4

Trading Artificial Intelligence

Economic Interests, Societal Choices, and Multilateral Rules

Dan Ciuriak and Vlada Rodionova

1 INTRODUCTION

After technology's decade of disillusion, societies confront the decade of decision: how to address the myriad issues already encountered with digital technology in reality or conceptualized in virtual realities, as use cases proliferate and as applications gain power. As a general-purpose technology with applications that can touch on virtually any human endeavour, the integration of artificial intelligence (AI) into social and economic frameworks poses particularly thorny issues. The full extent to which it will be embraced and the terms and conditions under which it will be allowed into our lives will likely vary across jurisdictions, reflecting differences in governance structures, societal preferences, and economic interests, with regulatory decisions being made in a context of limited experience, highly imperfect information, and at best a rudimentary understanding of the complex feedbacks that will be unleashed as the integration of AI proceeds.

From a trade perspective, regulatory decisions concerning the operation of AI within societies will constitute non-tariff measures (NTMs) that condition market access for the hyper-specialized AI applications that are already in use and the many more that are under development and slated to be brought to markets over the coming years.

The multilateral trade system has some experience addressing issues encountered with the introduction of new technologies, including the range of considerations bearing on risk tolerance, such as, inter alia, the use of available scientific evidence, the factors to be considered in assessing risk, the role of international standards in establishing acceptable levels of risk, and even in providing flexibility for differences in consumer tastes and preferences (i.e. political choice, including involvement of civil society) with regard to risk, including through the invocation of the precautionary principle.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

At the same time, the "dual-use" character of AI[1] and the data that train it[2] make national security entanglements seemingly unavoidable and perhaps even ultimately unbounded in scope, while the prospect of large valuable economic rents from AI applications incentivizes strategic trade and investment policies.[3]

With AI and machine learning (ML), we are navigating largely uncharted waters. The Stanford 100-year project on AI (Stanford AI100) advised against premature regulation on the grounds this could prevent the development of potentially beneficial technologies, stifle innovation, and/or drive innovation to less restrictive jurisdictions.[4] However, given the geopolitical AI arms race currently underway, and given the lure of large prospective economic rents, there is no likelihood of the pace of development and deployment of AI actually slowing down. By the same token, the terms and conditions under which AI accesses markets will be developed through a learning-by-doing process in which societies conduct natural experiments in allowing applications while "regulatory sandboxes" are used to develop the rules that in turn pave the way for international market access.

In this chapter, we discuss the rites of passage of AI as it enters the trading system. The next section discusses the challenge of getting AI applications to market and how they are being handled. Section III then discusses the hurdles that societal impacts may throw up, including national security, political choice, and income distribution. The final section ventures a discussion of how the integration of AI into international commerce might unfold.

II GETTING ARTIFICIAL INTELLIGENCE TO MARKET: NAVIGATING THE REGULATORY FRAMEWORK

A *The Artificial Intelligence Future Is Here*

If we replace the term "AI" with "smart", we realize immediately that AI is already all around us: AI applications power the smart assistants on cell phones, the range of smart home applications now widely in use, proliferating smart applications in business, and above all increasingly intelligent machines that combine a plethora of AI-driven functions to acquire increasingly flexible, human-like capabilities, up to and including humanoid robots

[1] G Allen and T Chan, "Artificial Intelligence and National Security" (2017) Belfer Center for Science and International Affairs, www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

[2] L Bezuidenhout, "Data Sharing and Dual-Use Issues" (2013) 19(1) *Science and Engineering Ethics* 83.

[3] D Ciuriak, "Economic Rents and the Contours of Conflict in the Data-Driven Economy" (2020) Centre for International Governance Innovation, www.cigionline.org/publications/economic-rents-and-contours-conflict-data-driven-economy.

[4] P Stone et al., "Artificial Intelligence and Life in 2030" (2016), http://ai100.stanford.edu/2016-report.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

carrying on conversations on stage[5] and AI television news anchors reading the news.[6]

Stanford AI100 places widespread introduction of ML in software services and mobile devices as starting in 2000,[7] even before the breakthroughs in technology that powered the development of modern AI. Kelly identifies these breakthroughs as follows:[8] the development of "deep learning" based on stacked neural networks by Geoffrey Hinton in 2006 (which effectively industrialized learning); the application of parallel processing computer chips to neural networks by Andrew Ng and his team at Stanford in 2009; and the accumulation of big data, which greatly increased with the mobile revolution that followed the introduction of the iPhone in 2007. Agrawal, Gans, and Goldfarb[9] place the commercial debut of AI only in 2012. Ciuriak and Ptashkina[10] place the dawn of the data-driven economy circa 2010, more or less coincident with the breakthroughs that powered the commercial application of AI.

Well before these breakthroughs, the development of regulatory frameworks and quality assurance systems for AI were already underway, since the basic issues raised in developing standards for AI were already encountered in developing quality assurance for "expert systems", which date back to the 1960s.[11] These systems were based either on data (encoded knowledge of a very specific area) or deep learning based on comprehensive structural knowledge of the subject matter, and used an "inference engine" that sought to mimic the decision-making process of a human expert.[12] The generic problems raised by these applications are as follows:

- The validation of an expert system requires human experts, who are in some sense more expert than the expert system itself. But leading human experts do not always agree, experts might not be available, and some might be biased; and the ethical contribution to a decision might be different from expert to expert.[13] And how does one validate AI that performs at levels superior to humans?

[5] See, for example, "DIA 2019 Munich, Robot Sophia Interview", www.youtube.com/watch?v=Y0HkIG2x4FU.

[6] See, for example, "Xinhua Unveils World's First Female AI News Anchor", www.youtube.com/watch?v=5iZuffHPDAw.

[7] See history timeline in the Stanford 100-year project on AI, "One Hundred Year Study on Artificial Intelligence (AI100), History" (Stanford University), https://ai100.stanford.edu/history-1.

[8] K Kelly, "The Three Breakthroughs That Have Finally Unleashed AI on the World" (27 October 2014), www.wired.com/2014/10/future-of-artificial-intelligence.

[9] A Agrawal et al., *Prediction Machines: The Simple Economics of Artificial Intelligence* (Boston, MA, Harvard Business Review Press, 2018).

[10] D Ciuriak and M Ptashkina, "The Data-Driven Economy and the Role of the State", in B Haggart et al. (eds), *Contests for Power and Authority in Internet Governance: Return of the State* (Routledge, in press) .

[11] E Feigenbaum, "Expert Systems: Principles and Practice", in BW Wah (ed), *The Encyclopedia of Computer Science* (New York, Wiley, 1992).

[12] J Rushby, "Quality Measures and Assurance for AI Software" (NASA Contract Report 4187, Washington, DC, 1988), www.csl.sri.com/papers/csl-88-7/csl-88-7r.pdf.

[13] For a discussion of ethical inputs into AI decisions, see A Etzioni and O Etzioni, "AI Assisted Ethics" (2016) 18 *Ethics and Information Technology* 149.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

- AI trained on data can only draw inferences within the scope and experience base of those data. But there is no way to definitively specify what is comprehensive coverage of the knowledge required to draw an expert inference. For example, humans often reason by analogy; how does one code the intuition that informs when an analogy is apt?
- Conventional validation requires precise testing of outputs. But definitive assessments are not possible with AI that will draw inferences from new information, even though the AI can be tested for repeatability and stability with given data inputs.

In the modern era, where AI is developed in non-deterministic processes through training on big data, in which the decision-making process cannot be broken down into sub-programs that can be individually tested, the problem becomes still more complex. While "black box" testing approaches have been developed, these are considered to be more "workarounds" than solutions to the problem of quality assurance.[14] Notably, an AI chatbot trained on Twitter quickly became a foul-mouthed racist and had to be shut down,[15] highlighting the issues raised for regulation by open-ended training data.

