PROCEEDINGS OF SCIENCE

Regulating Emerging Technologies: Opportunities and Challenges for Latin America

Mirjana Stankovic, PhD, LLM[1]
Tambourine Innovation Ventures
World Bank Group
University of North Carolina at Chapel Hill
USA
E-mail: mirjana.stankovic@fulbrightmail.org

Nikola Neftenov, LLM
Tambourine Innovation Ventures
North Macedonia
E-mail: nick@tivinc.com

The world is on the brink of an all-encompassing technological and social revolution moving with exponential velocity. Innovative technological trends such as Artificial Intelligence (AI), the Internet of Things (IoT), robotics, 3D printing, nanotechnology, augmented and virtual reality, emerge and converge, generating the Fourth Industrial Revolution (4IR).

The 4IR exists in a social setting and not just as a disruptive business case. Societies need to design regulatory approaches that are not only human-led and human-centered, but also nature-led and nature-centered. Balance needs to be struck between *societal and public interests*, such as human dignity and identity, trust, nature preservation and climate change, and *private sector interests*, such as business disruptiveness and profits. As novel business models such as fintech and the sharing economy emerge, regulators are faced with a host of challenges that range between rethinking traditional regulatory models, coordination problems, regulatory silos, and the robustness of dated rules.

This paper will highlight the unique regulatory challenges posed by emerging technologies in the 4IR: the unpredictable nature of business models that rely on emerging technologies; the importance of data ownership, control, privacy and security; and the AI conundrum. The paper then will proceed in defining and providing a set of 4 principles to guide the future of regulation in the 4IR: innovative and adaptive regulation, outcome-focused regulation, evidence-based regulation, and collaborative regulation.

Artificial Intelligence for Science, Industry and Society, AISIS2019
October 21-25, 2019
Universidad Nacional Autónoma de México, Mexico City, México

[1] Speaker

1. Introduction

The world is on the brink of an all-encompassing technological and social revolution moving with exponential velocity. Innovative technological trends such as Artificial Intelligence (AI), the Internet of Things (IoT), robotics, 3D printing, nanotechnology, augmented and virtual reality, emerge and converge, generating the Fourth Industrial Revolution (4IR).[2] This revolution is different than the previous ones due to the extensiveness of its scope and the vitality of its impact on human interaction and identity, distribution, production and consumption systems around the globe. The 4IR is pervasive and non-linear; oftentimes the consequences of emerging technologies cannot be anticipated with certainty. The 4IR is an era where machines learn on their own; self-driving cars communicate with smart transportation infrastructure; and smart devices and algorithms respond to and predict human needs and wants.

In order to optimally leverage the 4IR for societal benefits, we need governance frameworks, protocols and policy systems that ensure inclusive and equitable benefits for all. The 4IR exists in a social setting and not just as a disruptive business case. Societies need to design regulatory approaches that are not only human-led and human-centered, but also nature-led and nature-centered. Balance needs to be struck between *societal and public interests*, such as human dignity and identity, trust, nature preservation and climate change, and *private sector interests*, such as business disruptiveness and profits. As novel business models such as fintech[3] and the sharing economy[4] emerge, regulators are faced with a host of challenges that range between rethinking traditional regulatory models, coordination problems, regulatory silos, and the robustness of dated rules.

Undeniably, a complex web of regulations would impose prohibitive costs on new entrants into markets led by development of emerging technologies. Global digital talent is concentrated in developed countries and in the hands of a few large firms. Imposing cumbersome compliance costs with a robust system of regulations would lead to a situation where only large firms could afford to comply. This reinforces the need to build flexible and dynamic regulatory models to respond to the changes and optimize their impact.[5]

Emerging technologies might lead to unforeseeable outcomes absent clear regulations and ethical guidelines. This risk is exacerbated by the fact that novel technologies can be used by private individuals or non-state actors more easily. These technologies can have damaging repercussions in the field of data privacy, information and cyber security, providing hackers with ways to access sensitive personal data, hijack systems or manipulate devices that are connected to the Internet.[6]

This paper will highlight the unique regulatory challenges posed by emerging technologies in the 4IR: the unpredictable nature of business models that rely on emerging technologies; the importance of data ownership, control, privacy and security; and the AI conundrum. The paper then will proceed in defining and providing a set of 4 principles to guide

[2] K. Schwab, *The Fourth Industrial Revolution: What it Means, How to Respond,* World Economic Forum, 2016 [https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/].

[3] Financial technology (Fintech) is used to describe new tech that seeks to improve and automate the delivery and use of financial services. At its core, fintech is utilized to help companies, business owners and consumers better manage their financial operations, processes, and lives by utilizing specialized software and algorithms that are used on computers and, increasingly, smartphones. Fintech, the word, is a combination of "financial technology". J. Kagan, *What is Financial Technology – Fintech,* Investopedia, 2019 [https://www.investopedia.com/terms/f/fintech.asp].

[4] The sharing economy is an economic model defined as a peer-to-peer (P2P) based activity of acquiring, providing, or sharing access to goods and services that is often facilitated by a community-based on-line platform. Most notorious examples are Uber and AirBnB. J. Chappelow, *Sharing Economy,* Investopedia, 2019 [https://www.investopedia.com/terms/s/sharing-economy.asp].

[5] Y. Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation,* Harvard Journal of Law & Technology, Volume 31, Number 2 Spring 2018 [https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf].

[6] N. Al-Rodhan, *Security, Ethics and Emerging Technologies,*World Economic Forum, 2014 [https://www.weforum.org/agenda/2014/03/security-ethics-emerging-technologies/].

the future of regulation in the 4IR: innovative and adaptive regulation, outcome-focused regulation, evidence-based regulation, and collaborative regulation.

1.1 Regulatory challenges in the Fourth Industrial Revolution era

Can regulators keep up with fintech?” “Your Apps Know Where You Were Last Night, and They’re Not Keeping It Secret.” “Regulators scramble to stay ahead of self-driving cars.” “Digital health dilemma: Regulators struggle to keep pace with health care technology innovation.” Headlines like these have been a central challenge to regulators across the globe.

Traditional regulatory structures are complex, fragmented, risk averse, and adjust slowly to shifting social circumstances, with various public agencies having overlapping authority. In contrast, a unicorn startup can develop into a company with global reach in a matter of a couple of years, if not months. For instance, Airbnb went from start-up in 2008 to a Silicon Valley unicorn in 2011 valued at a billion dollars, based on $112 million invested by venture capitalists.[7]

Mexico and Uruguay are the only two countries from Latin America that have developed and are developing AI policies and strategies to date. These policies and strategies provide a structure for the use of AI in the public sector, as well as a roadmap for where the private sector should direct its investments. Currently, a coherent strategy or approach to AI does not exist in Latin America. This situation, however, is not an isolated case as it follows a similar path to those in other related fields, such as open data and digital government. Generally, a few governments are leaders in terms of policy making and agenda setting, with other regional governments following suit. [8] Argentina on the other hand, has expressed ambitions towards creating a long-term National AI Plan for both the public and private sectors since 2019. This National AI Plan falls under the country’s Innovative Argentina 2030 Plan and the 2030 Digital Agenda. Through the creation of this strategy, Argentina wants to promote the development of an AI ecosystem within its borders, and anticipate some of the risks this emerging technology could pose in terms of ethics and data protection.[9]

Emerging technologies are multifaceted and transcend national boundaries. Since there are no global regulatory standards, coordinating with regulators across borders is a challenge. This chapter presents the most salient issues related to regulation of emerging technologies: the unpredictable nature of business models that rely on emerging technologies; the importance of data ownership, control, privacy and security; and the AI conundrum.

