ICP Developer Community
Decentralized AI Working Group

August 15th, 2024

Introductory Briefing on
AI Law, Regulation, Compliance

Recap of AI Milestones

- 1958, New York Times publishes a story about an experimental "thinking machine" called a Perceptron - an early neural network and the, *"first device to think as the human brain … Perceptron will make mistakes at first, but will grow wiser as it gains experience."*
- 1969, Marvin Minsky and Seymour Papert published a book called Perceptrons that summarily dismissed the neural networks' potential to succeed at complex tasks and for more than a decade, interest and funding favoured symbolic logic approaches.
- 1997, IBM's Deep Blue - first computer chess-playing system to beat a reigning world chess champion, Garry Kasparov, under regular chess match conditions
- 2004, NASA Mars rovers Spirit and Opportunity equipped with AI to navigate rocky terrain.
- 2011, IBM Watson DeepQA designed to receive natural language questions and respond accordingly, beat two of US *Jeopardy* quiz show's most formidable champions, Ken Jennings and Brad Rutter.
- 2012, Geoffrey Hinton (studying neural networks since 1970s), and his two grad students; Alex Krizhevsky and Ilya Sutskever, present groundbreaking visual-recognition network AlexNet to win the ImageNet competition.

Recap of AI Milestones

- 2011 – 2016, Siri and Alexa and natural language processing capabilities that understand spoken question and respond with an answer - programmed to understand a lengthy list of questions and not answer what falls outside their purview.
- 2016, Hanson Robotics create Sophia, a “human-like robot” capable of facial expressions, jokes, and conversation - Saudi Arabia granted Sophia citizenship in 2017, making her the first artificially intelligent being to be given that right. (*criticized as Sophia thereby granted rights which Saudi women were then still denied*)
- 2016, DeepMind’s AlphaGO goes on to beat Lee Sedol, one of the best Go players in the world.
- 2020, GPT-3 – a 175 billion parameter large language model (LLM) able to generate computer code, poetry, and prose - *reviewed by Farhad Manjoo in The New York Times, GPT-3 was described as "amazing", "spooky", "humbling“ and "more than a little terrifying.*

What kind of Law and Regulation is, *"AI Law and Regulation"*

The world encompasses diverse cultures, moral epistemologies and ethical traditions – with different traditions of justice, jurisprudence, legal orders and regulation. Areas international law developing out of prominent common interests:

Law of the sea (protecting the international seabed), cultural heritage (protection of monuments), development law (sustainable development), climate change law (protecting biological diversity, reducing emission of greenhouse gases, and counteracting man-made influence on climate change), human rights law (safeguarding human dignity), international criminal law (ending impunity for genocide), and nonproliferation law (stopping nuclear proliferation).

- Artificial Intelligence law and regulation will inevitably span sectors and jurisdictions and draw on a established categories of law and regulation:
    - Data security, privacy, access, sharing processing, transfers etc. …
    - Intellectual property, copyright …
    - Human rights law, National Constitutions and Charters …
    - Jus cogens (Latin phrase meaning "compelling law.")
      designates peremptory norms from which no particular agreements may derogate.

Some early legal and regulatory foundations

- 1948 Universal Declaration of Human Rights is an international document adopted by the United Nations General Assembly and enshrines the rights and freedoms of all human beings.
    - Although not legally binding, the contents of the UDHR have been elaborated and incorporated into subsequent international treaties, regional human rights instruments, and national constitutions and legal codes.
- International Bill of Human Rights, completed in 1966; came into force in 1976, Comprised of Universal Declaration of Human Rights (adopted in 1948), the International Covenant on Civil and Political Rights (ICCPR, 1966) with its two Optional Protocols and the International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966).
- 1967 Outer Space Treaty, formally the “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies”.
- Coming into force in 1994, the United Nations Convention on the Law of the Sea – replaced the older "freedom of the seas" concept, dating from the 17th century wherein national rights were limited to a specified belt of water extending from a nation's coastlines.