Notwithstanding these essentially unbounded concerns, use cases for AI through expert systems have proliferated and myriad applications have, as noted, already passed the applicable regulatory procedures and industry-established quality benchmarks without apparently encountering significant problems in terms of accessing international markets. How was this done? We turn to this question next.

B *Horizontal Standards*

The modern era of powerful AI emerged in a regulatory context informed by the experience acquired developing quality assurance for expert systems within the software engineering stream, under the auspices of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The ISO/IEC 90003 Software Engineering standards for expert systems date back to 1998. At the industry level, relevant quality assurance approaches include Total Quality Management (TQM), Six Sigma, and a number of others.

With technology rapidly advancing, many AI-specific standards are being developed at the national and international levels. For example:

[14] ME Mehle, "Quality Assurance for AI Software and Machine Learning" (*Cosylab*, 5 April 2020), www.cosylab.com/2020/04/05/qa-for-ai-and-ml.

[15] E Hunt, "Tay, Microsoft's AI Chatbot, Gets a Crash Course in Racism from Twitter" (*The Guardian*, 24 March 2016), www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

- The US National Institute of Standards and Technology (NIST) has released a Plan for Federal Engagement in AI Standards Development,[16] which lists nine areas of focus, including human interactions, performance testing, and trustworthiness. The US approach is generally "light touch", relying on self-regulation by industry, and emphasizing commercial opportunity.
- China's Standardization Administration of China (SAC) has released a White Paper to support China's international engagement on AI standards for key technologies and interoperability, including on algorithmic transparency, liability, bias, and privacy, among other ethical and security issues.[17]
- The European Commission has, inter alia, issued a White Paper on AI; a report on safety and liability implications of AI, the Internet of Things (IoT), and robotics; and, through a High-Level Expert Group, ethical guidelines for trustworthy AI.[18]
- Japan has established an Advanced Integrated Intelligence Platform Project (AIP), which features a comprehensive programme on AI, including standards.[19]
- The United Nations has been active on the human rights aspects of AI, developing recommendations on ethical issues raised by the development and application of AI.[20]
- The Organisation for Economic Co-operation and Development (OECD) Ministerial Council has agreed a set of high-level OECD Principles on Artificial Intelligence.[21]
- As regards the deeper issues raised by ML, international standards under development include the ISO/IEC CD 23053 ("Framework for Artificial Intelligence Systems Using Machine Learning") and the ISO/AWI TR 23348 ("Statistics – Big Data Analytics – Model Validation"). These may provide a common approach for assessing compliance of AI software in high-risk applications in regulated industries.[22]

[16] NIST, "U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools" (2019), www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[17] J Ding et al., "Chinese Interests Take a Big Seat at the AI Governance Table" (*New America*, 20 June 2018), www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table.

[18] European Commission, "Artificial Intelligence" (2020), https://ec.europa.eu/digital-single-market/en/artificial-intelligence.

[19] "About AIP" (*Riken*), https://aip.riken.jp/about-aip.

[20] "Elaboration of a Recommendation on the Ethics of Artificial Intelligence" (*UNESCO*), https://en.unesco.org/artificial-intelligence/ethics; J Pielemeier, "AI and Global Governance: The Advantages of Applying the International Human Rights Framework to Artificial Intelligence" (2019) United Nations University Center for Policy Research.

[21] "Forty-two Countries Adopt New OECD Principles on Artificial Intelligence" (OECD, 22 May 2019), www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm.

[22] Mehle, note 13 above.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

Trustworthiness standards are of particular interest as they cover a gamut of difficult issues, including accuracy, explainability, resiliency, safety, reliability, objectivity, and security.[23] The ISO technical committee on AI published its first overview of trustworthiness in AI only on 28 May 2020.[24] While this document discusses these various aspects of trustworthiness, the specification of *levels* of trustworthiness for AI systems remains beyond the scope of the ISO process. And, of course, it is precisely the level of trustworthiness where social and political choice is decisive, as demonstrated by the heated debate over the use of facial recognition by public authorities.[25]

Progress in these areas is being driven by necessity because AI is being deployed commercially and regulation cannot wait. For example, the European Union's (EU's) General Data Protection Regulation (GDPR) establishes explainability as a right: under the GDPR, individuals have a right to ask businesses that use their personal data for automated processing how decisions that affect them were made – and businesses must be able to explain to be compliant. Moreover, the GDPR establishes the right to request human intervention for review of an AI decision, and grants new investigatory, advisory, corrective, and punitive powers to the EU's data protection authorities, putting firms on notice.[26] Explainability has also engaged the attention of the military in developing protocols for military use of AI.[27] "Explainable AI" has thus become an important frontier for research[28] – and, indeed, has acquired its own acronym, "XAI".

In short, while horizontal AI-specific regulations were largely missing in action in the early phase of integration of AI into the economy and society, this gap is fast being filled.

[23] NIST, note 15 above, at 3.

[24] Technical Committee ISO/IEC JTC 1/SC 42 on Artificial Intelligence, www.iso.org/obp/ui/#iso:std:iso-iec:tr:24028:ed-1:v1:en.

[25] M Andrejevic and N Selwyn, "Facial Recognition Technology in Schools: Critical Questions and Concerns" (2020) 45 *Learning, Media and Technology* 115; M Hirose, "Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology" (2016) 49 *Connecticut Law Review* 1591; J Greene, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM" (*Washington Post*, 22 June 2020), www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition.

[26] For a sceptical view of the reality of the "right of explainability" under the GDPR, see S Wachter et al., "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7 *International Data Privacy Law* 76; for a view that the overall scheme "provides a muscular 'right to explanation' with sweeping legal implications for the design, prototyping, field testing, and deployment of automated data processing systems", see B Casey et al., "Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise" (2019) 34 *Berkeley Technology Law Journal* 145.

[27] M Turek, "Explainable Artificial Intelligence (XAI)" (*DARPA*, 2020), www.darpa.mil/program/explainable-artificial-intelligence.

[28] AB Arrieta et al., "Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges Toward Responsible AI" (2019) 58 *Information Fusion* 82; D Gunning et al., "XAI – Explainable Artificial Intelligence" (2019) 4 *Science Robotics* 7120.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

C *Vertical or Industry/Product-Specific Standards – Mechanical Functions*

The largely unimpeded commercial progress of AI to date has arguably reflected several characteristics of the market, in addition to the general absence of restrictive horizontal standards:

- Industrial applications were developed by highly sophisticated companies working with sophisticated clients, including government agencies, with the AI embedded in machinery that was subject to an industry- or sector-specific (hence "vertical") regulatory framework.
- Consumer-facing applications were embedded in products marketed mostly by "superstar" firms (e.g. cell phones with "smart" assistants and other AI-powered applications) and subject to product-specific standards and regulations administered by designated agencies with deep expertise in regulating on behalf of unsophisticated households.

The least problematic applications from a standards perspective are those where AI performs purely mechanical functions; performance in these types of functions tends to be measurable and the behaviour of the AI, even with learning, converges to an observable standard. AI applications that replace human cognitive/decision functions and involve agency on the part of the AI (i.e. where the AI makes autonomous decisions with real-world impacts) attract more regulatory attention. Applications can of course combine mechanical and cognitive functions. Accordingly, certification for domestic markets of particular AIs may involve a multiplicity of approvals.