1.1.1 The unpredictable nature of business models that rely on emerging technologies

Products and services that have embedded emerging technologies’ solutions evolve quickly and shift from one regulatory category to another. For example, if a ride-hailing company begins delivering food, it can fall under the jurisdiction of health regulators. If it expands into delivering drone services, it will fall under the purview of aviation regulators. If it uses self-driving cars for passengers, it may come under the jurisdiction of telecommunications regulators. Maintaining consistency in regulations is difficult in the sharing economy where the lines between categories and classification of services and products are often blurred.

An illustrative example in this regard is Airbnb.[10] Regulators around the world have been wondering if they should regulate Airbnb as a real estate service, and thus subject the company to

[7] Agence France-Presse, *Airbnb: The First 10 Years- Start-Up to Unicorn to US$30 Billion Business,* South China Morning Post, 2018 [https://www.scmp.com/lifestyle/travel-leisure/article/2153851/how-airbnb-founders-went-cash-strapped-roommates].

[8] H. Miller, R. Stirling, *Government Artificial Intelligence Readiness Index 2019,* Oxford Insights, 2019 [https://www.oxfordinsights.com/ai-readiness2019].

[9] Bnamericas, *National AI Policies Popping Up Across South America,* Bnamericas, 2019 [https://www.bnamericas.com/en/news/national-ai-policies-popping-up-across-south-america--marketing-or-strategy].

[10] Airbnb, Inc. is an online marketplace for arranging or offering lodging, primarily homestays, or tourism experiences. The company does not own any of the real estate listings, nor does it host events; it acts as a broker, receiving commissions from each booking, at http://www.airbnb.com/.

property regulations. Recently, Airbnb has won a court battle in the European Union (EU) that affects how the company is regulated in the future. The EU's Court of Justice has ruled that Airbnb should not be considered an estate agent but an "information society service," meaning it can avoid certain responsibilities and continue operating as an e-commerce platform.[11]

Uber[12] faced a similar predicament, and in 2017 the EU Court of Justice ruled that the company is a transportation service, and not a platform. The Court ruled that the difference between Uber and Airbnb is in the level of control exercised by Airbnb over the services hosted on its platform. Unlike Uber that has controlled pricing and automatically paired up sellers and customers, Airbnb has allowed property owners to set their own prices and rent their homes using other channels.[13]

The evolving, interconnected nature of disruptive business models can also make it difficult to assign liability for the harm done. For example, if a self-driving car crashes and kills someone, who is going to be held liable – the system's programmers, the driver behind the wheel, or the car's manufacturer, or the manufacturer of the vehicle's onboard sensory equipment? The general inclination across different jurisdictions has been towards assigning strict liability[14] for the damage caused by emerging technologies, under certain circumstances, such as use of these technologies in public spaces (e.g., drones, self-driving cars).[15]

The legal concept of liability is challenged even more by the concept of reinforcement learning, a training method that allows AI to learn from past experiences. Imagine a scenario where an AI-controlled traffic light learns that it is more efficient to change the light one second earlier, and this leads to more drivers running the light and causing more accidents. In this particular example, human control is several times removed, hence making it difficult for regulators to assign liability. [16]

3D printing is another emerging technology that challenges the traditional legal concept of liability. If a 3D house crashes down, who is to blame – the supplier who supplied the design, the manufacturer who 3D printed the house parts, or the manufacturer of the 3D printer?

Blockchain and its decentralized nature present different type of concern to regulators. Even though blockchain applications have been praised for their security and immutability, their anonymous and decentralized nature is a novel challenge for regulators around the globe. An illustrative example in this regard is the cyberattack of the Decentralized Autonomous Organization (DAO), a decentralized investment fund running on Ethereum, a blockchain platform. DAO's creators intended to build a democratic financial institution whose code would eliminate the need for human control and oversight. However, in 2016 a hacker took advantage of a flaw in DAO's code and stole $50 million of virtual currency. The hacker has not been identified yet, and due to the decentralized nature of the system liability cannot be assigned to anyone or anything.[17]

[11] J. Porter, *Airbnb Avoids Tougher Regulation in Europe as EU Court Rules it's not an Estate Agent,* The Verge, 2019 [https://www.theverge.com/2019/12/19/21029606/airbnb-estate-agent-eu-ruling-platform-regulation].

[12] Uber Technologies, Inc., commonly known as Uber, is an American multinational ride-hailing company offering services that include peer-to-peer ridesharing, ride service hailing, food delivery, and a micromobility system with electric bikes and scooters, at https://www.uber.com/.

[13] Ibid.

[14] J. Villasenor, *Products Liability law as a Way to Address AI Harms,* Brookings, 2019 [https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/]; P. Opitz, *Civil Liability and Autonomous Robotic Machines: Approaches in the EU and US,* TTLF Working Papers No.43, 2019 [https://law.stanford.edu/wp-content/uploads/2019/02/opitz_wp43.pdf].

[15] European Commission, *Liability for Artificial Intelligence and Other Emerging Digital Technologies,* European Commission, 2019 [https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199].

[16] Ibid.

[17] K. Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human,* WIRED, 2016 [https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/].

1.1.2. The importance of data: ownership, control, privacy and security

The rising use of smartphones, security cameras, connected devices, and sensors has created a massive digital footprint and data overload. An illustration of data overload can be seen in the case of self-driving cars that are expected to churn out around 4,000 gigabytes of data per day.[18]

People's lives can benefit greatly when decisions are informed by pertinent data that reveal hidden and unexpected connections and market trends. For instance, identifying and tracking genes associated with certain types of cancer can help inform and improve treatments. However, ordinary people, oftentimes unaware, bear many of the costs and risks of participating in data markets. In many jurisdictions, the so-called data brokers are amassing and selling personal data, and this is a perfectly legal practice.[19]

The data economy brings along disruptive changes propelled by emerging technologies such as AI and machine learning. For instance, human bankers are already replaced by AI and big data. Many fintech lending startups have started using alternative data sources, and traditional insurance companies are following suit. Regulators are struggling in providing guidelines in this area that would enable the financial industry to innovate, and at the same time protect consumers from bias and discrimination. The New York's Department of Financial Services has released new guidelines[20] that will allow life insurance companies to use customers' social media data to determine their premiums (as long as they do not discriminate).[21]

From a regulatory point of view, the crux of the question is who has access and control over all this data. Is it the government, the users, or the service providers who store the data? From a legal perspective, data per se cannot be owned, and there is no legal system that offers ownership of raw data.[22]

If the service provider has access to personal information, what obligation does it have to store and protect it? Can personal data be shared with third parties, so-called data brokers? Can a car manufacturer charge a higher price to car buyers who refuse to share personal data?

There is no global agreement on data protection, and regulators around the globe take very different, oftentimes conflicting, stances in regulating data within their national borders. For instance, the EU's General Data Protection Regulation (GDPR)[23], as one of the most prominent regulatory instruments in data protection, provides for the principle of privacy, strict controls over cross-border data transmissions, and the right "to be forgotten". The GDPR will likely influence other countries in revising their data protection legislation. The GDPR is already having an extraterritorial grasp in the private sector's data transactions across borders. Global companies are revising privacy policies in compliance with the GDPR, and content websites outside Europe have already started denying access to European consumers because they could not ensure compliance with the GDPR.

Unlike the EU approach, the US approach has been more segmented and focused on sector-specific rules (e.g. health care, financial, and retail) and state laws. In the US, it is not

[18] S. Barua, *'Flood of Data Will Get Generated in Autonomous Cars',* Auto Tech Review, n.d. [https://autotechreview.com/features/flood-of-data-will-get-generated-in-autonomous-cars].

[19] L. Matsakis, *The WIRED Guide to Your Personal Data (and Who is Using it),* WIRED, 2018 [https://www.wired.com/story/wired-guide-personal-data-collection/].