Some early legal and regulatory foundations

- In 2003 the World Summit on the Information Society (WSIS) – convened by the International Telecommunication Union, a specialized agency of the United Nations proclaimed in their "Geneva Declaration":
  - 42. *Intellectual Property protection is important to encourage innovation and creativity in the Information Society; similarly, the wide dissemination, diffusion, and sharing of knowledge is important to encourage innovation and creativity. Facilitating meaningful participation by all in intellectual property issues and knowledge sharing through full awareness and capacity building is a fundamental part of an inclusive Information Society.*
  - *52. Cultural diversity is the* ***common heritage of humankind****. The Information Society should be founded on and stimulate respect for cultural identity, cultural and linguistic diversity, traditions and religions, and foster dialogue among cultures and civilizations. The promotion, affirmation and preservation of diverse cultural identities and languages as reflected in relevant agreed United Nations documents including UNESCO's Universal Declaration on Cultural Diversity, will further enrich the Information Society.*
- UN Convention on the Law of the Sea and Outer Space Treaty both make provision for fair and equitable access and benefit-sharing in areas beyond national jurisdiction, or the so-called "global commons".
- Likely helpful parallels with international biomedical law - such as apply to the information of the human genome and related genetic manipulations.
  - International biomedical law instruments claim to adopt a human rights-based approach to the regulation of biology and medicine – therefore to maximize the benefits for the affected individuals and to minimize any possible harm, giving due regard to the impact of life sciences on the rights of future generations.

Some early legal and regulatory foundations

- Just for food for thought before we look at the present progress of AI law and regulation:

PRINCIPLES TO GUIDE THE GOVERNANCE OF HUMAN GENOME EDITING [1]:

- Promoting well-being
- Transparency
- Due care
- Responsible science
- Respect for persons
- Fairness
- Transnational cooperation

1. National Academies of Sciences, Engineering, and Medicine. 2017. Human Genome Editing: Science, Ethics, and Governance. Washington, DC: The National Academies Press. doi: https://doi.org/10.17226/24623.

Some early legal and regulatory foundations

To inform how decisions are made:

- Openness, transparency, honesty, accountability
- Responsible regulatory stewardship
- Responsible stewardship of science
- Responsible stewardship of research resources

To inform what decisions are made:

- Inclusiveness
- Caution
- Fairness
- Social justice
- Non-discrimination
- Equal moral worth
- Respect for persons
- Solidarity
- Global health justice

WHO Expert Advisory Committee on Developing Global Standards for Governance and Oversight of Human Genome

Some early legal and regulatory foundations

Special challenges:

- postnatal somatic human genome editing
- prenatal (in utero) somatic human genome editing
- enhancement

For AI, add "posthumous applications"?

Some early legal and regulatory foundations

Tools, institutions and processes for governance (of human genome editing):

- Declarations, treaties, conventions, legislation and regulations
- Judicial rulings
- Ministerial decrees
- Conditions on research funding
- Moratoria
- Accreditation, registration or licensing
- National science and medicine societies and institutions
- Patents and licenses
- Professional self-regulation
- Public advocacy and activism
- Research ethics guidelines and research ethics review
- Collaboration with publishers and conference organizers
- Education and training of researchers and clinicians

Emergence of Artificial Intelligence, Specific Law and Regulation

In the early days of AI law and regulation came “National Strategies” (on AI) and International Agreements

- In 2017, Canada was the first country to establish a national AI strategy - The Pan-Canadian Artificial Intelligence Strategy.

