



Regulation

Stephen Downes

December 17, 2021

Scope of Regulation

- Ethical governance: focusing on the most pertinent ethical issues raised by AI such as fairness, transparency and privacy
- Explainability and interpretability: for example, the idea of a 'right to explanation' of algorithmic decisions
- Ethical auditing: mechanisms that examine the inputs and outputs of algorithms for bias and harms

Corrinne Cath, 2018, <https://royalsocietypublishing.org/doi/pdf/10.1098/rsta.2018.0080>

Map: https://docs.google.com/spreadsheets/d/1utA1ug1nKF3B4MMmC_AQeyo1IK5jH_abMK9oFHEJekk/edit#gid=0

Cover image: <https://www.bloomberg.com/news/articles/2021-11-19/crypto-industry-s-solution-to-regulation-is-self-regulation>

Explainability Revisited

The ICO and The Alan Turing Institute identify six main varieties:

- Rationale: reasons behind a decision.
- Responsibility: who made the AI system and how to obtain a human review
- Data: What data went into the model and how was data used
- Fairness: how we know the AI is unbiased and individuals are treated equitably.
- Safety and performance: How are accuracy, reliability, security and robustness ensured
- Impact explanation: how are effects and decisions monitored

<https://www.arnoldporter.com/-/media/files/perspectives/publications/2021/06/ai-regulationstaying-ahead-of-curveschildkraut0621.pdf?la=en>

Europe: The AI Act

- Definition of AI, place of market
- Risk-based approach: some AI practices are banned (Title II)
 - Bans tech that's subliminal, exploits vulnerabilities, social score, real-time biometrics (subject to conditions)
- Regulated compliance of high-risk AI with existing rights
- Potentially risk AI must bear a CE mark of product compliance

European Commission finally presented its Proposal for a Regulation laying down harmonised rules on artificial intelligence <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

Summary: <https://www.lexology.com/library/detail.aspx?g=e6c7bcfe-7df3-4bd4-afd7-a2430d64de33>

Also: <https://www.fieldfisher.com/en/insights/the-eu-ai-regulation-part-1>

Facial Recognition Bans

- Bans in Massachusetts, Maine, Minneapolis
- Amazon, IBM and Microsoft will stop selling the tech
- But still, investor cash is rolling in



<https://www.banfacialrecognition.com/>

<https://techcrunch.com/2021/07/26/facial-recognition-flush-with-cash/>

United States: NIST Plan

“American AI Initiative,” guided by five principles:

- Driving technological breakthroughs;
- Driving the development of appropriate technical standards;
- Training workers with the skills to develop and apply AI technologies;
- Protecting American values, including civil liberties and privacy, and fostering public trust and confidence in AI technologies; and
- Protecting U.S. technological advantage in AI, while promoting an international environment that supports innovation.

<https://www.bakermckenzie.com/-/media/files/people/chae-yoon/rail-us-ai-regulation-guide.pdf>

https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

Canada: Regulatory Framework

- Canadian Privacy Commissioner: an appropriate law for AI would:
 - Allow personal information to be used for new purposes
 - Authorize these uses within a rights based framework
 - Create provisions specific to automated decision-making
 - Require businesses to demonstrate accountability

AI+Society Initiative <https://techlaw.uottawa.ca/aisociety/regulation>

A Regulatory Framework for AI: Recommendations for PIPEDA Reform
https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/

The Future of AI Regulation in Canada <https://www.torys.com/our-latest-thinking/publications/2021/05/the-future-of-ai-regulation-in-canada>



China: Social Impact

Major initiatives:

- Draft guidelines on recommender systems (including the right to turn them off), requirement for user consent for use of personal data
- Overall limits on tech and AI companies “that would prevent platforms from violating user privacy, encouraging users to spend money, and promoting addictive behaviors”
- Strong anti-trust, anti-monopoly laws, liability for abusing a dominant market position by discriminatory pricing, concern about working conditions

<https://venturebeat.com/2021/10/03/what-we-can-learn-from-chinas-proposed-ai-regulations/>

<https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/china>

<https://montrealetics.ai/the-chinese-approach-to-ai-an-analysis-of-policy-ethics-and-regulation/>

Global Privacy Agency: Accountability

- Assess the potential impact to human rights
- Test the robustness, reliability, accuracy and data security
- Keep records of impact, design, development, testing and use
- Disclose data protection, privacy and rights impact assessment
- Disclosing the use, the data, and the logic involved in the AI
- Ensure an accountable human actor is identified
 - And seven more

<https://globalprivacyassembly.org/wp-content/uploads/2020/10/FINAL-GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf>

Other Regulatory Areas

- Data regulation
 - Data rights – customers and suppliers need to clearly define data use rights
 - the GDPR and more
- Intellectual property
 - Defining ‘authorship’ of AI-generated content
- Civil wrongs (torts)
 - Manufacturing and design defects
 - Failure to warn of risks

Goodhart's Law

- the idea that any metric ceases to be a valid metric the moment it becomes a target for optimization (and gets “metric-hacked”)
- E.g. bounty on cobras
 - Works well at first
 - But people begin raising cobras
 - These are eventually released



https://en.wikipedia.org/wiki/Goodhart%27s_law

<https://www.holistics.io/blog/four-types-goodharts-law/>

Image: <https://danikalaw.com/attribution-and-goodharts-law/>

Regulatory Lag and Regulatory Markets

- Given the pace of AI progress, laws will often be outdated by the time they're passed.
- “Regulatory markets for AI” — a system whereby governments set safety metrics (e.g. “fewer than X collisions caused by self-driving cars per Y miles driven”) and drive whole sectors of the economy to compete on those targets.

Recognizing Our Limitations

- People don't understand AI
 - Especially octogenarian legislators
 - Though social science has done a lot to expose the risks
- There's a need for a constant dialogue

<https://www.tandfonline.com/doi/full/10.1080/13669877.2021.1957985>