One of the most straightforward uses of AI is to automate routine business or production processes or to reassign specific human functions to machines for accuracy. These types of applications have been adopted rapidly and widely and spread globally, without seemingly encountering barriers.

Industry is already familiar with industrial robots. Integrating AI into an industrial robot makes the robot more intelligent in the sense of being able to perform more complex functions. In such traditional industrial robotic applications, robots can substitute for particular human roles entirely and even work in isolation from humans. A quintessential example is provided by the role of AI in supply chain management automation. The integration of AI, improved sensors, sophisticated warehouse management software, IoT telecommunications systems, and automated robotic technology effectively allows warehouses to operate autonomously on a literally "lights-out" basis.[29]

More commonly, AI applications in workplace settings support human–robot interaction within a shared workspace. Instead of replacing people with autonomous modules, such collaborative AIs (so-called cobots), trained with ML techniques and

[29] R Bowles, "Warehouse Robotics: Everything You Need to Know in 2019" (*Logiwa*, 24 August 2020), www.logiwa.com/blog/warehouse-robotics.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

big data, work with humans, providing extra precision, speed, and consistency without fatigue in routinized tasks, while leaving the less routine aspects to humans. There are many examples of cobot applications already in use.[30] One example is "pick and place" functions, which involve mundane repetitive tasks that require cognition and result in errors due to boredom; such jobs can be more efficiently (and more safely given the propensity for repetitive strain injuries) done by robots with advanced vision systems and trained by AI, while the human member of the team focuses on aspects that require decisions. Another is "packaging and palletizing", which includes a range of functions from shrink-wrapping and boxing to placing products on a pallet for shipment.

Routine quality inspection functions are also being turned over to cobots that inspect finished parts by comparing images from multiple high-resolution cameras that capture all angles of a product simultaneously and are not prone to mental fatigue. More sophisticated cobot applications under development include an aircraft inspection assistant cobot in the "Hangar of the Future", which automates aircraft inspection as part of maintenance, repair, and overhaul operations.[31] Trucking is likely to go down this route with AI systems taking over the long-haul highway portions, leaving the first and last mile which involve more complicated environments to human drivers.

While many (if not most) of these tasks involve AI enabling the replacement of physical labour by robots, there are other cases where the AI replaces the skilled function. It is typically the case in these instances that the AI is hyper-competent and the AI's work is superior to the human's. This is likely the future for much assembly-type manufacturing that requires precision work such as automotive and aircraft assembly – see, for example, the use of AI and ML techniques to refine the installation of aircraft skins by Boeing.[32] Healthcare has emerged as a major use case for cobots where the AI is hyper-competent in this sense, particularly surgery-assisting cobots that use AI to improve the precision of surgical procedures.[33]

Other interesting examples of this include Sony's Hawkeye in tennis, which uses AI to make line calls. In tennis, the AI over-rules the human line caller in a challenge. In the 2020 US Open, AI made all the line calls on fifteen of the

[30] Robotics Online Marketing Team, "Robotic Surgery: The Role of AI and Collaborative Robots" (*Robotics Online Blog*, 9 July 2019), www.robotics.org/blog-article.cfm/Robotic-Surgery-The-Role-of-AI-and-Collaborative-Robots/181.

[31] "Hangar of the Future: Excelling in MRO" (Airbus, 6 December 2016), www.airbus.com/newsroom/news/en/2016/12/Hangar-of-the-future.html.

[32] H Solan, "Artificial Intelligence, Machine Learning Advances Hit Factory Floor" (Boeing), www.boeing.com/features/innovation-quarterly/feb2019/people-aifactory.page.

[33] Robotics Online Marketing Team, note 29 above; V Chalmers, "Scientists Develop a Ground-Breaking Robot 'Which Could Revolutionise Spinal Surgery' Because It Can Drill Holes with 0.1mm Accuracy - Better Than EVER Recorded for Humans" (*Daily Mail*, 7 January 2019), https://med.news.am/eng/news/20680/scientists-develop-a-ground-breaking-robot-which-could-revolutionise-spinal-surgery-because-it-can-drill-holes-with-01mm-accuracy–better-than-ever-recorded-for-humans.html.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

seventeen courts;[34] meanwhile, in the 2020 French Open, the failure to deploy the AI line-calling system was decried following an apparent mis-call at a critical moment in the match between Canada's Denis Shapovalov and Spain's Roberto Carballes Baena, leading to a rising tide of sentiment within the professional ranks in favour of the system. A retail market version ("InOut") is already in use.[35] Similar applications have been developed for goal-line decisions in football.[36] Baseball is experimenting with turning over the ball-strike calls to AI based on analysis that human umpires incorrectly call pitches (e.g. Chen et al. find that umpires call only about 60 per cent of close pitches accurately and show systematic bias due to effects such "anchoring" or the "gambler's fallacy"[37]). In its first baseball application, the human is advised by the AI and it is the human that makes the definitive call.[38]

Clearly, such AI applications have navigated complex sector-specific regulatory systems to get to market (such as those for medical devices or civil aviation) – or none at all (such as those for sports). From a trade perspective, the technology typically enters a new market either through foreign direct investment or through a transaction between a sophisticated supplier and a sophisticated buyer with considerable tailoring of the application to the specific circumstances and needs of the buyer. Accordingly, the future for the international dissemination of such AI applications does not appear to be any more problematic than its experience to date has been.

D *Vertical or Industry/Product-Specific Standards – Cognitive/Decision Functions*

AI that performs human cognitive/decision functions, in contexts where agency is involved and the decision criteria are less clear-cut and the consequences more significant than making a ball/strike call in baseball or a line call in tennis, will likely face substantially higher hurdles to achieve acceptance. The essential analogue would be competence regulation for human experts. Depending on the nature of the judgements the AI would be called to make, how it is trained might come into play.

[34] C Clarey, "Automated Line Calls Will Replace Human Judges at U.S. Open" (*The New York Times*, 3 August 2020), www.nytimes.com/2020/08/03/sports/tennis/us-open-hawkeye-line-judges.html.

[35] "In/Out v2.0: The Portable Line Call Device with Millimeters Accuracy" (Inout), https://inout.tennis/en/index.htm.

[36] L Silkin, "Artificial Intelligence: The New Driving Force Behind Sports Performance and Entertainment" (Lexology, 13 February 2019), www.lexology.com/library/detail.aspx?g=7d3990a1-0a9e-4f2b-8a6d-2a2b5b035730.

[37] D Chen, TJ Moskowitz, and K Shue, "Decision-Making under the Gambler's Fallacy: Evidence from Asylum Judges, Loan Officers, and Baseball Umpires" (NBER Working Paper No. 22026, February 2016).

[38] J Bogage, "Baseball's Robot Umpires Are Here. And You Might Not Even Notice the Difference" (*Washington Post*, 10 July 2019), www.washingtonpost.com/sports/2019/07/10/baseballs-robot-umpires-are-here-you-might-not-even-notice-difference.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

In the legal domain, for example, the amount of unstructured data mobilized for legal cases is enormous. It is no surprise that natural language processing (NLP) and image recognition techniques lend themselves to extract efficiencies in the preparation of legal cases. As the marketing of these tools is between sophisticated businesses, there are no apparent issues.

At the same time, deploying advanced algorithms in actual legal procedures raises concerns related to the core principles and guarantees of judicial systems. In this regard, the European Commission for the Efficiency of Justice (CEPEJ) adopted the first European Ethical Charter[39] on the use of AI in the justice system in 2018. The charter outlines principles to guide policymakers, legislators, and justice professionals to help them to embrace and, where needed, confront the spread of AI applications in judicial systems. These principles aim to ensure compliance with fundamental rights, non-discrimination, quality and security, transparency, and controllability.