2021 Analysis of UK Artificial Intelligence law:

“AI is currently regulated through a complex patchwork of legal and regulatory requirements. Analysis identified at least 18 key legal frameworks that indirectly control the development and use of AI in the UK. Consequently, there is no regulator or supervisory authority solely responsible for overseeing the use, development or effects of AI. Instead, AI is regulated indirectly by different frameworks and their associated regulators”

Emergence of Artificial Intelligence, Specific Law and Regulation

Jan. 2023 – China introduces regulation on administration of deep synthesis of the internet China introduces regulations aimed at “deep synthesis” technology to tackle security issues related to the creation of realistic virtual entities and multimodal media, including “deepfakes.” These regulations apply to both providers and users across different media and mandate measures, such as preventing illegal content, adhering to legal compliance, verifying user identities, securing consent for biometric editing, safeguarding data security, and enforcing content moderation.

Aug. 2023 “China updates cyberspace administration of generative AI measures China’s updated policy adopts a more targeted regulatory approach, focusing on applications with public implications rather than a blanket regulation. The amendments soften the regulatory language, changing directives like “ensure the truth, accuracy, objectivity, and diversity of the data” to “employ effective measures to enhance the quality of training data and improve its truth, accuracy, objectivity, and diversity. Encouraging generative AI development, shifting away from the prior punitive focus.”

June 2023 U.S. policymakers propose National AI Commission Act - calls for establishing a National AI Commission tasked with crafting a comprehensive AI regulatory framework.

Emergence of Artificial Intelligence, Specific Law and Regulation

October 2023

Biden's **Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**

- Require that developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government.
- Develop standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy
- Protect against the risks of using AI to engineer dangerous biological materials
- Protect Americans from AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content
- Establish advanced cybersecurity program to develop AI tools to find and fix vulnerabilities in critical software.
- Order the development of a National Security Memorandum that directs further actions on AI and security
- Protecting Americans' Privacy
- Advancing Equity and Civil Rights
- Standing Up for Consumers, Patients, and Students
- Supporting Workers
- Promoting Innovation and Competition
- Advancing American Leadership Abroad
- Ensuring Responsible and Effective Government Use of AI

Emergence of Artificial Intelligence, Specific Law and Regulation

Countries with AI Strategies in Place (2024):

- Algeria,* Argentina, Azerbaijan,* Australia, Austria, Bahrain, Bangladesh, Benin,* Botswana,* Brazil, Belgium,* Bulgaria, Canada, Chile, China, Colombia, Croatia, Cyprus, Czech Republic, Denmark, Dominican Republic,* Egypt, Arab Republic, Ethiopia, Estonia, Finland, France, Germany, Ghana, Greece, Hong Kong, Hungary, India, Indonesia, Iran,* Iraq,* Ireland, Israel,* Italy, Japan, Jordan,* Kenya, Korea Republic, Latvia, Lithuania, Luxembourg, Malta, Malaysia, Mauritius, Mexico, The Netherlands, North Korea, Norway, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russia, Rwanda, Saudi Arabia, Serbia, Sierra Leone, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Thailand, Tunisia,* Turkey, Ukraine, United Arab Emirates, United Kingdom, United States, Uruguay, Vietnam

Countries with AI Strategies in Development (2024):

Andorra,* Antigua and Barbuda,* Barbados,* Armenia,* Belarus,* Costa Rica,* Cuba,* Iceland, Jamaica,* Kenya, Morocco, New Zealand,* Nigeria,* Pakistan,* Senegal,* Uzbekistan

Source: https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf

Definition of AI in regulation

Country	Definition
EU	[EU AI Act 2021 proposal] "It proposes a single future-proof definition of AI." [Provisional Act March 13, 2024] "A key characteristic of AI systems is their capability to infer." "AI models [...] form part of AI systems."
US	[US Bill of Rights] AI as an "automated system". [EO] AI is "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments."
China	[Interim measures] "Art. 2: These measures apply to the use of generative AI technologies to provide services to the public in the [mainland] PRC for the generation of text, images, audio, video, or other content (hereinafter generative AI services)]."
UK	[White paper] "3.2.1 Defining Artificial Intelligence" "[...] AI by reference to the 2 characteristics that generate the need for a bespoke regulatory response [...]" [adaptivity and autonomy]