[20] J. Baron, *Life Insurers Can Use Social Media Posts to Determine Premiums, as Long as They Don't Discriminate,* Forbes, 2019 [https://www.forbes.com/sites/jessicabaron/2019/02/04/life-insurers-can-use-social-media-posts-to-determine-premiums/#42002dc823ce].

[21] T. Lau, U. Akkaraju, *When Algorithms Decide Whose Voices Will Be Heard,* Harvard Business Review, 2019 [https://hbr.org/2019/11/when-algorithms-decide-whose-voice-will-be-heard?utm_campaign=hbr&utm_source=linkedin&utm_medium=social].

[22] C. F. Kerry, J. B. Morris, *Why Data Ownership is the Wrong Approach to Protecting Privacy,* Brookings, 2019 [https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/].

[23] European Commission, *Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock,* Brussels, COM(2019) 374 Final, 2019 [https://ec.europa.eu/info/law/law-topic/data-protection_en].

unusual for credit card companies to know what their customers consume. For instance, Uber knows where its customers go and how they behave while taking the drive. Facebook knows if its users like to read CNN or Breitbart News.

These differences in regulatory approaches stem from different cultural approaches to the issue of privacy. In the EU, the right to privacy, and the right to have personal data protected, are fundamental rights guaranteed by the EU Charter of Fundamental Rights.[24] The EU has an umbrella data protection framework that does not differentiate between data held by private or public actors, with only a few exceptions (e.g. national security). By contrast, in the US the right to privacy is not considered a fundamental right. The right to privacy is counter-balanced by strong rights to free speech and freedom of information. Nevertheless, even in the US, some cities and states have started regulating privacy following the EU's GDPR model.

Privacy of public data is usually protected through anonymization. Identifiable things such as names, phone numbers, and email addresses are stripped out. Data sets are altered to be less precise, and "noise" is introduced to the data. However, a recent study by Nature Communications[25] suggests that anonymization does not always equate privacy. Researchers from Imperial College London and the University of Louvain have developed a machine-learning model that estimates how easy individuals can be re-identified from an anonymized data set by entering their zip code, gender, and date of birth. On average, in the US, using those three records, you could be correctly located in an "anonymized" database 81% of the time. Given 15 demographic attributes of someone living in North Carolina, there's a 99.98% chance you could find that person in any anonymized database.[26]

Another key regulatory challenge in the era of emerging technologies is information security and cybersecurity. Cybersecurity is particularly important in areas such as fintech, digital health, digital infrastructure, and intelligent transportation systems where private, sensitive data can be compromised. Take for instance the case of self-driving cars that need to communicate between themselves and the transport infrastructure. Designers and manufacturers of self-driving cars should take necessary precautions to ensure that the system is not overtaken by hackers who might try to steer the vehicle into causing accidents, or to manipulate traffic lights in order to disrupt traffic.[27]

1.1.3. The AI conundrum

AI presents one of the most difficult challenges to traditional regulation. Three decades ago, one could think of a software being programmed. But the way to think about it in terms of shifting to an AI environment is that the software is not programmed anymore, it is trained. This is the main differing factor between programming and training. Today, we are dealing with networks of information that often have surprising capacities. AI is not organic intelligence, and it does not behave by following the same rules which humans abide by. AI is not simply replacing human activities external to human bodies; it is also replacing human decision-making inside human minds. AI itself is not one technology, or even one singular development. It is a bundle of technologies whose mode of decision-making is often not fully understood even by AI developers.

AI solutions can help address key global challenges and deliver significant benefits. However, AI also generates challenges related to inequality, privacy, and discrimination. Self-learning algorithms already anticipate human needs and wants, govern our newsfeeds, and drive

[24] European Parliament, *Charter of Fundamental Rights of the European Union,* Official Journal of the European Communities (2000/C 364/01), 2000 [https://www.europarl.europa.eu/charter/pdf/text_en.pdf].

[25] L. Rocher, J. M. Hendrickx, Y-A. De Montjoye, *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models,* Nature Communications, 2019 [https://nature.com/articles/s41467-019-10933-3].

[26] C. Jee, *You're Very Easy to Track Down, Even When Your Data Has Been Anaonymized,* MIT Technology Review, 2019 [https://www.technologyreview.com/s/613996/youre-very-easy-to-track-down-even-when-your-data-has-been-anonymized].

[27] M. D. Fenwick, W. A. Kaal, E. P. M. Vermeulen, *Regulation Tomorrow: What Happens When Technology Is Faster Than The Law?,* American University Business Law Review, Volume 6, Issue 3, 2017 [https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1028&context=aublr].

our cars. How can we ensure that this technology benefits people widely? If AI and autonomous machines are to play a key role in our everyday lives, what sort of normative and ethical frameworks should guide their design?

It is very difficult to relate something as technical as AI to a robust regulation. On one hand, most regulatory systems require transparency and predictability, on the other most lay people do not understand how AI works. The more advanced certain types of AI become, the more they become "black boxes", where the creator of the AI system does not really know the basis on which the AI is making its decisions. Accountability, foreseeability, compliance, and security are questioned in this regard.[28]

The "black box" problem

AI algorithms make strategic decisions, from approving loans to determining diabetes risk. Often these algorithms are closely held by the organizations that created them, or are so complex that even their creators cannot explain how they work. This is AI's "black box"—the inability to see what is inside an algorithm.

This problem has been exacerbated by the fact that regulators around the globe deploy algorithms for scoring systems to make decisions on sentencing, enforcement, and delivering social services to citizens. A study conducted by the AI Now Institute at NUY states that many of those systems are opaque to the citizens they hold power over.[29] Regulators have already started enacting regulations (algorithm accountability laws) that try to curtail the use of automated decision systems by public agencies. For instance, in 2018 New York City enacted a local Law in relation to automated decision systems used by agencies.[30] The Act created a task force to recommend criteria for identifying automated decisions used by city agencies, a procedure for determining if the automated decisions disproportionately impact protected groups. However, the law only permits making technical information about the system publicly available "where appropriate" and states that there is no requirement to disclose any "proprietary information".[31]

Some experts have suggested making algorithms open to public scrutiny. Many are not made public because of nondisclosure agreements with the companies that developed them. The EU GDPR requires companies to be able to explain how algorithms using the personal data of customers work and make decisions - the right to explanation. However, since this right has been mentioned in the Recital 71 of the GDPR many scholars point out that it is not legally binding. [32] Article 22 of the GDPR states that EU citizens can request that decisions based on automated processing concerning them or significantly affecting them and based on their personal data are made by natural persons, not only by computers. You also have the right in this case to express your point of view and to contest the decision.[33]

Another illustrative example of AI's black box in decision making is the case of using automated systems in recruitment and selection. Companies such as Goldman Sachs and Unilever

[28] M. Stankovic, R. Gupta, B. A. Rossert, G. I. Myers, M. Nicoli, *White Paper Exploring Legal, Ethical and Policy Implications of Artificial Intelligence,* Law, Justice and Development, 2017 [http://globalforumljd.com/new/sites/default/files/documents/resources/Artificial-Intelligence-White-Paper-Draft-5Oct2017.pdf].

[29] R. Richardson, J. M. Schultz, V. M. Southerland, *Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems,* AI Now Institute, 2019 [https://ainowinstitute.org/litigatingalgorithms-2019-us.html]; T. Simonite, *AI Experts Want to End 'Black Box' Algorithms in Government,* WIRED, 2017 [https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/].

[30] Local Law in Relation To Automate Decision Systems Used by Agencies of 2018 [https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0&Options=&Search].

[31] B. Kelly, Y. Chae, *INSIGHT: AI Regulations Aim at Eliminating Bias,* Bloomberg Law, 2019 [https://news.bloomberglaw.com/tech-and-telecom-law/insight-ai-regulations-aim-at-eliminating-bias].

