels-investigation-3569-KB1.pdf.

Dixon, Stephen R. and Christopher D. Wickens. "Automation reliability in unmanned aerial vehicle flight control: A reliance compliance model of automation dependence in high workload". *Human Factors* 48, no. 3 (2006): 474-486.

Dixon, Stephen R., Christopher D. Wickens and Jason S. McCarley. "On the independence of compliance and reliance: Are automation false alarms worse than misses?". *Human Factors* 49, no. 4 (2007): 564-572.

EU Declaration on Cooperation on Artificial Intelligence, April 10, 2018, https://ec.europa.eu/jrc/communities/en/node/1286/document/eu-declaration-cooperation-artificial-intelligence.

European Commission, *Commission notice on best practices for the conduct of proceedings concerning Articles 101 and 102 TFEU*, OJ C 308, 20 October 2011, 6-31.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Digital Single Market Strategy for Europe, COM(2015) 192 final*, May 6, 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the*

Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All, COM(2017) 288 final, May 10, 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0228.

European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, COM(2018) 237 final*, April 25, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.

European Commission, *AI HLEG – steering group of the European AI Alliance*, https://ec.europa.eu/futurium/en/european-ai-alliance/ai-hleg-steering-group-european-ai-alliance.

European Commission, *Stakeholder Consultation on Guidelines' first draft*, February 19, 2019, https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/stakeholder-consultation-guidelines-first-draft.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building Trust in Human-Centric Artificial Intelligence, COM(2019)168 final*, April 8, 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019DC0168.

European Commission, *EU artificial intelligence ethics checklist ready for testing as new policy recommendations are published*, June 26, 2019, https://ec.europa.eu/digital-single-market/en/news/eu-artificial-intelligence-ethics-checklist-ready-testing-new-policy-recommendations-are.

European Commission, *White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final*, February 19, 2020, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

European Commission, *Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence: Inception Impact Assessment, ARES(2020)3896535*, July 23, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-and-legal -requirements_en.

European Commission, *Public consultation on the AI White Paper: Final Report*, November 2020, https://ec.europa.eu/digital-single-market/en/news/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence.

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) amending Directive 2000/31/EC, 15.12.2020, COM(2020) 825 final*, December 15, 2020, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN.

European Commission, *Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions – 2030 Digital Compass: the European way for the Digital Decade, COM(2021) 118 final*, March 9, 2021, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

European Commission, *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain Union legislative acts, COM(2021) 206 final*, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

European Commission, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Fostering a European approach to Artificial Intelligence, COM(2021) 205 Final*, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:205:FIN.

European Commission, *Annexes to the Proposal for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM2021) 206 final*, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2021:206:FIN.

European Commission, *Commission Staff Working Document Impact Assessment, Annexes Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, *SWD(2021) 84 Final*, Part 1/2.

European Commission, *Commission Staff Working Document Impact Assessment, Annexes Accompanying the Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, *SWD(2021) 84 Final*, Part 2/2.

European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, March 2018, https://op.europa.eu/en/publication-detail/-/publication/dfebe62e-4ce9-11e8-be1d-01aa75ed71a1/language-en/format-PDF/source-78120382.

European Parliament, *European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017IP0051.

European Parliament, *European Parliament resolution of 20 October 2020 on a framework of ethical aspects of artificial intelligence, robotics and related technologies, 2020/2012(INL)*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_EN.html.

European Parliament, *European Parliament resolution of 20 October 2020 on a civil liability regime for artificial intelligence, 2020/2014(INL)*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html.

European Parliament, *European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies, 2020/2015(INI)*, https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html.

European Parliament, *European Parliament Draft Report, Artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, 2020/2016(INI)*, https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_EN.pdf.

European Parliament, *European Parliament Draft Report, Artificial intelligence in education, culture and the audio-visual sector, 2020/2017(INI)*, https://www.europarl.europa.eu/doceo/document/A-9-2021-0127_EN.html.

Expert committee of China's Ministry of Science and Technology (MOST), *Governance Principles for a New Generation of Artificial Intelligence: Develop Responsible Artificial Intelligence*, June 17, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinese-expert-group-offers-governance-principles-responsible-ai/ (translation).

Feintuck, Mike. "Precautionary maybe, but what's the principle? The precautionary principle, the regulation of risk and the public domain". *Journal of Law and Society* 32, no. 3 (2005): 371-398.

Floridi, Luciano. "Establishing the rules for building trustworthy AI". *Nature Machine Intelligence* 1 (2019): 261-262.

Floridi, Luciano. "Translating principles into practices of digital ethics: Five risks of being unethical". *Philosophy & Technology* 32, no. 2 (2019): 185-193.

Fogg, Brian J. *Persuasive Technology: Using Computers to Change What We Think and Do*. San Francisco: Morgan Kaufmann Publishers, 2003.