UK – Progress on Regulation of Artificial Intelligence

- UK Prime Minister said recently that AI “must be within a regulated framework”
- King of the United Kingdom's Speech of 17 July 2024:
  - New Labour government plans to "*seek to establish the most appropriate legislation to place requirements on those working to develop the most powerful AI models*". (Not expected to be as comprehensive as the EU's recently published AI Act.)
  - May make mandatory the currently voluntary commitments by leading developers of large language models/general purpose AI to submit algorithms to a safety assessment process, amending copyright legislation to allow organizations and individuals to opt out of allowing LLMs to scrape their content.

Related digital regulatory initiatives:

- **Digital Information and Smart Data Bill**.
- **Cyber Security and Resilience Bill**
- Department for Science, Innovation and Technology (DSIT), bringing together expertise in risk, regulation, and AI with backgrounds in data science, engineering, economics, and law… In 2024, we will launch a targeted consultation on a cross-economy AI risk register to ensure it comprehensively captures the range of risks.

EU - Artificial Intelligence Act

https://artificialintelligenceact.eu/

December 2023 - EU AI Act was endorsed by MEPs with 523 votes in favour, 46 against and 49 abstentions.

August 2024 – EU Artificial Intelligence Act (AI Act) came into force

- EU AI Act classifies AI systems into four different risk levels: unacceptable, high, limited, and minimal risk.
- Each class has different regulation and requirements for organizations developing or using AI systems.
- **Limited risk,** AI systems with a risk of manipulation or deceit - must be transparent, meaning humans must be informed about their interaction with the AI.
- **Minimal or no risk**, all other AI systems that do not fall under the above-mentioned categories, such as a spam filter. AI systems under minimal risk do not have any restrictions or mandatory obligations.
- Most obligations fall on providers (developers) of high-risk AI systems
- Deployers of high-risk AI systems have some obligations, though less than providers (developers).
    - Applies to deployers located in the EU, and third country users where the AI system's output is used in the EU

EU - Artificial Intelligence Act

- **Classifies AI according to its risk:**
  - “unacceptable risk”
    - Causing significant harm through: subliminal, manipulative, or deceptive techniques, exploiting vulnerabilities, social scoring, “pre-crime”, automated facial recognition database assembly, inferring emotions in workplaces or educational institutions, biometric categorisation systems,
  - Unacceptable also: 'real-time' remote biometric identification (RBI) in publicly accessible spaces for law enforcement, except when not using the tool would cause harm, in which cases:
    - Police must complete a **fundamental rights impact assessment** and **register the system in the EU database.**
    - Obtain **authorisation from a judicial authority or independent administrative authority**, in cases of urgency, deployment can commence, provided that authorisation is requested within 24 hours.

EU - Artificial Intelligence Act

- **Classifies AI according to its risk:**
  - "High Risk AI Systems"
    - Related to a safety component or product covered by EU Law (Applicable regulations in Annex I)
    - **If it profiles individuals, it's considered high-risk**
    - **Also – if relating to:** Critical infrastructure, Education and vocational training, Employment, workers management and access to self-employment, Access to and enjoyment of essential public and private services, Law enforcement, Migration, asylum and border control management, Administration of justice and democratic processes.
    - **EXCEPT IF:**
      - **Narrow procedural task**; or, **improves the result of a previously completed human activity**;
      - Detects decision-making patterns or deviations from prior decision-making patterns **and not meant to replace or influence the previously completed human assessment without proper human review**; or
      - **Performs a preparatory task to an assessment** relevant for the purpose of the use cases listed in Annex III.