[32] K. Hosanagar, V. Jair, *We Need Transparency in Algorithms, But Too Much Can Backfire,* Harvard Business Review, 2018 [https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire].

[33] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en

have used a hiring technology developed by the startup HireVue[34] that analyzes job candidates' facial expressions and voice to advise hiring managers.[35] It has been feared that using AI in hiring will re-create societal biases. This is compounded by the fact that the algorithm is a property of HireVue and its functioning and decision-making principles are kept secret from the public.[36] However, regulators have already started tackling these legal conundrums. For instance, the new Illinois Artificial Intelligence Video Interview Act[37] aims to help job candidates gain insight into how these hiring tools operate. According to this Act companies must notify applicants that AI will be used to consider applicants' "fitness" for a position. Companies should also elaborate on how these systems operate and what characteristics are considered when evaluating candidates. The companies must also enable candidates to consent to using automated hiring systems. The Law also limits who can view the recorded video interviews and mandates that firms must delete any video submitted by an applicant within a month of the applicant's request.[38]

Algorithmic bias

In a perfect world, using algorithms should lead to unbiased and fair decisions. However, many algorithms have been found to have inherent biases. AI systems can reinforce what they have been taught from data. They can amplify risks, such as racial or gender bias. Even a well-designed algorithm must make decisions based on inputs from a flawed and erratic reality. Algorithms can also make judgmental errors when faced with unfamiliar scenarios. This is the so-called artificial stupidity. Many such systems are "black boxes", the reasons for their decisions are not easily accessed or understood by humans—and therefore difficult to question, or probe. The fact that private commercial developers generally refuse to make their code available for scrutiny, because the software is considered proprietary intellectual property, is another form of non-transparency.

In 2016, ProPublica analyzed a commercially developed system that predicts the likelihood that criminals will re-offend, created to help judges make better sentencing decisions, and found that it was biased against people of color. [39]

Facial recognition algorithms have been proven to be biased when detecting people's gender. These AI systems were able to detect the gender of white men more accurately than gender of darker skin men. Similarly, Amazon's hiring and recruitment algorithm taught itself to prefer male candidates over female. The system was trained with data collected over a 10-year period that came mostly from male candidates.[40]

Several US cities, such as San Francisco and a few other communities have banned their police departments from using facial recognition.[41] The city council of Denver is also considering a facial recognition ban. Advocates of the regulation recently demonstrated that all nine members of the council could be matched to individuals on the local sex offender registry with 92% accuracy.[42]

[34] S. Chandler, *The AI Chatbot Will Hire You Now,* WIRED, 2017 [https://www.wired.com/story/the-ai-chatbot-will-hire-you-now/].

[35] Ibid.

[36] Tech Policy, *The AI Hiring Industry is Under Scrutiny – But it'll be Hard to Fix,* MIT Technology Review, 2019 [https://www.technologyreview.com/f/614694/hirevue-ai-automated-hiring-discrimination-ftc-epic-bias/].

[37] Public Act 101-0260, 2020 [http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101-0260].

[38] R. Heilweil, *Illinois Says You Should Know if AI is Grading Your Online Job Interviews,* VOX, 2020 [https://www.vox.com/recode/2020/1/1/21043000/artificial-intelligence-job-applications-illinios-video-interivew-act].

[39] J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias,* ProP [https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing].

[40] J. Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women,* Reuters 2018 [https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G].

[41] R. Metz, *Beyond San Francisco, More Cities are Saying no to Facial Recognition,* CNN Business, 2019 [https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html].

[42] J. Porter, *Surprising Results After Activists Test Facial Recognition Technology on Denver City Council,* The Denver Channel, 2020 [https://www.thedenverchannel.com/news/local-news/surprising-results-after-activists-test-facial-recognition-technology-on-

Humans make snap judgements about the people they meet for the first time. Our initial perception of a person may not always be correct. This is an issue faced by facial recognition which is still in its nascent stages. A group of Melbourne based researchers asked human volunteers to judge thousands of photos for the same characteristics and then used that dataset to create Biometric Mirror. Biometric Mirror uses an AI to analyze a person's face by scanning his or her face and later displays 14 characteristics about them, including their age, race, and perceived level of attractiveness. However, this analysis is more often than not false, as the AI generates this based on the subjective information provided to it by the initial human volunteers. This poses many challenges, as the AI can discriminate in unethical or problematic ways which could have societal consequences.[43]

Legitimate news and information are sometimes blocked, illustrating the weaknesses of AI in determining what is appropriate. For instance, Facebook blocked a 1972 Pulitzer Prize winning photo of a Vietnamese girl because of nudity. The company was accused of abusing its power and the photo was later reinstated. These examples have led to a growing argument that IT firms posting news stories should be subject to regulations similar to those that media firms face.

Deepfakes[44], computer-generated and highly manipulated videos or presentations, present another significant problem. Some governments have started regulating them. For instance, China has made it a criminal offense to publish deepfake videos created with AI or virtual reality. From January 2020 any deepfake video or audio recording should be clearly designated as such, otherwise content providers, which are expected to police the system, together with offending users will be prosecuted.[45] Facebook has issued a ban on users using deepfakes, in an attempt to stop the dissemination of misinformation in the upcoming 2020 US presidential election.[46] The problem with this policy is that it does not prohibit all computer manipulated videos; for instance the policy did not address a deceptively edited clip of the US House Speaker Nancy Pelosi that went viral on the social network in 2019. The video was sent by Facebook for review to a third-party fact-checker who rated it as "false," and de-ranked it in News Feeds, without removing it.[47]

An Orwellian scenario of algorithmic bias in regulation would require every citizen to get a social score, based on a set of values. The government services that citizens receive will be based on this score. Such a system is set to become fully operational in China in 2020.[48] The aim is for every Chinese citizen to be trailed by a file compiling data from public and private sources by 2020, and for those files to be searchable by fingerprints and other biometric features. Under the national social credit system people would be penalized for the crime of spreading online rumors, among other offenses, and that those deemed "seriously untrustworthy" can expect to receive substandard services.

The poor people problem in regulating AI

denver-city-council]; K. Johnson, *From Washington State to Washington, D.C., Lawmakers Rush to Regulate Facial Recognition,* Venture Beat, 2020 [https://venturebeat.com/2020/01/19/from-washington-state-to-washington-dc-lawmakers-rush-to-regulate-facial-recognition/?utm_medium=techboard.mon.20200120&utm_source=email&utm_content=&utm_campaign=campaign].

[43] K. Houser, *The "Biometric Mirror" Judges You the Way We've Taught it to: With Bias,* The Byte, 2018 [https://futurism.com/the-byte/biased-ai-biometric-mirror].

[44] Deepfake is a term for videos and presentations enhanced by AI and other modern technology to present falsified results. One of the best examples of deepfakes involves the use of image processing to produce video of celebrities, politicians or others saying or doing things that they never actually said or did. [https://www.techopedia.com/definition/33835/deepfake].

[45] N. Statt, *China Makes it a Criminal Offense to Publish Deepfakes or Fake News Without Disclosure,* The Verge, 2019 [https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality].

[46] D. Harwell, *Top AI Researchers Race to Detect 'Deepfake' Videos: 'We Are Outgunned',* The Washington Post, 2019 [https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/?tid=lk_inline_manual_2].

[47] T. Romm, D. Harwell, I. Stanley-Becker, *Facebook Bans Deepfakes, But New Policy May Not Cover Controversial Pelosi Video,* The Washington Post, 2020 [https://www.washingtonpost.com/technology/2020/01/06/facebook-ban-deepfakes-sources-say-new-policy-may-not-cover-controversial-pelosi-video/].