Forrester, Ian S. "From Regulation 17/62 to Article 52 of the Charter of Fundamental Rights". In *General Principles of EU Law and European Private Law*, edited by Ulf Bernitz, Xavier Groussot and Felix Schulyok, 343-371. Alphen aan den Rijn: Kluwer Law International, 2013.

Frankish, Keith and William M. Ramsey (eds.). *The Cambridge Handbook of Artificial Intelligence*. Cambridge: Cambridge University Press, 2014.

Gautier, Axel, Ashwin Ittoo and Pieter Van Cleynenbreugel. "AI algorithms, price discrimination and collusion: A technological, economic and legal perspective". *European Journal of Law and Economics* 50, no. 3 (2020): 405-435.

General Secretariat of the Council, *European Council Meeting – Conclusions, EUCO 14/17*, October 19, 2017, http://data.consilium.europa.eu/doc/document/ST-14-2017-INIT/en/pdf.

Goddard, Kate, Abdul Roudsari and Jeremy C. Wyatt. "Automation bias: A systemic review of frequency, effect mediators, and mitigators". *Journal of the American Medical Informatics Association: JAMIA* 19, no. 1 (2012): 121-127.

Groutt, Paul A. and Silvia Sonderegger. "Structural approaches to cartel detection". In *European Competition Law Annual 2006: Enforcement of Prohibition of Cartels*, edited by Claus-Dieter Ehlermann and Isabela Atanasiu. 83-103. Oxford: Hart Publishing, 2007.

Gruszczynski, Lukasz. *Regulating Health and Environmental Risks under WTO Law: A Critical Analysis of the SPS Agreement*. Oxford: Oxford University Press, 2010.

Hagendorff, Thilo. "The ethics of AI ethics – An evaluation of guidelines". *arXiv*, February 28, 2019, https://arxiv.org/abs/1903.03425.

Hammond, Emily. "Nuclear power, risk, and retroactivity". *Vanderbilt Journal of Transnational Law* 48 (2015): 1059-1082.

Hardgrave, Bill C., Fred D. Davis and Cynthia K. Riemenschneider. "Investigating determinants of software developers' intention to follow methodologies". *Journal of Management Information Systems* 20, no. 1 (2003): 123-151.

Harrington, Joseph E. Jr. "Detecting cartels". In *Handbook of Antitrust Economics*, edited by Paolo Buccirossi, 213-258. Cambridge: The MIT Press, 2008.

Harrington, Joseph E. Jr. "How do cartels operate?". *Foundation and Trends in Microeconomics* 2, no. 1 (2006): 1-105.

Harrington, Joseph E. Jr. and Myong-Hun Chang. "When can we expect a corporate leniency program to result in fewer cartels?". *The Journal of Law & Economics* 58, no. 2 (2015): 417-449.

Haven, David. "Ocean pollution". *Marine Technology Society Journal* 34, no. 2 (2000): 59-61.

Heyman, Bob. "Values and health risks". In *Risk, Safety and Clinical Practice: Health Care Through the Lens of Risk*, edited by Bob Heyman, Monica Shaw, Andy Alaszewski and Mike Titterton, 59-84. Oxford: Oxford University Press, 2008.

Hood, Christopher, Henry Rothstein and Robert Baldwin. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford: Oxford University Press, 2001.

Huber, Martin and David Imhof. "Machine learning with screens for detecting bid-rigging cartels". *International Journal of Industrial Organization* 65 (2019): 277-301.

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Draft Ethics Guidelines for Trustworthy AI: Working Document for stakeholders' consultation*, December 18, 2018, https://digital-strategy.ec.europa.eu/en/library/draft-ethics-guidelines-trustworthy-ai.

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, April 8, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Policy and Investment Recommendations for Trustworthy AI*, June 26, 2019, https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations -trustworthy-artificial-intelligence.

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Policy and Investment Recommendations for Trustworthy AI*, June 26, 2019, https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations -trustworthy-artificial-intelligence.

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *Trustworthy AI Assessment List*, June 26, 2019, https://ec.europa.eu/futurium/en/ethics-guidelines-trustworthy-ai/register-piloting-process-0.

Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, *The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, July 17, 2020, https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

Janssens, Christine. *The Principle of Mutual Recognition in EU Law*. Oxford: Oxford University Press, 2013.

Jesse, Mathias and Dietmar Jannack. "Digital nudging with recommender systems: Survey and future directions". *Computers in Human Behavior Report* 3 (2021): 1-14.

Kahneman, Daniel. *Thinking Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Kahneman, Daniel, Olivier Sibony and Cass R. Sunstein. *Noise: A Flaw in Human Judgement*. New York: Little, Brown and Company, 2021.