In the latter regard, international practice already shows the wide range of possibilities in how societies might act: China has established an AI Internet court presided over by an AI judge for cases involving legal disputes in the digital domain;[40] Estonia has launched a project to build a robot judge to preside over small claims disputes involving sums of less than € 7,000;[41] the United States allows a limited yet still controversial[42] use of AI in informing legal decisions concerning whether to incarcerate defendants pending trial; but France, on the other hand, has banned the use of AI in legal proceedings.[43] This effectively spans the waterfront of possible positions on AI's role from full agency, to supporting role, to outright ban.

Healthcare is also witnessing pioneering developments of AI applications, given the availability of enormous amounts of data that greatly exceeds human cognitive capacity to effectively manage,[44] increases in computational power, and the

[39] "European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment" (2018), https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

[40] G Du and M Yu, "Big Data, AI and China's Justice: Here's What's Happening" (*China Justice Observer*, 1 December 2019), www.chinajusticeobserver.com/a/big-data-ai-and-chinas-justice-heres-whats-happening.

[41] V Kumar, "AI Moves to Court: The Growing Footprints of AI in the Legal Industry" (*Analytics Insight*, 23 January 2020), www.analyticsinsight.net/ai-moves-court-growing-footprint-ai-legal-industry.

[42] "Using risk assessment tools to make fair decisions about human liberty would require solving deep ethical, technical, and statistical challenges, including ensuring that the tools are designed and built to mitigate bias at both the model and data layers, and that proper protocols are in place to promote transparency and accountability. The tools currently available and under consideration for widespread use suffer from several of these failures", Partnership on AI, "Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System" (2019), www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system.

[43] See Legifrance (2019), www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000038261761?r=nrSLylJGaZ. The Justice Reform Act, Article 33 limits judicial analytics. "The identity data of magistrates and members of the registry cannot be reused with the object or effect of evaluating, analyzing, comparing or predicting their actual or supposed professional practices" [free translation].

[44] ME Matheny et al., "Artificial Intelligence in Health Care: A Report from the National Academy of Medicine" (2020) 323 *Journal of the American Medical Association* 509.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

development of ML techniques to retrieve information from unstructured data as well as in imaging and signal detection tasks. As a result, the healthcare system provides many examples of AI that are already widely deployed in areas such as radiology, oncology, and ophthalmology,[45] and even general medical decision-making, such as triaging patients in a hospital setting;[46] and AI-powered chatbot triage services as an alternative to telephone helpline services to dispense healthcare advice and direct patients to local and out-of-hours medical services.[47]

Not all AI products for healthcare face significant regulatory oversight – for example, consumer-facing platforms or assistants that dispense conventional advice (e.g. guiding patients in their preparation for surgery or through the recovery process). Such applications that are already widely distributed involve modern versions of expert systems that are embedded in online products and that are relatively simple in terms of the understanding of terminology, data protection, human involvement, safety, and risk management. The level of trustworthiness can be decided by market competition which fosters industry standards as regards accuracy, robustness of technical capabilities, and other application-specific criteria. Standards can be overwritten by authorities if any concerns arise.

The US Food and Drug Administration (FDA) has taken the lead in developing a regulatory framework for approval of AI/ML medical devices in more critical applications.[48] It has established three levels of clearance for AI/ML-based medical applications, namely:

- a 510(k) which clears Class I or II devices for market if they can be established to be at least as safe and effective as another similar, legally marketed device;
- pre-market approval for Class III devices that require greater regulatory evaluation of the scientific evidence because of potential risks to health (e.g. pacemakers); and
- a de novo pathway for novel medical devices for which there are no legally marketed counterparts, for which the FDA performs a risk-based assessment to establish safety and effectiveness.

Already we can see the potential for differing conclusions across major regulatory jurisdictions as to what is sufficiently safe and effective to be put on the market, given the scope for differing risk tolerances, including for devices requiring pre-market clearance where there is potential for different regulatory agencies to reach different conclusions; and even more so for de novo devices.

[45] S Benjamens et al., "The State of Artificial Intelligence-Based FDA-Approved Medical Devices and Algorithms: An Online Database" (2020) 3 *Digital Medicine* 1.

[46] S Horng et al., "Creating an Automated Trigger for Sepsis Clinical Decision Support at Emergency Department Triage Using Machine Learning" (2017) 12 *PLOS One* 1.

[47] S O'Hear, "Babylon Health Partners with UK's NHS to Replace Telephone Helpline with AI-Powered Chatbot" (TechCrunch, 4 January 2017), https://techcrunch.com/2017/01/04/babylon-health-partners-with-uks-nhs-to-replace-telephone-helpline-with-ai-powered-chatbot.

[48] Benjamens et al., note 43 above.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

An example of embedded AI that provides a glimpse into the regulatory framework through which it moves is provided in the aviation sector, where aircraft incorporate a myriad of systems that co-share flying operations with human pilots,[49] performing both mechanical and cognitive functions. In the Boeing 737 Max case, a faulty sensor resulted in incorrect information being fed into an AI system (the automated flight-control system, Maneuvering Characteristics Augmentation System, or MCAS), which resulted in two crashes.[50] An international panel of experts[51] was formed to review the causes of the breakdowns in Boeing's internal safety disciplines and the US Federal Aviation Authority's certification and oversight procedures. The panel made a dozen recommendations,[52] which established de facto conditions for the re-entry into service of this Boeing aircraft around the world.

E *The Locked Versus the Unlocked*

Since the first AI/ML device received FDA approval (a wearable-tech monitoring system introduced in 2012),[53] some sixty-four AI/ML-based medical devices and algorithms have received FDA approval and been put on the market. While this early experience is encouraging, a still more complex issue has been encountered in this area. The current regulatory approach for medical devices was designed for devices that are "locked" (i.e. devices that give the same answer each time the same inputs are presented) and feature only discrete modifications from time to time. It is now recognized that this needs to be adapted for algorithms that *learn* with each application.[54]

In this regard, the FDA has put out a discussion paper setting out a proposed regulatory framework for modifications to AI/ML-based Software as a Medical

[49] L Eliot, "Boeing 737 MAX 8 and Lessons for AI: The Case of AI Self-Driving Cars" (AI Trends, 22 March 2019), www.aitrends.com/ai-insider/boeing-737-max-8-and-lessons-for-ai-the-case-of-ai-self-driving-cars.

[50] R Kraus, "'Aggressive and Riskier' A.I. – and Bureaucracy – Caused the Boeing Crashes, Report Says" (Mashable, 2 June 2019), https://mashable.com/article/boeing-737-max-aggressive-risky-ai.

[51] The Joint Authorities Technical Review (JATR) comprised experts from two US agencies (the Federal Aviation Authority and the National Aeronautics and Space Administration), and civil aviation authorities from Australia, Brazil, Canada, China, Europe, Indonesia, Japan, Singapore, and the United Arab Emirates.

[52] W Bellamy III, "International Regulators Submit Joint Technical Review of 737 MAX Flight Control System to FAA" (*Aviation Today*, 14 October 2019), www.aviationtoday.com/2019/10/14/international-regulators-submit-joint-technical-review-737-max-flight-controls-faa.

[53] "Bringing to Market Solutions Based on Their Health Platform That Incorporates Mobile, Tablet, Cloud and Physiological Monitoring Technologies for Early Screening and Diagnosis through Completion of Care, Preventice Is Helping Health Care Providers Achieve Higher-Quality Outcomes" (CEOCFO, 7 January 2013), www.ceocfointerviews.com/interviews/Preventice12-CEOCFO-Article.pdf.