[48] T. Lau, U. Akkaraju, *When Algorithms Decide Whose Voices Will Be Heard,* Harvard Business Review, 2019 [https://hbr.org/2019/11/when-algorithms-decide-whose-voice-will-be-heard?utm_campaign=hbr&utm_source=linkedin&utm_medium=social].

Poorer countries face a novel set of challenges in regulating AI and other emerging technologies. Most of the standards and principles used in regulating AI are conceived and set by developed countries. This may result in suboptimal allocation of resources in less developed countries. For instance, the production of self-driving vehicles may require safety standards that make the cars too expensive for less developed countries' markets.

Connectivity and access to new technologies remain unattainable for many people living in less developed countries, who are unable to benefit from the opportunities offered by emerging technologies due to weak connectivity, high access costs to the digital economy, and low levels of human capital development.

Due to weaker governance and regulatory systems, poorer countries may not have the resources to protect themselves against hacking, deepfakes, algorithmic bias, invasion of privacy, and black boxes in the AI systems. Countries with weaker governance may also lack strong and well-informed institutions to protect against authoritarian abuse of AI devices, such as automated social score ranking systems and use of facial recognition technology. Moreover, the low "datafication" of developing countries' economies and the unavailability of big data might make it useless to deploy AI capabilities to analyze data. With non-existent or outdated legal systems, many poorer countries are also not up to the task of having efficient enforcement systems of cybercrime laws.

1.2 Regulatory principles in the Fourth Industrial Revolution era

1.2.1. Innovative and adaptive regulation

Traditional regulatory models are time consuming and robust. It takes months and sometimes years to draft new regulations in response to market developments and technology push. This needs to change. The modern regulatory models are innovative and collaborative. They rely on trial and error and co-design of regulation and standards, and have shorter feedback loops. Regulators can seek feedback using a number of "soft-law" innovative instruments such as policy labs, regulatory sandboxes, crowdsourcing, codes of conduct, best-practice guidance and self-regulation. Soft-law instruments accommodate changes in technology and business models, and allow regulators to address issues without stifling innovation.[49]

In Latin America, the absence of clear regulatory, policy and ethical frameworks in emerging technologies, and in AI in particular, has contributed to "experimentation without proper guidance" as observed by the Latin American Open Data Initiative (ILDA) in the paper "Automating with Caution".[50] It is important for policymakers in Latin America and all around the globe to become innovative and to deploy participative approaches in regulation of emerging technologies. Moreover, as many Latin American countries are considering privacy laws, following the example of the EU's GDPR, regulators should bear in mind that local jurisdictions face their own challenges and local circumstances, which need to be taken into account when discussing about how these types of regulation will be implemented in the Latin American context.[51]

Regulatory Sandboxes

A regulatory sandbox is a safe space for testing innovative products and services without having to comply with the applicable set of regulations. The main aim of regulators that establish

[49] W. D. Eggers, M. Turley, P. Kishnani, *The Future of Regulations,* Deloitte 2018 [https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html]; European Commission, *Ethical and Regulatory Challenges to Science and Research Policy at the Global Level,* European Commission, 2012 [https://publications.europa.eu/en/publication-detail/-/publication/84fc3de4-6641-4d9e-be58-9ca7da3d397b/language-en].

[50] F. Scrollini, *Automatizar Con Cautela: Datos e Inteligencia Artificial en America Latina,* ILDA, n.d. [https://idatosabiertos.org/automatizar-con-cautela-datos-e-inteligencia-artificial-en-america-latina/].

[51] H. Miller, R. Stirling, *Government Artificial Intelligence Readiness Index 2019,* Oxford Insights, 2019 [https://www.oxfordinsights.com/ai-readiness2019].

sandboxes is to foster innovation by lowering regulatory barriers and costs for testing disruptive innovative technologies, while ensuring that consumers will not be negatively affected. The concept of regulatory sandboxes, and any other form of collaborative prototyping environment, builds on the tradition of open source software development, the use of open standards and open innovation.[52]

Regulatory sandboxes are created by regulators around the globe. Examples are abundant. Japan introduced a regulatory sandbox in 2018 where foreign and domestic firms and organizations are able to demonstrate and experiment with new technologies such as blockchain, AI and IoT in financial services, healthcare and transportation. These sandbox experiments also take place in virtual spaces, rather than being limited geographical regions like Japan's National Strategic Special Zones. Sandboxes are a means through which new businesses are assessed, after which the government can introduce deregulation measures.[53]

An illustrative example of an innovative regulatory sandbox is Michigan's MCity, an autonomous transportation regulatory testbed where large-scale deployment would be dangerous but controlled experiments can provide useful insights for companies and regulators.[54]

Public agencies are also taking innovative approaches to regulating drones. For instance, the US is piloting a sandbox approach for drones. Beginning in 2017, the Unmanned Aircraft System (UAS) Integration Pilot Program has brought state, local, and tribal governments together with private sector entities, such as UAS operators or manufacturers, to accelerate safe drone integration. The Federal Aviation Administration has chosen 10 public-private partnerships to test drones. The pilot programs test the safe operation of drones in a variety of conditions which are currently forbidden, such as flying at night or beyond line of sight of operators, allowing companies to test applications including medical equipment delivery, monitoring oil pipelines, and scanning the perimeter of an airport.[55]

Singapore established a 5-year regulatory sandbox for self-driving cars in 2017, effectively turning the whole city-state into a test zone for the technology.[56] Also, the Government of Taiwan has created regulatory sandboxes for unmanned vehicles, vessels and drones in addition to its legislative efforts to harmonize drone regulations under the existing Civil Aviation Act. According to the Unmanned Vehicles Technology Innovation Experimentation Act, the Government of Taiwan will allow a period of up to four years for possible deregulation to encourage start-ups and enterprises to conduct innovative experiments related to technological development of unmanned vehicles, vessels and drones.[57]

The concept of regulatory sandboxes has also been criticized for the potential of creating market distortions and unfair competition by the possibility of regulators becoming too close with and protective of the regulatory sandbox participants.

Policy Labs

A policy lab is a group of actors that have various competencies in developing a regulatory framework. They deploy a set of user-centric methods and competencies to test, experiment and

[52] L. Wintermeyer, D. Markova, *A Development in Open Innovation Industy Sandbox Consultation Report,* Industry Sandbox, 2017 [https://www.innovatefinance.com/wp-content/uploads/2018/07/industry-sandbox-consultation-report.pdf].

[53] JapanGov, *Japan's Blockchain Sandbox is Paving the Way for the Fintech Future,* Forbes, 2019 [https://www.forbes.com/sites/japan/2019/06/26/japans-blockchain-sandbox-is-paving-the-way-for-the-fintech-future/#17539e103279].

[54] https://mcity.umich.edu/

[55] M. Meyers, W. D. Eggers, *What Government Can Learn From Venture Capital,* Deloitte, 2019 [https://www2.deloitte.com/us/en/insights/industry/public-sector/government-venture-capital.html]

[56] E. Yu, *Singapore Wants New Laws to Keep up With Autonomous, Ride-Sharing Vehicles,* ZD NET, 2017 [http://www.zdnet.com/article/singapore-wants-new-laws-to-keep-up-with-autonomous-ride-sharing-vehicles/].

[57] Shay & Partners, *New Drone Regulations to Come Into Force in 2020,* Lexology, 2019 [https://www.lexology.com/library/detail.aspx?g=c580b404-e2eb-4856-b250-9da5b49427b4].

learn to develop new policy solutions.[58]

In the US, some states and local government have already established policy labs in order to partner with academia and make use of their administrative data to evaluate and improve programs and policies, while safeguarding personal privacy. The policy labs provide technical infrastructure and governance mechanisms to help governments gain access to analytical talent, these data labs are helping to convert data into insights and driving more evidence-based policymaking and service delivery.[59]

1.2.2. Outcome-focused regulation

Outcome-focused regulation is a set of rules that prescribe achieving specific, desirable and measurable results, unlike traditional regulatory models that are prescriptive and input based.[60] This offers the private sector greater flexibility in choosing its way of complying with the law.

