NORTON ROSE FULBRIGHT

AI regulation

Global guide

As organisations continue with their roll-out of AI, the global regulatory landscape is becoming increasingly complex. AI-specific laws like the EU AI Act already applicable and new AI-specific laws are proposed, adding to the range of existing laws and regulations applicable to AI.

Our global guide provides you with an overview of the key points on AI regulation across twelve jurisdictions, equipping you with the tools to navigate the regulatory issues applicable to your AI projects across:

- AI-specific laws
- Data protection
- HR, employment, and discrimination
- Medical devices and healthcare
- Financial services regulation and guidance

Contents

AI in Australia

Overview

- The Australian Government is implementing an AI Action Plan that aims to create an environment in which AI can be developed and adopted.
- The government is not proposing to introduce comprehensive AI legislation.
- The data protection regulator, the Office of the Australian Information Commissioner (OAIC), has provided guidance on the applicability of privacy laws to AI.

AI Laws

- No standalone AI law is in place yet; currently a patchwork of existing laws, industry-specific regulations and non-binding guidance and standards define the AI legal landscape.
- The Department of Industry, Science and Resources published a Voluntary AI Safety Standard which recommends 10 guardrails for organisations to follow when developing and deploying AI.
- The Department has also proposed mandatory guardrails which heavily overlap with the Voluntary AI Safety Standard.
- Existing laws apply to AI, in particular:
  - *Privacy Act 1988* (Cth)
  - *Competition* and *Consumer Act 2010* (Cth)
  - Intellectual property legislation such as the *Copyright Act* 1968 (Cth)
  - Directors' duties under the *Corporations Act 2001* (Cth)

Data protection law and guidance

- The Privacy Act and Australian Privacy Principles are applicable:
  - Key principles include fairness, transparency and accuracy.
  - Collection of personal information must be necessary, and consent is required for the collection of sensitive personal information.
  - From 10 June 2025, a new statutory tort of serious invasions of privacy allows individuals to bring claims if their privacy is intruded upon or their personal information is misused.
  - From 10 December 2026, privacy policies must inform individuals when decisions are made using automated processes (many of which will likely include AI).

- Currently small businesses with an annual turnover of less than AUD3 million are exempt from the Privacy Act requirements (except for the statutory tort), however amendments are expected in 2026 which may remove this exemption.
- The OAIC has also provided guidance on the applicability of privacy obligations to commercially available AI.

HR, employment, and discrimination

- There is a variety of legislation to protect people from discrimination and harassment:
  - *Racial Discrimination Act 1975* (Cth)
  - *Sex Discrimination Act 1984* (Cth)
  - *Australian Human Rights Commission Act 1986* (Cth)
  - *Disability Discrimination Act 1992* (Cth)
  - *Age Discrimination Act 2004* (Cth)
  - State and Territory specific legislation which generally overlaps with the federal legislation
- The Australian Human Rights Commission (AHRC) has statutory responsibilities under legislation to enforce the prohibition on discrimination and harassment, and promote equal opportunity.
- The AHRC has made submissions to committees on Adopting AI and on the Mandatory Guardrails for AI in High-Risk Settings, with recommendations to ensure the safe implementation of AI.

Medical devices / healthcare

- Medical devices (including software) are subject to the *Therapeutic Goods Act 1989* (Cth) and the *Therapeutic Goods (Medical Devices) Regulations 2002*, which impose a range of safety and conformity obligations.
- The Therapeutic Goods Administration (TGA) has provided updated guidance on software and AI as a medical device.
- Generally, software (including AI) that is supplied in Australia for health or medical purposes comes under this legislation and must be registered with the TGA and included in the Australian Register of Therapeutic Goods.
- Where a developer adapts, builds on or incorporates AI into their product or service offering to a user or patient in Australia - the developer is deemed to be the manufacturer and must comply with obligations under the legislation.

Financial services regulation and guidance

- Financial services are governed by a range of legislation, including:
  - *Corporations Act 2001* (Cth)
  - *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
  - *Competition and Consumer Act 2010* (Cth)
  - Prudential and Reporting Standards and guidance for authorised deposit-taking institutions
- There are also several regulators for the sector, including the Australian Securities and Investments Commission (ASIC), Australian Prudential Regulation Authority (APRA), Reserve Bank of Australia, and the Australian Competition and Consumer Commission.

ASIC has published a review into the adoption of AI by financial service providers and raised concerns that the rate of adoption is outpacing risk and governance arrangements. It encourages financial service providers to take a proactive approach to ensure their use of AI does not breach existing obligations, consumer protection laws and directors' duties.

AI in Canada

Overview

- Canada was the first country in the world to introduce a national AI strategy which includes various initiatives to support responsible use of AI including, the Advisory Council on Artificial Intelligence and the Safe and Secure Artificial Intelligence Advisory Group.
- In 2023, Canada launched the Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems which now has 46 signatories.