Kinsella, William J. "Being 'post-Fukushima': Divergent understandings of sociotechnical risk". *Fukushima Global Communication Programme Working Paper Series* (2015). https://i.unu.edu/media/ias.unu.edu-en/news/12850/FGC-WP-18-FINAL.pdf.

Kranzberg, Melvin. "Technology and history: 'Kranzberg's laws'". *Technology and Culture* 27, no. 3 (1986): 544-560.

Lanzing, Marjolein. "'Strongly recommended' revisiting decisional privacy to judge hypernudging in self-tracking technologies". *Philosophy & Technology* 32, no. 3 (2019): 59-568.

Leese, Matthias. "The new profiling: Algorithms, black boxes, and the failure of antidiscriminatory safeguards in the European Union". *Security Dialogue* 45, no. 5 (2014): 494-511.

Lehman-Wilzig, Sam N. "Frankenstein unbound: Towards a legal definition of artificial intelligence". *Futures* 13, no. 6 (1981): 442-457.

Lodge, Martin. "Regulation, the regulatory State and European politics". *West European Politics* 31, no. 1-2 (2008): 280-301.

Loevinger, Lee. "Jurimetrics: Science and prediction in the field of law". *Minnesota Law Review* 46, no. 1 (1961): 255-275.

Lupton, Deborah. *Risk*. 2nd ed. Abingdon: Routledge, 2013.

Majone, Giandomenico. "The rise of the regulatory State in Europe". *West European Politics* 17, no. 3 (1994): 77-101.

McDonald, Aleecia M. and Lorrie Faith Cranor. "The cost of reading privacy policies". *I/S: A Journal of Law and Policy for the Information Society* 4, no. 3 (2008): 543-568.

McNamara, Andrew, Justin Smith and Emerson Murphy-Hill. "Does ACM's code of ethics change ethical decision making in software development?". *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (2018): 729-733.

Mindell, David A. *Our robots, ourselves: Robotics and the myths of autonomy*. New York: Viking Adult, 2015.

Mittelstadt, Brent. "Principles alone cannot guarantee ethical AI". *Nature Machine Intelligence* 1 (2019): 501-507.

Mittelstadt, Brent, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter and Luciano Floridi. "The ethics of algorithms: Mapping the debate". *Big Data & Society* 3, no. 2 (2016): 1-21.

Motta, Massimo and Michele Polo. "Leniency programs and cartel prosecution". *International Journal of Industrial Organization* 21, no. 3 (2003): 347-379.

Müller, Vincent C. (ed.). *Risks of Artificial Intelligence*. Boca Raton: Chapman and Hall/CRC, 2015.

Muschara, Tony. *Risk-Based Thinking: Managing the Uncertainty of Human Error in Operations*. Abingdon: Routledge, 2018.

Nemitz, Paul. "Constitutional democracy and technology in the age of artificial intelligence". *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 1-14.

Nissenbaum, Helen. "A contextual approach to privacy online". *Daedalus* 140, no. 4 (2011): 32-48.

Norman, Joseph, Rupert Read, Yaneer Bar-Yam and Nassim N. Taleb. "Climate models and precautionary measures". *Issues in Science and Technology* 31, no. 4 (2015): 15-16.

Parasuraman, Raja and Dietrich Manzey. "Complacency and bias in human use of automation: An attentional integration". *Human Factors* 52, no. 3 (2010): 381-410.

Peterson, Martin. *The Ethics of Technology: A Geometric Analysis of Five Moral Principles*. Oxford: Oxford University Press, 2017.

Petit, Nicolas. "Artificial Intelligence and automated law enforcement: A review paper". *SSRN*, March 21, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3145133.

Petit, Nicolas. *Droit Européen de la Concurrence*. Paris: Domat, 2013.

Petit, Nicolas and Jerome De Cooman. "Models of law and regulation for AI". In *The Routledge Social Science Handbook of AI*, edited by Anthony Elliott, 199-221. Abingdon: Routledge, 2021.

Rothstein, Henry, Phil Irving, Terry Walden and Roger Yearsley. "The risks of risk-based regulation: Insights from the environmental policy domain". *Environmental International* 32 (2006): 1056-1065.

Rubinstein, Ira S. "Big Data: The end of privacy or a new beginning?". *International Data Privacy Law* 3, no. 2 (2013): 74-87.

Rubinstein, Ira S. and Nathaniel Good. "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents". *Berkeley Technology Law Journal* 28, no. 2 (2011): 1333-1413.

Russel, Stuart and Peter Norvig. *Artificial Intelligence: A Modern Approach*. 3rd ed. Upper Saddle River: Pearson, 2010.

Sanchez-Grealls, Albert. "'Screening for cartels' in public procurement: Cheating at solitaire to sell fool's gold?". *Journal of European Competition Law & Practice* 10, no. 4 (2019): 199-211.