[54] Benjamens et al., note 43 above.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

Device (SaMD), which involves a total lifecycle approach to regulation, based on four principles:[55]

- establish clear expectations on quality systems and good ML practices (GMLP);
- conduct pre-market review for those SaMD that require pre-market submission to demonstrate reasonable assurance of safety and effectiveness and establish clear expectations for manufacturers of AI/ML-based SaMD to continually manage patient risks throughout the lifecycle;
- monitor the AI/ML device and incorporate a risk management approach and other guidance in development, validation, and execution of algorithm changes; and
- transparency to users and FDA using post-market real-world performance reporting for maintaining continued assurance of safety and effectiveness.

These principles – in particular the third, which requires a continual programme of monitoring and validation – highlight the issues posed by the inherent fluidity of deployed AI/ML devices and algorithms that are undergoing continuous modification with acquired experience. Coupled with the ubiquitous concerns about bias and data security, this fluidity underscores the need to establish and maintain a high-trust environment between the creators of the AI, the user community, and the regulators. Similar levels of confidence and transparency will be required between national regulatory bodies to ensure international market access. However, as AI will rely heavily on trade secrets to protect the intellectual property in AI applications (e.g. algorithms and data), the issues concerning the quality and biases inherent in the data used to train AI algorithms may prove to become points of friction in international trade.

III GETTING ARTIFICIAL INTELLIGENCE TO MARKET: NAVIGATING SOCIETAL CHOICE AND INSECURITY

While the integration of AI into the trading system has been more or less seamless at the technical level, as it begins to have systemic significance, new hurdles are likely to emerge. Three of these in particular loom large as potential points of friction: societal impacts, national security concerns, and the question of the impact of AI on jobs. We address these next.

A *Societal Impacts*

The nexus of AI/ML/big data not only impacts at the micro level on individuals and firms but also drives a complex co-evolution of technology, the economy, and society

[55] FDA, "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD)" (2019), www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

that takes on its own dynamic, as captured in the title of Kevin Kelly's 1994 book, *Out of Control: The New Biology of Machines, Social Systems, and the Economic World*. The pace of evolution in machine space is dictated by the resources committed to innovation and thus is almost arbitrarily fast. The technological instinct is indeed to move fast and disrupt; however, with disruptive technological change, the co-evolution of societal structures and of the economy ensures that, along with all that is gained, there is also much that is lost. Moreover, governance systems that evolved in an age of much slower technological change are not well equipped to get out in front of the implications of new technologies. The result is system friction:

> The shift of our economy and society online is taking place without referendum. What could go wrong? As it turns out, plenty.[56]

This friction surfaced in the "techlash" that flared in the second half of the 2010s.[57] There were numerous contributing factors beyond the pace of change. For example, there was widespread apprehension about the potentially dystopian directions of change,[58] many of which were popularized by the television series, *Black Mirror*, and even amplified by Elon Musk who said in an interview, "With artificial intelligence we're summoning the demon".[59] The fragility of democracy in silico was underscored by the revelation of manipulation of electorates in historical events such as the Brexit Referendum and the 2016 Trump presidential campaign by firms such as Cambridge Analytica using Facebook data and applying AI-driven quantitative social psychology tools.[60]

Even more fundamentally, the concentration of wealth enabled by the data-driven economy irrevocably altered the balance of power within modern societies. This is underscored by the fact that a company like Facebook has 2.5 billion clients

[56] D Ciuriak and B Wylie, "Data and Digital Rights: More Questions Than Answers – But Enumerating the Questions Is Essential" (2018), https://papers.ssrn.com/abstract=3300263.

[57] R Botsman, "Dawn of the Techlash" (*The Guardian*, 11 February 2018), www.theguardian.com/commentisfree/2018/feb/11/dawn-of-the-techlash; E Smith, "The Techlash Against Amazon, Facebook and Google – and What They Can Do" (*The Economist*, 20 January 2018), www.economist.com/briefing/2018/01/20/the-techlash-against-amazon-facebook-and-google-and-what-they-can-do; RD Atkinson et al., "A Policymaker's Guide to the 'Techlash' – What It Is and Why It's a Threat to Growth and Progress" (Information Technology and Innovation Foundation, 28 October 2019), https://itif.org/publications/2019/10/28/policymakers-guide-techlash.

[58] W Hartzog and E Selinger, "Facial Recognition Is the Perfect Tool for Oppression" (2018), http://cyberlaw.stanford.edu/publications/facial-recognition-perfect-tool-oppression.

[59] G Kumparak, "Elon Musk Compares Building Artificial Intelligence to 'Summoning The Demon'" (TechCrunch, 26 October 2014), https://techcrunch.com/2014/10/26/elon-musk-compares-building-artificial-intelligence-to-summoning-the-demon.

[60] RD Atkinson et al., note 56 above. C Cadwalladr, "The Great British Brexit Robbery: How Our Democracy Was Hijacked" (*The Guardian*, 7 May 2017), www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy; T Gross, "Reporter Shows the Links Between the Men Behind Brexit and the Trump Campaign" (National Public Radio, 19 July 2018), www.npr.org/2018/07/19/630443485/reporter-shows-the-links-between-the-men-behind-brexit-and-the-trump-campaign.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

for its applications[61] – more than the populations of the United States, the EU, and China combined. This change in power relations was evidenced in the behaviour of the technology CEOs who did not fail to sense their new status:

> By displacing the print and broadcast media in influencing public opinion, technology is becoming the new Fourth Estate. In our system of checks and balances, this makes technology co-equal with the executive, the legislature, and the judiciary. When this new Fourth Estate declines to appear before [the International Grand Committee] – as Silicon Valley executives are currently doing – it is symbolically asserting this aspirational co-equal status. But it is asserting this status and claiming its privileges without the traditions, disciplines, legitimacy or transparency that checked the power of the traditional Fourth Estate.[62]

These factors combined to generate pushback on the technology companies, their CEOs, and indeed the practical implementation of the technology nexus of AI/ML and big data.

At the national level, the likely source of issues for international trade will be invocation of the precautionary principle to exclude certain uses or technologies altogether based on societal preferences. The international community has some practical experience with this. Generally, under the World Trade Organization (WTO) Agreement, in particular the Technical Barriers to Trade (TBT) Agreement and the Agreement on the Application of Sanitary and Phytosanitary Measures (the "SPS Agreement"), countries have the right to set higher standards than accepted international standards,[63] although they are subject to general tests of reasonableness such as avoiding arbitrary or unjustifiable distinctions in risk tolerance across different situations (including, of course, not discriminating against imports compared to domestic products). At the same time, where relevant scientific evidence is insufficient, a WTO member may provisionally apply restrictive measures based on available pertinent information subject to the requirement that a more objective assessment of risk is made within a reasonable period.[64] While not directly referencing the precautionary principle that is formally incorporated in multilateral environmental agreements such as the Cartagena Protocol on Biosafety, the WTO Agreement thus does allow for precaution in setting rules.[65]

[61] A Hutchinson, "Facebook Climbs to 2.5 Billion Monthly Active Users, But Rising Costs Impede Income Growth" (*Social Media Today*, 30 January 2020), www.socialmediatoday.com/news/facebook-climbs-to-25-billion-monthly-active-users-but-rising-costs-imped/571358.

[62] J Balsillie, "Jim Balsillie: 'Data Is Not the New Oil – It's the New Plutonium'" (*Financial Post*, 28 May 2019), https://financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium.

[63] S Charnovitz, "The Supervision of Health and Biosafety Regulation by World Trade Rules" (2000) 13 *Tulane Environmental Law Journal* 271.