Outcome-focused regulations stipulate positive outcomes that regulators want to encourage. For instance drone regulation can be prescriptive and focus on inputs: “One must have a license to fly a drone with more than xx kilowatts of power (not very helpful)”, or it can be outcome-based and focus on effects: “One cannot fly a drone higher than 400 feet, or anywhere in a controlled airspace (better)”.[61]

The real benefits of emerging technologies lie in their ability to interconnect and converge. For instance, blockchains can be used to secure data generated through IoT enabled devices, or machine learning models can be used to amplify the abilities of human bankers. Innovators need enough space to innovate for such interconnections to happen, and outcome-focused regulation can provide this.[62]

Fostering iterative regulatory approaches

It is important that regulators deploy iterative regulatory approaches by revisiting existing rules and ensuring the regulations remain agile and adaptable to changing technologies.

For instance, Singapore has adopted progressive regulations for the testing of self-driving vehicles, due to its high population density and limited space to expand. In 2017, Singapore modified its road traffic law to accommodate “automated vehicles’ technologies and their disruptive character. In order to ensure that regulations remain agile the rules will remain in effect for five years, and the government has the option to revise them sooner. The autonomous vehicles testing falls under the purview of a single agency, the Land Transport Authority, thus eliminating the possibility of patchy oversight and different agencies and rules regulating the automated vehicles field. The authority actively partners with research institutions and the private sector to facilitate pilots of autonomous vehicles.[63]

On the other hand, many developing countries are lagging behind in fostering innovative, iterative and outcome-focused regulation of emerging technologies. For instance, autonomous vehicles adoption in Mexico currently faces a range of barriers, with a lack of specific regulations,

[58] https://www.vinnova.se/en/m/Smart-policy-development/what-is-a-policy-lab/

[59] A. Feldman, S. Goldsmith, *Why Every Mayor Should Consider Launching a Policy Lab,* Governing, 2017 [http://www.governing.com/commentary/col-why-every-mayor-should-consider-launching-policy-lab.html].

[60] https://www.inspection.gc.ca/about-the-cfia/acts-and-regulations/safe-and-responsive-regulatory-framework/outcome-based-regulations/eng/1545927831816/1545927832066

[61] W. D. Eggers, M. Turley, P. Kishnani, *The Future of Regulation,* Deloitte, 2018 [https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html].

[62] Ibid

[63] D. M. Pankratz, K. Nuttall, W. D. Eggers, M. Turley, *Regulating the Future of Mobility,* Deloitte, 2018 [https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/regulating-transportation-new-mobility-ecosystem.html].

no active tests and little industrial activity.[64]

1.2.3. Evidence-based regulation

Evidence-based regulation is a modern regulatory model that is data-driven and risk-based. It is a dynamic and based on real-time data flows between the private sector and regulators. The data could then be compared with regulations to decide whether a firm is in compliance. Firms in compliance would be listed as *safe,* and if not, the data systems could produce a set of action items to meet the standard.

The first capital city in the world to regulate ridesharing was Canberra in Australia. Before the service had begun, and Uber signaling its intention to enter the local market prompted the local government to take a systematic and evidence-based approach in reforming the ridesharing sector. The ridesharing business model differs from the traditional taxi industry in terms of risk. The additional information that is available to both drivers and passengers through the booking service, such as rank and hail work by taxis, significantly reduces the risk involved with anonymous transactions. Additionally, a reputation rating system provides an incentive for drivers and customers alike to behave respectfully. By integrating of a booking system and payments, payment risks such as cash handling and non-payment have been minimized. The City of Canberra designed a new regulatory framework that is adaptable to new technologies by taking into account the approach to risk from different business models. It further anticipated the emergence of novel business models, such as fleets of automated vehicles providing on-demand transport. The designed system does not regulate individual business, but it provides a regulatory framework and promotes fair treatment of different business models, thus making the framework more flexible.[65] The Government formally monitors the outcomes of the new regulatory framework through the collection of qualitative and quantitative data on industry changes, including customer outcomes and impacts on various stakeholders. This data is used by an ACT to analyze changes in supply and demand and in the quality of services delivered to consumers. This evaluation is intended to be used to see if the industry is experiencing change that is in line with the modelled forecasts and to determine whether further actions are required.[66]

Open data has also been used by regulators to complement their own data. A regulator in the case of digital health software could monitor products through publicly available data on software bugs and error reports, customer feedback, software updates, app store information, and social media.

Once the data flows are integrated, this part of the regulatory process can be automated. Enforcement can become dynamic and reviewing and monitoring can be built into the system. For example, the City of Boston which inspects every restaurant in order to monitor and improve food safety and public health. These health inspections are usually random, which can increase time spent at restaurants that have been following the rules carefully, thus missing opportunities to improve health and hygiene in restaurants with food safety issues. In Boston, the search for health code violations is narrowed down through the use of a winning algorithm which uses data generated from social media. These algorithms detect words, phrases, ratings and patterns that allows them to predict violations, thus helping public health inspectors execute their working duties better and more efficiently. This algorithm could allow the City of Boston to catch the same number of health violations with 40 percent fewer inspections, by simply better targeting city resources at dirty-kitchen hotspots. As of 2017, these winning algorithms have been employed by the City of Boston and have found 25 percent more health violations, as well as surfacing around

[64] KPMG International, Autonomous Vehicles Readiness Index: Assessing Countries' Openness And Preparedness For Autonomous Vehicles 35 (Jan. 2018), [https://home.kpmg.com/content/dam/kpmg/co/images/2018/01/GM-TL-Carros%20aut%C3%B3nomos.pdf]; *archived at* [https://perma.cc/Q3RD-SZH4].

[65] *Guiding Principles for Responding to and Enabling Innovation,* 2017 [https://www.industry.gov.au/sites/default/files/2019-03/coag_industry_and_skills_council_guiding_principles_for_responding_to_and_enabling_innovation.pdf].

[66] ABC Radio Canberra, *Uber Launches in ACT as Canberra Becomes First City to Regulate Ride Sharing,* ABC News, 2015 [https://www.abc.net.au/news/2015-10-30/uber-launches-in-canberra/6898514].

60 percent of critical violations earlier than before. The city has been able to catch public health risks sooner and to get a smarter view of how to utilize scarce public resources by taking advantage of past data and combining it with new sources of information.[67]

Moving to a "cloud computing model of regulation" in which scalability is built into the regulatory model could be the way forward. For instance, if a company's product or service is targeting only a handful of uses, it might receive fewer checks as its potential adverse impacts could be limited. Only after that company has grown would it be faced with a more thorough investigation.[68]

A Pre-Cert pilot program for digital health developers that demonstrate a culture of quality and organizational excellence based on objective criteria (e.g. software design, development, and testing) has been created by the US Food and Drug Administration. This Program has been envisioned as a voluntary pathway embodying a regulatory model that is tailor-made assessing the safety and effectiveness of software technologies without inhibiting patient access to these technologies.[69] This is in stark contrast to the current regulatory paradigm. Because software as a medical device allows for product to be adaptable and can respond to glitches, adverse events, and other safety concerns quickly, the FDA has been working to establish a regulatory framework that will be equally responsive when issues arise in order to help consumers continue to have access to safe and effective products. The idea behind this is to allow the FDA to accelerate time to market for lower-risk health products and focus its resources on those posing greater potential risks to patients. This will allow pre-certified developers to market lower-risk devices without an additional FDA review, or with a simpler market review, as the FDA monitors the performance of these companies continuously, with real-world data.[70]

1.2.4. Collaborative regulation

This *ecosystem approach*—when multiple regulators from different nations collaborate with one other and with those being regulated—can encourage innovation while protecting consumers from potential fraud or safety concerns. Private, standard-setting bodies and self-regulatory organizations also play key roles in facilitating collaboration between innovators and regulators.