EU - Artificial Intelligence Act

- "General purpose AI Systems"
  - Significant generality, capable to competently perform a wide range of distinct tasks, can be integrated into a variety of downstream systems or applications (does not cover AI used before release on the market for *research, development and prototyping activities*).
- Providers of General Purpose AI (GPAI) must provide technical documentation, instructions for use, comply with the Copyright Directive, and publish a summary about the content used for training.
  - **GPAI model providers to put in place a policy to respect existing EU copyright law, which applies to the entire AI cycle from the input level to the output level.**
- Free and open licence GPAI model providers only need to comply with copyright and publish the training data summary, unless they present a systemic risk.
  - GPAI models are considered systemic when the cumulative amount of compute used for its training is greater than 10^{25} floating point operations per second (FLOPS)
- All providers of GPAI models that present a systemic risk – open or closed – must also conduct model evaluations, adversarial testing, track and report serious incidents and ensure cybersecurity protections

EU - Artificial Intelligence Act

Providers of High risk AI must:

- Establish a **risk management system** throughout the high risk AI system's lifecycle;
- Ensuring that training, validation and testing datasets are relevant, sufficiently representative and, to the best extent possible, free of errors and complete according to the intended purpose.
- **Provide technical documentation** to demonstrate compliance and provide authorities with the information to assess that compliance.
- **Automatically record events relevant for identifying national level risks and substantial modifications** throughout the system's lifecycle.
- **Provide instructions for use** to downstream deployers to enable the latter's compliance.
- Design their high risk AI system to **allow deployers to implement human oversight**.
- Design their high risk AI system to **achieve appropriate levels of accuracy, robustness, and cybersecurity**.
- **Ensure compliance with quality management system**.

EU - Artificial Intelligence Act

After coming into force (August 2024), the AI Act will apply by the following compliance deadlines:

- 6 months for prohibited AI systems.
- 12 months for GPAI.
- 18 months after entry into force, the Commission will provide guidance on determining if an AI system is high risk, with list of practical examples of high-risk and non-high risk use cases.
- 24 months for high risk AI systems under Annex III.
- 36 months for high risk AI systems under Annex I.
- Codes of practice must be ready 9 months after entry into force (address international harmonization, detail obligations, include contributions of GPAI model providers, relevant national competent authorities).

US - Artificial Intelligence Law and Regulation

Several federal proposed laws related to AI, examples include:

- The SAFE Innovation AI Framework, which is a bipartisan set of guidelines for AI developers, companies and policymakers. This is not a law, but rather a set of principles to encourage federal law-making on AI
- The REAL Political Advertisements Act, which aims to regulate generative AI in political advertisements
- The Stop Spying Bosses Act, which aims to regulate employers surveilling employees with machine learning and AI techniques
- The Draft No FAKES Act, to protect voice and visual likenesses of individuals from unauthorized recreations from Generative AI
- The AI Research Innovation and Accountability Act, establishing a framework for AI innovation. It would create an enforceable testing and evaluation standard for high-risk AI systems and require companies that use high-risk AI systems to produce transparency reports.

US - Artificial Intelligence Law and Regulation

State legislatures have also introduced a substantial number of bills aimed at regulating AI, notably:

- On May 17, 2024, Colorado enacted the first comprehensive US AI legislation, the Colorado AI Act. The Act creates duties for developers and for those that deploy AI. The Act focuses on automated decision-making systems and defines a covered high-risk AI system as one that "when deployed, makes, or is a substantial factor in making a consequential decision." The Act will go into effect in 2026
- The California Consumer Privacy Act
  - Contains provisions on the use of automated decision-making tools.
  - Additionally, the California Privacy Protection Agency released draft rules on these provisions governing consumer notice, access and opt-out rights with respect to automated decision-making technology,
- More than 40 state AI bills were introduced in 2023, with Connecticut and Texas actually adopting statutes.