[64] Article 5.7 of the SPS Agreement.

[65] The panel in the WTO dispute on marketing approvals by the EU for genetically modified organisms referred to the "precautionary approach" (WTO Panel Report, *EC – Approval and Marketing of Biotech Products*, para. 7.3065).

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

This base of experience, particularly the extensive debate concerning the precautionary principle,[66] helps prepare us for the challenges of carving out legitimate policy-based derogations for trade in AI from the freedom of commerce that international economic law defends.

A likely more challenging aspect of the pushback is at the sub-national level. A quintessential example of this, given the breadth of issues raised, was the communitarian response to the ambitious, futuristic smart city proposal for the Toronto waterfront Quayside district put forward by Sidewalk Labs, a subsidiary of Alphabet/Google, which aimed to essentially "disrupt the neighbourhood" in multiple dimensions.[67] This proposal was eventually withdrawn after a concerted battle by community activists.[68]

Governance flashpoints in the Sidewalk Toronto case included the proposal to claim a share of property taxes (essentially privatizing municipal governance); privacy concerns about the capture of the enormous flow of data that the district would generate through ubiquitous sensors (concerns which led to the resignation of the privacy adviser, Ann Cavoukian);[69] and more general governance concerns given that the administration of the smart city district would involve a private firm replacing regulations established through democratically accountable processes with its own frameworks[70] and digital incentives (e.g. one element of the plan was to grant residents access to certain spaces based on how much data they provide, or rewarding them for "good behaviour"[71]).

Another set of objections focused on the financial aspects of the proposal, starting with the inside track that Alphabet/Google appeared to have had for the project,[72]

66 IM Goklany, *The Precautionary Principle: A Critical Appraisal of Environmental Risk Assessment* (Washington, DC, Cato Institute, 2001); J Tait, "More Faust Than Frankenstein: The European Debate about the Precautionary Principle and Risk Regulation for Genetically Modified Crops" (2001) 4 *Journal of Risk Research* 175; G Majone, "What Price Safety? The Precautionary Principle and Its Policy Implications" (2002) 40 *Journal of Common Market Studies* 89; CR Sunstein, "Beyond the Precautionary Principle" (2003) 151 *University of Pennsylvania Law Review* 1003; CJ Pereira Di Salvo and L Raymond, "Defining the Precautionary Principle: An Empirical Analysis of Elite Discourse" (2010) 19 *Environmental Politics* 86.

67 C Crowe, "Disruptor of the Year: Sidewalk Labs" (Smart Cities Dive, 9 December 2019), www.smartcitiesdive.com/news/smart-city-disruptor-sidewalk-labs-alphabet-toronto-dive-awards/566277; N Ahmed, "The City vs. Big Tech" (*Briarpatch Magazine*, 2 July 2019), https://briarpatchmagazine.com/articles/view/the-city-vs.-big-tech.

68 Ibid.

69 J O'Kane, "Privacy Expert Ann Cavoukian Resigns from Sidewalk Toronto Smart-City Project: 'I Had No Other Choice'" (*Globe and Mail*, 2018), www.theglobeandmail.com/business/article-privacy-expert-ann-cavoukian-resigns-from-sidewalk-toronto-smart-city.

70 For example, Sidewalk Labs proposed designing a system for Digital Transparency in the Public Realm to facilitate what it termed "the co-creation of prototypes that can advance digital transparency and enable agency in the world's public spaces". "Designing for Digital Transparency in the Public Realm" (Sidewalk Labs), www.sidewalklabs.com/dtpr.

71 Ahmed, note 66 above.

72 D Skok, "Cracks in the Sidewalk" (MacLeans, 1 April 2019), https://archive.macleans.ca/article/2019/4/1/cracks-in-the-sidewalk.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

which evoked the sense of overweening influence wielded by "big tech"; the vast asymmetry in information between the Canadian government bodies negotiating the deal and Sidewalk Labs, in particular concerning the ownership and ultimate monetization of the intellectual property and data that the smart city would generate;[73] and the economic power that the administering company, a multinational digital "superstar" firm, would have had over the district, which raised the omnipresent sceptre of market failure to which the data-driven economy is inherently susceptible.[74]

The Sidewalk Toronto example highlights the likely role of cities and communitarian activism in mediating social acceptance of AI. We have already seen communitarian activism drive policy on single-use plastics and Styrofoam products, with some US states and cities banning their use; and, highlighting the frictions, we have also seen some states imposing pre-emptive laws to *prevent* their cities from banning such products.[75] The use of AI for facial recognition has similarly met with divergent policies, with embrace in some states and bans in others[76] – and even international sanctions for alleged human rights abuses.[77] Reflecting the reading of public opinion, Microsoft, Amazon, and IBM publicly committed not to sell facial recognition to police departments because of human rights concerns over surveillance and racial profiling in the context of Black Lives Matters protests, until there is federal legislation that regulates its use and takes into account human rights issues.[78]

The scope for sub-national variance of treatment is also illustrated by regulations being developed for autonomous vehicles. Husch and Teigen highlight the many differences in the rules frameworks that have been adopted in the United States, where regulation of autonomous vehicles falls to the states.[79] Since 2012, there has been inconsistent acceptance, with some forty states having enacted legislation related to autonomous vehicles, implemented an executive order, or both.[80]

With urbanization growing steadily and expected to raise the share of the world's population living in cities from over 55 per cent in 2020 to 68 per cent

[73] J Hinton and N Raffoul, "For Economic Outcomes of Sidewalk Toronto We Need to Talk about Intellectual Property" (*The Globe and Mail*, 18 February 2019), www.theglobeandmail.com/business/commentary/article-for-economic-outcomes-of-sidewalk-toronto-we-need-to-talk-about.

[74] D Ciuriak, "The Economics of Data: Implications for the Data-Driven Economy" (2018), https://papers.ssrn.com/abstract=3118022.

[75] CT Schlachter, "Regulation Trends on Plastic Bag Bans and Preemptions" (2019) Working Paper.

[76] K Hill, "The Secretive Company That Might End Privacy as We Know It" (*New York Times*, 18 January 2020), www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[77] R Orol, "Can Sanctions Keep China's Surveillance Market in Check?" (CIGI, 12 November 2019), www.cigionline.org/articles/can-sanctions-keep-chinas-surveillance-market-check.

[78] Greene, note 45 above.

[79] B Husch and A Teigen, "Regulating Autonomous Vehicles" (2017) 25 Legis Brief.

[80] "Autonomous Vehicles, Self-Driving Vehicles Enacted Legislation" (National Conference of State Legislatures, 18 February 2020), www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

by 2050,[81] cities will gain increasing clout in governance and will be looking for technological solutions to the infrastructure and administrative challenges posed by newly highlighted pandemic risks, environmental sustainability imperatives, and income inequality. They will thus be both the *demandeurs* for AI technology and the battlegrounds for its acceptance.

B *National Security*

The digital transformation, the advent of the data-driven economy, and particularly the coming implementation of fifth-generation telecommunications networks (5G) and IoT applications, which 5G will power, combine to fundamentally transform the concept of national security. This reflects in the first instance the proliferation of vulnerabilities to cyber attacks, whether from state actors, from criminal elements (e.g. ransomware attacks on cities and public institutions), or even from university students gaming the system (e.g. the infamous Mirai bot event that crippled the Internet in 2016 was initially thought to be the work of a state actor before being traced to US college students).[82] As 5G and growing AI applications transform the backbone infrastructure of an economy (i.e. transportation, telecommunications, energy, and finance) from a passive utility into an interactive "central nervous system",[83] national security principles have to be updated quite fundamentally.