One way forward is being developed by the Asia-Pacific Economic Cooperation (APEC) forum through Cross-Border Privacy Rules (CBPR) system, serving as a mechanism that fosters trust and facilitates data flows amongst participants. A key benefit of the APEC regime is that it enables personal data to flow freely even in the absence of two governments having agreed to formally recognize each other's privacy laws as equivalent. Instead, APEC relies on businesses to ensure that data collected and then sent to third parties either domestically or overseas continues to protect the data consistent with APEC privacy principles. The APEC CBPR regime also requires independent entities who can monitor and hold businesses accountable for privacy breaches.[71]

The U.S.-EU Privacy Shield is another example of how interoperability between the EU approach to privacy and the U.S. accountability-approach might be achieved. In this regard, Privacy Shield avoids countries (in this case the U.S.) having to adopt a top-down privacy regime akin to the EU's GDPR. Instead, Privacy Shield allows a subset of businesses in a given country

[67] https://www.drivendata.org/competitions/5/keeping-it-fresh-predict-restaurant-inspections/

[68] . D. Eggers, M. Turley, P. Kishnani, *The Future of Regulations,* Deloitte 2018 [https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html];

[69] US FDA, *Digital Health Software Precertification (Pre-Cert) Program,* FDA 2018 [https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program]

[70] W. D. Eggers, M. Turley, P. Kishnani, *The Future of Regulations,* Deloitte 2018 [https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html].

[71] J. P. Meltzer, P. Lovecock, *Regulating For a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia,* Brookings, 2018 [https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/].

to agree to a particular privacy regime in order to be deemed equivalent by the EU. This enables the free flow of personal data between the EU and the business participating in Privacy Shield.[72]

For those countries party to the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), the commitments on privacy in the e-commerce chapter provide another framework for integrating privacy, trade, and cross-border data flows.[73]

References

[1] K. Schwab, *The Fourth Industrial Revolution: What it Means, How to Respond,* World Economic Forum, 2016 [https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/].

[2] K. Schwab, *The Fourth Industrial Revolution: What it Means, How to Respond,* World Economic Forum, 2016 [https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/].

[3] J. Chappelow, *Sharing Economy,* Investopedia, 2019 [https://www.investopedia.com/terms/s/sharing-economy.asp].

[4] Y. Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation,* Harvard Journal of Law & Technology, Volume 31, Number 2 Spring 2018 [https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf].

[5] N. Al-Rodhan, *Security, Ethics and Emerging Technologies,*World Economic Forum, 2014 [https://www.weforum.org/agenda/2014/03/security-ethics-emerging-technologies/].

[6] Agence France-Presse, *Airbnb: The First 10 Years- Start-Up to Unicorn to US$30 Billion Business,* South China Morning Post, 2018 [https://www.scmp.com/lifestyle/travel-leisure/article/2153851/how-airbnb-founders-went-cash-strapped-roommates].

[7] H. Miller, R. Stirling, *Government Artificial Intelligence Readiness Index 2019,* Oxford Insights, 2019 [https://www.oxfordinsights.com/ai-readiness2019].

[8] Bnamericas, *National AI Policies Popping Up Across South America,* Bnamericas, 2019 [https://www.bnamericas.com/en/news/national-ai-policies-popping-up-across-south-america--marketing-or-strategy].

[9] J. Porter, *Airbnb Avoids Tougher Regulation in Europe as EU Court Rules it's not an Estate Agent,* The Verge, 2019 [https://www.theverge.com/2019/12/19/21029606/airbnb-estate-agent-eu-ruling-platform-regulation].

[10] J. Villasenor, *Products Liability law as a Way to Address AI Harms,* Brookings, 2019 [https://www.brookings.edu/research/products-liability-law-as-a-way-to-address-ai-harms/];

[11] P. Opitz, *Civil Liability and Autonomous Robotic Machines: Approaches in the EU and US,* TTLF Working Papers No.43, 2019 [https://law.stanford.edu/wp-content/uploads/2019/02/opitz_wp43.pdf].

[72] Ibid

[73] Ibid

[12] European Commission, *Liability for Artificial Intelligence and Other Emerging Digital Technologies,* European Commission, 2019 [https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199].

[13] K. Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human,* WIRED, 2016 [https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/].

[14] S. Barua, *'Flood of Data Will Get Generated in Autonomous Cars',* Auto Tech Review, n.d. [https://autotechreview.com/features/flood-of-data-will-get-generated-in-autonomous-cars].

[15] L. Matsakis, *The WIRED Guide to Your Personal Data (and Who is Using it),* WIRED, 2018 [https://www.wired.com/story/wired-guide-personal-data-collection/

[16] J. Baron, *Life Insurers Can Use Social Media Posts to Determine Premiums, as Long as They Don't Discriminate,* Forbes, 2019 [https://www.forbes.com/sites/jessicabaron/2019/02/04/life-insurers-can-use-social-media-posts-to-determine-premiums/#42002dc823ce].

[17] T. Lau, U. Akkaraju, *When Algorithms Decide Whose Voices Will Be Heard,* Harvard Business Review, 2019 [https://hbr.org/2019/11/when-algorithms-decide-whose-voice-will-be-heard?utm_campaign=hbr&utm_source=linkedin&utm_medium=social].

[18] C. F. Kerry, J. B. Morris, *Why Data Ownership is the Wrong Approach to Protecting Privacy,* Brookings, 2019 [https://www.brookings.edu/blog/techtank/2019/06/26/why-data-ownership-is-the-wrong-approach-to-protecting-privacy/].

[19] European Commission, *Data Protection Rules as a Trust-Enabler in the EU and Beyond – Taking Stock,* Brussels, COM(2019) 374 Final, 2019 [https://ec.europa.eu/info/law/law-topic/data-protection_en].

[20] European Parliament, *Charter of Fundamental Rights of the European Union,* Official Journal of the European Communities (2000/C 364/01), 2000 [https://www.europarl.europa.eu/charter/pdf/text_en.pdf].

[21] L. Rocher, J. M. Hendrickx, Y-A. De Montjoye, *Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models,* Nature Communications, 2019 [https://nature.com/articles/s41467-019-10933-3].

[22] C. Jee, *You're Very Easy to Track Down, Even When Your Data Has Been Anaonymized,* MIT Technology Review, 2019 [https://www.technologyreview.com/s/613996/youre-very-easy-to-track-down-even-when-your-data-has-been-anonymized].

[23] M. D. Fenwick, W. A. Kaal, E. P. M. Vermeulen, *Regulation Tomorrow: What Happens When Technology Is Faster Than The Law?,* American University Business Law Review, Volume 6, Issue 3, 2017 [https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1028&context=aublr].

[24] M. Stankovic, R. Gupta, B. A. Rossert, G. I. Myers, M. Nicoli, *White Paper Exploring Legal, Ethical and Policy Implications of Artificial Intelligence,* Law, Justice and Development, 2017 [http://globalforumljd.com/new/sites/default/files/documents/resources/Artificial-Intelligence-White-Paper-Draft-5Oct2017.pdf].

[25] R. Richardson, J. M. Schultz, V. M. Southerland, *Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems,* AI Now Institute,

2019 [https://ainowinstitute.org/litigatingalgorithms-2019-us.html]; T. Simonite, *AI Experts Want to End 'Black Box' Algorithms in Government,* WIRED, 2017 [https://www.wired.com/story/ai-experts-want-to-end-black-box-algorithms-in-government/].

[26] Local Law in Relation To Automate Decision Systems Used by Agencies of 2018 [https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0&Options=&Search].