Sartor, Giovanni. "Human rights in the information society: Utopias, dystopias and human values". In *Philosophical Dimensions of Human Rights*, edited by Claudio Corradetti, 293-307. London: Springer, 2012.

Schrepel, Thibault. "Computational antitrust: An introduction and research agenda", *Stanford Computational Antitrust* 1 (2021): 1-15.

Senerath, Awanthika, Marthie Grobler and Nalin Asanka Gamagedara Archchilage. "Will they use it or not? Investigating software developers' intention to follow privacy engineering methodologies". *ACM Transactions on Privacy and Security* 22, no. 4 (2019): 1-30.

Smuha, Nathalie A. "From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence". *Law, Innovation and Technology* 13, no. 1 (2021): 57-84.

Smuha, Nathalie A. "The EU approach to ethics guidelines for trustworthy Artificial Intelligence". *Computer Law Review International* 4 (2019): 97-106.

Solove, Daniel J. "Introduction: Privacy self-management and the consent dilemma". *Harvard Law Review* 126, no. 7 (2013): 1880-1903.

Staksrud, Elisabeth. "Online grooming legislation: Knee-jerk regulation?". *European Journal of Communication* 28, no. 2 (2013): 152-167.

Symeonidis, Georges. "In which industries is collusion more likely? Evidence from the UK". *The Journal of Industrial Economics* 51, no. 1 (2003): 45-74.

Taleb, Nassim N. *The Black Swan. The Impact of the Highly Improbable*. New York: Random House, 2007.

Turchin Alexey and David Denkenberger. "Classification of global catastrophic risks connected with artificial intelligence". *AI & Society* 35 (2020): 147-163.

Tversky, Amos and Daniel Kahneman. "Judgement under uncertainty: Heuristics and biases". *Science* 185, no. 4157, (1974): 1124-1131.

van Dijk, Niels, Alessia Tanas, Kjetil Rommetveit and Charles Raab. "Right engineering? The redesign of privacy and personal data protection". *International Review of Law, Computers & Technology* 32, no. 2-3 (2018): 230-256.

von Bonin Andreas and Sharon Malhi. "The use of artificial intelligence in the future of competition law enforcement". *Journal of European Competition Law & Practice* 11, no. 8 (2020): 468-471.

von der Leyen, Ursula. *A Union that strives for more: My agenda for Europe*, July 16, 2019, https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf.

von der Leyen, Ursula. *Mission letter to Margrethe Vestager, Executive Vice-President for A Europe fit for the Digital Age*, Brussels, December 1, 2019, https://ec.europa.eu/commission/commissioners/sites/default/files/commissioner_mission_letters/mission-letter-margrethe-vestager_2019_en.pdf.

Wagner, Ben. "Ethics as an escape from Regulation: From ethics-washing to ethics shopping?". In *Being Profiled: Cogitas Ergo Sum: 10 Years of Profiling the European Citizen*, edited by Emre Bayamlioglu, Irina Baraliuc, Liisa Janssens and Mireille Hildebrandt, 84-89. Amsterdam: Amsterdam University Press, 2018.

Westerlund, Mika. "The emergence of deepfake technology: A review". *Technology Innovation Management Review* 9, no. 11 (2019): 40-53.

Whelan, Peter. *The Criminalization of European Cartel Enforcement: Theoretical, Legal, and Practical Challenges*. Oxford: Oxford University Press, 2014.

White House, The. *The Biden Administration Launches AI.gov Aimed at Broadening Access to Federal Artificial Intelligence Innovation Efforts, Encouraging Innovators of Tomorrow*, May 05, 2021, https://www.whitehouse.gov/ostp/news-updates/2021/05/05/the-biden-administration-launches-ai-gov-aimed-at-broadening-access-to-federal-artificial-intelligence-innovation-efforts-encouraging-innovators-of-tomorrow/.

Wickens, Christopher D., Benjamin A. Clegg, Alex Z. Vieane and Angelia L. Sebok. "Complacency and automation bias in the use of imperfect automation". *Human Factors and Ergonomics Society* 57, no. 5 (2015): 728-739.

Wildavsky, Aaron. *Searching for Safety: Social Theory and Social Policy*. Abingdon: Routledge, 2017, first published 1988.

Wright, David and John Copas. "Prediction scores for risk assessment". In *Law and Uncertainty: Risks and Legal Processes*, edited by Robert Baldwin, 21-38. London: Kluwer International Law, 1997.

Yeung, Karen. "'Hypernudge': Big Data as a mode of regulation by design". *Information, Communication & Society* 20, no. 1 (2017): 118-136.

Zerilli, John and Adrian Weller. "The technology". In *The Law of Artificial Intelligence*, edited by Matt Hervey and Matthew Lavy. London: Sweet & Maxwell, 2021.