US - Artificial Intelligence Law and Regulation

Many state privacy bills have different definitions of automated decision-making technology or "profiling":

- A recent Texas statute establishing an AI advisory council (HB 2060) defines an "*automated decision system" as "an algorithm, including an algorithm incorporating machine learning or other artificial intelligence techniques, that uses data-based analytics to make or support governmental decisions, judgments or conclusions*"

- Connecticut's Public Act No. 22-15 defines "profiling" as "*any form of automated processing performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements*"

- The California Privacy Protection Act defines "profiling" as "*any form of automated processing of personal information, [...] to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements*."

References

- https://www.coursera.org/articles/history-of-ai
- https://en.wikipedia.org/wiki/Regulation_of_artificial_intelligence
- https://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights#
- https://en.wikipedia.org/wiki/International_Bill_of_Human_Rights
- https://en.wikipedia.org/wiki/World_Summit_on_the_Information_Society
- https://en.wikipedia.org/wiki/Common_heritage_of_humanity
- https://blog.irvingwb.com/blog/2024/07/ai-is-uniquely-suited-to-regulation-by-design.html
- UK Artificial Intelligence Regulation Impact Assessment IA No: RPC Reference No: RPC-DCMS-5260(1) Lead department or agency: Department for Science, Innovation & Technology
- https://assets.publishing.service.gov.uk/media/6697f5c10808eaf43b50d18e/The_King_s_Speech_2024_background_briefing_notes.pdf
- https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
- https://ised-isde.canada.ca/site/ai-strategy/en

References

- https://aiindex.stanford.edu/wp-content/uploads/2024/04/HAI_2024_AI-Index-Report.pdf
- https://en.wikipedia.org/wiki/Artificial_Intelligence_Act
- https://www.sec.gov/files/rules/proposed/2023/34-97990.pdf https://www.jdsupra.com/legalnews/sec-proposes-rules-on-the-use-of-ai-by-8228482/
- https://www.lexology.com/library/detail.aspx?g=38ecf296-7a7d-40b0-bd64-51515c584bae
- https://www.coloradosos.gov/CCR/eDocketDetails.do?trackingNum=2023-00438
- https://cyber.harvard.edu/story/2024-06/global-ai-regulation-protecting-rights-leveraging-collaboration
- https://ourworldindata.org/grapher/national-strategies-on-artificial-intelligence
- https://digital-strategy.ec.europa.eu/en/policies/ai-pact
- https://www.g20.org/pt-br/noticias/brasil-lanca-plano-de-us-4-bi-para-ia-e-prepara-acao-global-sobre-o-tema
- https://economia.uol.com.br/noticias/estadao-conteudo/2024/07/30/governo-preve-criar-nuvem-brasileira-de-armazenamento-de-dados-em-plano-de-ia.htm
- https://brazilian.report/tech/2024/08/05/lead-global-south-ai-regulations/

References

- https://www.cbc.ca/news/politics/ai-pioneer-canada-needs-law-to-regulate-ai-now-1.7105463
- https://tech.eu/2023/12/18/dfinity-launches- a-game-changing-subnet-to-help-devs-build-gdpr-compliant-dapps/?s=31&mc_cid=50ee1646cf
- https://www.acma.gov.au/dp-reg-joint-public-statement
- https://www.reuters.com/technology/irish-privacy-regulator-fines-meta-more-than-400-mln-2023-01-04/
- https://policyoptions.irpp.org/magazines/march-2024/online-harms-act/
- https://www.acma.gov.au/dp-reg-joint-public-statement
- https://www.reuters.com/legal/google-settles-5-billion-consumer-privacy-lawsuit-2023-12-28/
- https://www.classaction.org/media/brown-et-al-v-google-llc-et-al.pdf
- https://academic.oup.com/book/39826/chapter-abstract/339954720?redirectedFrom=fulltext
- https://www.lawfaremedia.org/article/china-gains-as-u.s.-abandons-digital-policy-negotiations
- https://www.law-democracy.org/live/rti-rating/
- https://berjon.com/gpc-under-the-gdpr/
- https://www.fct-cf.gc.ca/en/pages/law-and-practice/artificial-intelligence