[27] B. Kelly, Y. Chae, *INSIGHT: AI Regulations Aim at Eliminating Bias,* Bloomberg Law, 2019 [https://news.bloomberglaw.com/tech-and-telecom-law/insight-ai-regulations-aim-at-eliminating-bias].

[28] K. Hosanagar, V. Jair, *We Need Transparency in Algorithms, But Too Much Can Backfire,* Harvard Business Review, 2018 [https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire].

[29] S. Chandler, *The AI Chatbot Will Hire You Now,* WIRED, 2017 [https://www.wired.com/story/the-ai-chatbot-will-hire-you-now/].

[30] Tech Policy, *The AI Hiring Industry is Under Scrutiny – But it'll be Hard to Fix,* MIT Technology Review, 2019 [https://www.technologyreview.com/f/614694/hirevue-ai-automated-hiring-discrimination-ftc-epic-bias/].

[31] Public Act 101-0260, 2020 [http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101-0260].

[32] R. Heilweil, *Illinois Says You Should Know if AI is Grading Your Online Job Interviews,* VOX, 2020 [https://www.vox.com/recode/2020/1/1/21043000/artificial-intelligence-job-applications-illinios-video-interivew-act].

[33] J. Angwin, J. Larson, S. Mattu, L. Kirchner, *Machine Bias,* ProP [https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing].

[34] J. Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women,* Reuters 2018 [https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G].

[35] R. Metz, *Beyond San Francisco, More Cities are Saying no to Facial Recognition,* CNN Business, 2019 [https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html].

[36] J. Porter, *Surprising Results After Activists Test Facial Recognition Technology on Denver City Council,* The Denver Channel, 2020 [https://www.thedenverchannel.com/news/local-news/surprising-results-after-activists-test-facial-recognition-technology-on-denver-city-council].

[37] K. Johnson, *From Washington State to Washington, D.C., Lawmakers Rush to Regulate Facial Recognition,* Venture Beat, 2020 [https://venturebeat.com/2020/01/19/from-washington-state-to-washington-dc-lawmakers-rush-to-regulate-facial-recognition/?utm_medium=techboard.mon.20200120&utm_source=email&utm_content=&utm_campaign=campaign].

[38] K. Houser, *The "Biometric Mirror" Judges You the Way We've Taught it to: With Bias,* The Byte, 2018 [https://futurism.com/the-byte/biased-ai-biometric-mirror].

[39] N. Statt, *China Makes it a Criminal Offense to Publish Deepfakes or Fake News Without Disclosure,* The Verge, 2019 [https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality].

[40] D. Harwell, *Top AI Researchers Race to Detect 'Deepfake' Videos: 'We Are Outgunned',* The Washington Post, 2019 [https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/?tid=lk_inline_manual_2].

[41] T. Romm, D. Harwell, I. Stanley-Becker, *Facebook Bans Deepfakes, But New Policy May Not Cover Controversial Pelosi Video,* The Washington Post, 2020 [https://www.washingtonpost.com/technology/2020/01/06/facebook-ban-deepfakes-sources-say-new-policy-may-not-cover-controversial-pelosi-video/].

[42] T. Lau, U. Akkaraju, *When Algorithms Decide Whose Voices Will Be Heard,* Harvard Business Review, 2019 [https://hbr.org/2019/11/when-algorithms-decide-whose-voice-will-be-heard?utm_campaign=hbr&utm_source=linkedin&utm_medium=social].

[43] W. D. Eggers, M. Turley, P. Kishnani, *The Future of Regulations,* Deloitte 2018 [https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html];

[44] European Commission, *Ethical and Regulatory Challenges to Science and Research Policy at the Global Level,* European Commission, 2012 [https://publications.europa.eu/en/publication-detail/-/publication/84fc3de4-6641-4d9e-be58-9ca7da3d397b/language-en].

[45] F. Scrollini, *Automatizar Con Cautela: Datos e Inteligencia Artificial en America Latina,* ILDA, n.d. [https://idatosabiertos.org/automatizar-con-cautela-datos-e-inteligencia-artificial-en-america-latina/].

[46] H. Miller, R. Stirling, *Government Artificial Intelligence Readiness Index 2019,* Oxford Insights, 2019 [https://www.oxfordinsights.com/ai-readiness2019].

[47] L. Wintermeyer, D. Markova, *A Development in Open Innovation Industy Sandbox Consultation Report,* Industry Sandbox, 2017 [https://www.innovatefinance.com/wp-content/uploads/2018/07/industry-sandbox-consultation-report.pdf].

[48] JapanGov, *Japan's Blockchain Sandbox is Paving the Way for the Fintech Future,* Forbes, 2019 [https://www.forbes.com/sites/japan/2019/06/26/japans-blockchain-sandbox-is-paving-the-way-for-the-fintech-future/#17539e103279].

[49] M. Meyers, W. D. Eggers, *What Government Can Learn From Venture Capital,* Deloitte, 2019 [https://www2.deloitte.com/us/en/insights/industry/public-sector/government-venture-capital.html]

[50] E. Yu, *Singapore Wants New Laws to Keep up With Autonomous, Ride-Sharing Vehicles,* ZD NET, 2017 [http://www.zdnet.com/article/singapore-wants-new-laws-to-keep-up-with-autonomous-ride-sharing-vehicles/].

[51] Shay & Partners, *New Drone Regulations to Come Into Force in 2020,* Lexology, 2019 [https://www.lexology.com/library/detail.aspx?g=c580b404-e2eb-4856-b250-9da5b49427b4].

[52] A. Feldman, S. Goldsmith, *Why Every Mayor Should Consider Launching a Policy Lab,* Governing, 2017 [http://www.governing.com/commentary/col-why-every-mayor-should-consider-launching-policy-lab.html].

[53] D. M. Pankratz, K. Nuttall, W. D. Eggers, M. Turley, *Regulating the Future of Mobility,* Deloitte, 2018 [https://www2.deloitte.com/us/en/insights/focus/future-of-mobility/regulating-transportation-new-mobility-ecosystem.html].

[54] KPMG International, Autonomous Vehicles Readiness Index: Assessing Countries' Openness and Preparedness for Autonomous Vehicles 35 (Jan. 2018), [https://home.kpmg.com/content/dam/kpmg/co/images/2018/01/GM-TL-Carros%20aut%C3%B3nomos.pdf]; *archived at* [https://perma.cc/Q3RD-SZH4].

[55] *Guiding Principles for Responding to and Enabling Innovation,* 2017 [https://www.industry.gov.au/sites/default/files/2019-03/coag_industry_and_skills_council_guiding_principles_for_responding_to_and_enabling_innovation.pdf].

[56] ABC Radio Canberra, *Uber Launches in ACT as Canberra Becomes First City to Regulate Ride Sharing,* ABC News, 2015 [https://www.abc.net.au/news/2015-10-30/uber-launches-in-canberra/6898514].

[57] US FDA, *Digital Health Software Precertification (Pre-Cert) Program,* FDA 2018 [https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program]

[58] J. P. Meltzer, P. Lovecock, *Regulating For a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia,* Brookings, 2018 [https://www.brookings.edu/research/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/].

[59] http://www.airbnb.com/.

[60] https://www.uber.com/.

[61] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/my-rights/what-are-my-rights_en

[62] https://mcity.umich.edu/

[63] https://www.drivendata.org/competitions/5/keeping-it-fresh-predict-restaurant-inspections/

[64] https://www.vinnova.se/en/m/Smart-policy-development/what-is-a-policy-lab/

[65] https://www.inspection.gc.ca/about-the-cfia/acts-and-regulations/safe-and-responsive-regulatory-framework/outcome-based-regulations/eng/1545927831816/1545927832066

[66] https://www.techopedia.com/definition/33835/deepfake