Importantly from a trade perspective, these vulnerabilities are fundamentally different from those that informed the crafting of the current WTO national security exception as set out in the General Agreement on Tariffs and Trade (GATT) Article XXI. The framers of the GATT had World War II and the use of nuclear bombs in mind when providing examples of issues that might reasonably trigger the Article – circumstances that relate to fissionable materials (that is, nuclear weapons), traffic in arms, or measures taken in time of war or other emergencies in international relations.

By contrast, cyber attacks are high-frequency and relatively low-cost events, mostly carried out by bots with limited attributability to anyone, including to state actors. Security firm F-Secure, which deploys decoy servers to attract such attacks (so-called honeypots), recorded 5.7 billion attacks in 2019, up from 1.0 billion in 2018.[84]

[81] "68% of the World Population Projected to Live in Urban Areas by 2050, Says UN" (UN, 16 May 2018), www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html.

[82] B Bours, "How a Dorm Room Minecraft Scam Brought Down the Internet" (*Wired*, 13 December 2017), www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet.

[83] J Balsillie, "Six Recommendations for the International Grand Committee on Disinformation and 'Fake News'" (CIGI, 7 November 2019), www.cigionline.org/articles/six-recommendations-international-grand-committee-disinformation-and-fake-news.

[84] J Stattler, "Attack Landscape H22019" (F-Secure, 4 March 2020), https://blog.f-secure.com/attack-landscape-h2-2019-an-unprecedented-year-cyber-attacks.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

Sacramento-based Sutter Health reported 87 billion cyberthreats encountered in 2018.[85]

The cyber context resembles that of a biological immune system in a biosphere full of viruses, mostly fighting them off, but sometimes catching a cold – unpleasant but with consequences that fall far short of those associated with kinetic war (let alone nuclear war). The first suspected death attributable to a nonstate cyber attack occurred in 2020 in Duesseldorf, when a ransomware attack on a university hospital forced redirection of emergency cases elsewhere, delaying critical care.[86] The financial costs of such attacks are estimated in the millions of dollars but the overall cost at the economy level for the United States in 2019 amounted to only perhaps USD 7.5 billion or 0.036 per cent of US GDP.[87]

To be sure, the costs of disruption of infrastructure by state actors could be substantially higher – for example, a "kill switch" on an electrical grid being triggered. This possibility appears to have been established by infiltrations by governments of rivals' systems.[88] However, given the multiple sources of risks (including human, software, and hardware), it is far from clear that these concerns (or related concerns of cyber espionage) warrant extreme measures that preclude trade, such as the US' "5G Clean Path" programme that aims to freeze Chinese telecommunications equipment suppliers out of 5G systems outside of China.[89]

The WTO has little experience in dealing with national security issues as an exception.[90] One reason is that "trade restrictions during the Cold War period mainly related to non-Members, and there was no great need for justification under GATT".[91] Another is that countries were reluctant to set

[85] N Wetsman, "Health Care's Huge Cybersecurity Problem" (*The Verge*, 4 April 2019), www.theverge.com/2019/4/4/18293817/cybersecurity-hospitals-health-care-scan-simulation.

[86] N Wetsman, "Woman Dies During a Ransomware Attack on a German Hospital" (*The Verge*, 17 September 2020), www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity.

[87] A Hope, "Ransomware Costs in 2019" (*CPO Magazine*, 15 January 2020), www.cpomagazine.com/cyber-security/ransomware-costs-in-2019.

[88] D Volz and T Gardner, "In a First, U.S. Blames Russia for Cyber Attacks on Energy Grid" (*Reuters*, 15 March 2018), www.reuters.com/article/us-usa-russia-sanctions-energygrid-idUSKCN1GR2G3.

[89] This programme is framed as an attempt to "address the long-term threat to data privacy, security, human rights and principled collaboration posed to the free world from authoritarian malign actors". The programme effectively blacklists vendors, such as ZTE and Huawei. The initiative not only prevents US companies from buying services and products from untrusted vendors but also requires the leading US and foreign companies to remove their apps from the Huawei app store. See "The Clean Network" (US Department of State), www.state.gov/the-clean-network.

[90] D Ciuriak and M Ptashkina, "Toward a Robust Architecture for the Regulation of Data and Digital Trade" (2020) CIGI Paper No. 240; JB Heath, "National Security and Economic Globalization: Toward Collision or Reconciliation?" (2019) 42 *Fordham International Law Journal* 1431.

[91] T Cottier and P Delimatsis, "Article XIV bis GATS: Security Exceptions", in R Wolfrum et al. (eds), *WTO – Trade in Services: Max Planck Commentaries on World Trade Law: Vol. 6* (Leiden, Nijhoff, 2008).

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

precedents that might be used against them, and thus figuratively opening Pandora's box.[92]

Not surprisingly, the framing of national security exemptions in trade agreements is evolving. For example, the recent update of the North American Free Trade Agreement (NAFTA) – the US-Canada-Mexico Agreement (USMCA) – included a GATT Article XXI-type exception but dropped the examples. Unfortunately, it provided no alternative language, leaving fully open the question of what kinds of national security risks in this digital age would support an abrogation of trade commitments. This gap is especially problematic given the evolution of the global system of production and trade into a "made in the world" system of global value chains.

Decoupling and repatriation of international supply chains comprise one possible solution to national security concerns, but this would come at some considerable economic efficiency cost, would not actually remove the vulnerabilities from the IoT framework, and would in any event not be a realistic option for any economy other than perhaps the United States, the EU, or China.

AI finds itself in the eye of this particular storm. It is central to the national security frameworks of the major powers. As a practical example, China has indicated it would block the transfer of the AI algorithm underpinning the ByteDance TikTok operation.[93] The problem in this instance is not that the AI cannot get into a market, but rather that it cannot leave a market. This risk will hang over other companies – will Tesla, for example, be allowed to transfer its Chinese-developed technology to the USA if US bans on transfer of US technology to China continue? At the same time, control of AI that is in a position of influence over popular opinion in a country clearly will not be allowed for companies from countries that are considered strategic competitors.

Accordingly, national security could be a conversation killer for AI when market access comes up in an international trade context.

C *Labour Markets and the New "Guilded Age"*

AI can be thought of as a new form of productive capital – machine knowledge capital. As such, it is likely to complement human skills in some tasks and compete with them in others. If we think of "jobs" as packages of "tasks",[94] automation of tasks results in partial automation of all jobs. Consistent with the experience of skill-biased

[92] S Kho and T Peterson, "Turning the Tables: The United States, China, and the WTO National Security Exception" (*China Business Review*, 16 August 2019), www.chinabusinessreview.com/turning-the-tables-the-united-states-china-and-the-wto-national-security-exception.

[93] Z Xin and T Qu, "TikTok's Algorithm Not for Sale, ByteDance Tells US: Source" (*South China Morning Post*, 13 September 2020), www.scmp.com/economy/china-economy/article/3101362/tiktoks-algorithm-not-sale-bytedance-tells-us-source.

[94] M Arntz et al., "The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis" (2016) OECD Social Employment and Migration Working Papers No. 189.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

technological change over the past several decades,[95] income inequality is likely to increase as workers whose skills are mainly complemented by AI will realize rising returns to their human capital, while those whose skills are mostly substituted by AI will face job loss or strong downward competitive pressure on wages.[96]

Various scenarios have been suggested for the impact of AI on labour markets. Pessimistic scenarios[97] conclude there will be heavy job destruction. Less pessimistic scenarios[98] conclude that automation will mainly transform jobs rather than destroy them, but that low-qualified workers will likely bear the brunt of the adjustment costs since a greater proportion of their tasks can be automated compared to highly qualified workers. The main challenges in this scenario are facilitating job/task transition with training and addressing income inequality. Meanwhile, technology optimists conclude that AI will create jobs.[99]

Regardless of which scenario ultimately obtains, it seems clear that a new factor of production will claim its share of national income – and since this new factor primarily competes with human brain work, it follows that this share of income will be clawed away from today's white-collar work force. The current organization of society and economy in advanced countries in terms of status and income is based on human capital. People invest heavily to acquire both the knowledge capital and the credentials. Even though student debt is often crippling, the overall returns to a university degree are still very substantial: an estimate of the net present value of a university degree in the United States in 2018 was, on average, USD 344,000.[100] At the same time, at a price point where the annual cost of college equals USD 50,000, the odds of the investment in a college degree paying off fall to about 50–50.[101]

What happens in this context when the rents to higher education are eroded – that is, when the incomes that drive the net present value of a degree fall? The answer is, of course, structural adjustment along many margins – demand for higher education falls, prices fall, and the supply of this service contracts. Universities and colleges are pillars of their local economies. So these college towns would suffer as well from the multiplier effects. In this regard, the AI shock to white-collar work and the social organization around it in the advanced economies would resemble the China shock to industrial work and the social organization around it in the advanced countries in

[95] See for example, E Berman et al., "Implications of Skill-Biased Technological Change: International Evidence" (1998) 113 *Quarterly Journal of Economics* 1245.

[96] J Blit et al., "Automation and the Future of Work: Scenarios and Policy Options" (2018) CIGI Papers No. 174.

[97] CB Frey and MA Osborne, "The Future of Employment: How Susceptible Are Jobs to Computerisation?" (2017) 114 *Technological Forecasting & Social Change* 254.

[98] Arntz et al., note 93 above.

[99] B Reese, "AI Will Create Millions More Jobs Than It Will Destroy. Here's How" (Singularity Hub, 1 January 2019), https://singularityhub.com/2019/01/01/ai-will-create-millions-more-jobs-than-it-will-destroy-heres-how.

[100] D Webber, "Is College Worth It? Going Beyond Averages" (Third Way, 18 September 2018), www.thirdway.org/report/is-college-worth-it-going-beyond-averages.

[101] Ibid.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

the first decades of the twenty-first century[102] – except that the AI shock will likely be larger and likely come faster.

The political ramifications of this in the advanced countries can only be guessed at; however, the best guide perhaps is what happened with the China shock to industrial jobs and incomes – protectionism of all sorts. AI should expect a similar welcome as it starts to make serious inroads into the rents currently captured by white-collar work and to undermine the social edifice built on those rents.

In pre-industrial times, the protection of rents flowing to skilled artisans was through craft guilds. In their day, these acted as professional associations, restricting entry to capture rents, but also enforcing quality standards, preserving and transferring knowledge inter-generationally through the apprenticeship system, and providing financial support for their members.[103] Modern professions such as law, medicine, accounting, and architecture replicate guild practices by requiring a licence, passing a qualifying exam, or acquiring a diploma from a formal programme of study.[104] The modern guilds have been able to resist international services trade liberalization and may be expected to mobilize to moderate the entry of AI into their functions to protect the rents that flow to knowledge credentials. From this perspective, the age of AI – at least in its early years and decades – may be a new "guilded age" in which the professions find ways (which trade economists would see as non-tariff barriers) to restrict market entry.

IV DISCUSSION AND CONCLUSIONS

AI has made impressive inroads into our economy and society, but this was far from an overnight success, as it struggled through many decades and several AI winters, disappointing many hopes and prognostications along the way. With the emergence of the data-driven economy, the technological conditions for AI to blossom were finally in place – and blossomed it has. AI is now all around and contributes importantly to the value of internationally traded goods and services.

For the most part, AI has navigated the regulatory path to market entry without problems. However, as AI has become more powerful, high-level concerns have started to mount about its impact on society, national security, and the livelihoods of those who will compete with it. Based on the experience to date, regulatory concerns that could create market barriers to AI in the future are likely to align with the Pareto principle (the "80–20" rule), whereby most of the issues will prove to be easily handled at least at the technical level, allowing the integration of AI into economic

[102] David Autor et al., "The China Shock: Learning from Labor-Market Adjustment to Large Changes in Trade" (2016) 8 *Annual Review of Economics* 205.

[103] SR Epstein, "Craft Guilds, Apprenticeship, and Technological Change in Preindustrial Europe" (1998) 58 *The Journal of Economic History* 684.

[104] MS Larson, *The Rise of Professionalism: A Sociological Analysis* (Berkeley, CA, University of California Press, 1977).

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

and social life to proceed apace, while a smaller subset of cases that generate cross-cutting societal impacts and raise security and economic distributional concerns will generate most of the headaches.

The transition of AI from executing instructions to exercising agency, which raises thorny issues for legal doctrines,[105] still lies largely ahead and raises rather open-ended questions about social acceptance, alongside the already thorny issues raised by its use as a tool for political influence and social regulation. Also mostly ahead are the impacts of AI on the job market – in particular on white-collar work and the social structures built around human capital in the advanced economies (although blue-collar work will not be entirely spared either, as AI combined with robots will make the latter more flexible and more competitive with blue-collar workers).

A complicating factor (as if the above were not complicated enough!) is that AI is being developed at a pace that exceeds the ability of regulators to regulate it. This has stalled deployment of AI in domestic contexts (e.g. several major US firms have declined to supply AI for facial recognition until federal regulations are established) and promises to be still more problematic internationally, given that trust is at a nadir internationally – particularly between China and the United States, the two leading AI/ML centres. While this state of affairs seems unpromising for future collaboration, it might be noted that professional exchanges between the Chinese and US epidemiological communities during the COVID-19 crisis were as cordial and forthcoming as the political relations were not. Science transcends national boundaries and with AI/ML we will be dealing with truly cutting-edge science. Moreover, the issues of trust between humans might become rather moot when AI clearly surpasses individual human expertise. The path for AI into practice has generally been cleared by simple demonstrations of its capacity to do better.

The potential difficulty of untangling these issues is well illustrated by the US ban on the TikTok app based on its ownership by China's ByteDance. This case has triggered commentaries focused on the societal risks of the app itself,[106] the alleged national security risks posed by the data it collects,[107] and the value of the company (as much as USD 50 billion[108]).

History has been described as one damn thing after another. The first decade of the data-driven economy proved to be one of increasingly dense history, with

[105] Y Bathaee, "The Artificial Intelligence Black Box and The Failure of Intent and Causation" (2018) 31 *Harvard Journal of Law & Technology* 889.

[106] J Ochs, "The Negative Impact of TikTok on Teens" (Smart Social, 21 January 2020), https://smartsocial.com/negative-impact-tiktok.

[107] J Sherman, "Unpacking TikTok, Mobile Apps and National Security Risks" (Lawfare Blog, 2 April 2020), www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks.

[108] E Wang et al., "Exclusive: ByteDance Investors Value TikTok at $50 Billion in Takeover Bid – Sources" (*Reuters*, 29 July 2020), www.reuters.com/article/us-bytedance-tiktok-exclusive-idUSKCN24U1M9.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

the year 2020 serving up a perfect storm of historical developments. The technology nexus of AI/ML/big data played a not insignificant role in generating that history and also found itself an increasingly divisive bone of contention. As new applications proliferate, the discussion in this chapter suggests that the path of AI to international markets will become more complicated.

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press

https://doi.org/10.1017/9781108954006.005 Published online by Cambridge University Press