AI Laws

- There is currently no specific regulatory framework for AI in Canada.
- The *Artificial Intelligence and Data Act* (AIDA) was tabled by the federal government in June 2022, and sought to enact a comprehensive regulatory scheme for the development, deployment and operation of AI systems in Canada. The controversial proposed legislation died with the prorogation of Parliament in January 2025, bringing renewed uncertainty to the future of AI regulation in Canada.
- In March 2025, the federal government launched Canada's first AI Strategy for the federal public sector which aims to advance accountability, training and transparency in the adoption of responsible AI systems utilized by the federal government.
- Existing laws are applicable to AI, including:
  - *Personal Information Protection and Electronic Documents Act* (PIPEDA)
  - *Consumer Privacy Protection Act* (CPPA)
  - Provincial privacy laws, including Quebec's Law 25

Data protection law and guidance

- PIPEDA and similar provincial privacy legislation is currently applicable to use of AI systems:
  - Key principles include accountability, identifying purposes, consent, openness and safeguards.
  - There is no outright prohibition on the use of AI systems for automated decision-making in Canada, but data privacy laws focus on minimizing risk.
- The Office of the Privacy Commissioner of Canada has published a document entitled *Principles for responsible, trustworthy and privacy-protective generative AI technologies* that identifies considerations for applying the key privacy principles to emerging AI systems.

- Enforcement of compliance with privacy regulations and penalties occurs pursuant to PIPEDA under the jurisdiction of the Office of the Privacy Commissioner of Canada (OPC). The CPPA will introduce significantly stronger enforcement powers and increased fines for privacy violations involving automated decision-making and AI systems, including:
  - Administrative money penalties (AMPs) up to $10 million or three percent of global revenue for violating consent, transparency or data security requirements
  - Criminal penalties of up to $25 million or five percent of global revenue for obstruction of an inquiry by the federal privacy commissioner, destruction of data or other serious non-compliance.

HR, employment, and discrimination

- Various laws exist to protect people from bias, discrimination and harassment, including:
  - *Canadian Human Rights Act*, RSC, 1985, c H-6 (CHRA)
  - Provincial human rights legislation, such as the Ontario *Human Rights Code*, R.S.O. 1990, c. H.19 (OHRC)
  - *Consumer Privacy Protection Act* , Bill C-27 (CPPA)
  - *Canada Labour Code,* RSC, 1985, c L-2 (CLC)
  - Provincial employment standards legislation
- Bill 149, the *Working for Workers Four Act*, 2024, amended the regulations to Ontario's *Employment Standards Act, 2000* (ESA) to include a definition of "artificial intelligence" as part of a newly introduced scheme requiring AI-related disclosure by employers. Beginning in 2026, Bill 149 will require employers in Ontario to disclose in job postings if they are using AI in the hiring process to support with screening, assessing or selecting applicants.
- Similarly, Quebec's Law 25 explicitly enforces automated decision transparency for organizations, including employers, that utilize AI systems. Employers in Quebec must notify and explain AI-based decisions to applicants and employees.
- The Ontario Human Rights Commission and the Law Commission of Ontario launched a Human Rights Impact Assessment for AI Technologies (HRIA), which helps assess and mitigate human rights impacts of AI systems by organizations, including employers.

Medical devices / healthcare

- AI medical devices often process sensitive personal health information and therefore their use must comply with relevant privacy laws, including:
  - PIPEDA
  - Provincial health privacy laws, such as Ontario's *Personal Health Information Protection Act* (PHIPA)
- Health Canada regulates the approval of medical devices for use in Canada pursuant to the F*ood and Drugs Act* and accompanying *Medical Devices Regulations*.
  - This scheme outlines requirements for pre-market approval, quality management, clinical evaluation and post-market surveillance requirements.
  - Key principles applied in approving AI-based medical devices include transparency and explainability.

Financial services regulation and guidance

- Financial services in Canada are governed by various laws, including:
  - *Bank Act*
  - *Financial Consumer Agency of Canada Act*
  - *Competition Act*
  - *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*
- In 2024, the Office of the Superintendent of Financial Institutions (OSFI) and the Financial Consumer Agency of Canada (FCAC) released a joint report on best practices for adopting AI systems in the financial services industry.

The Canadian Securities Administrators (CSA) have also issued a notice on the application of existing securities laws to AI systems by capital market participants which highlights the importance of transparency, accountability and risk mitigation to foster a fair and efficient market environment.

AI in China

Overview

- The PRC government has taken various measures to promote and regulate the development of the AI industry. The policy direction of the field of AI is to achieve a balance by promoting the development of the AI industry while safeguarding the legitimate rights and interests of all parties involved.
- The central government has issued several documents to promote the development of the AI industry, and some local governments have issued detailed policies on practical measures. Certain departments of the central government have also issued administrative regulations and rules around the development of the AI industry which regulate the usage and development of AI tools.
- The Cyberspace Administration of China (CAC) is the most active official department who issued several regulation and measures on cybersecurity, personal data protection, AI generated content, etc. Other departments such as the China National Intellectual Property Administration (CNIPA) and the Ministry of Science and Technology (MOST) also published some guidelines and policies regarding IP establishment and promoting the development of the industry.
- Current litigation is mainly focused on copyright infringement caused by AI generated content. Some cases also relate to the AI training process. The number of patents related to AI are now accumulating, which gives a good basis for enforcement cases in the future.
- The government has published standards (soft law) covering various areas.
- One of the future areas of focus for AI legislation may be AI ethics.

AI Laws

- The CAC has issued rules on its own or jointly with other relevant authorities, covering:
  - The governance of generative AI services
  - The administration of deepfake technologies
  - The administration of algorithms of AI models
  - The administration of AI-generated content labelling

- Other departments also issue rules and guidelines in their specific areas:
  - CNIPA issued guidelines on AI related patent applications.
  - MOST issued policies and guidelines on supporting the development of AI industry.
  - Both the state council and the MOST released opinions and specifications of AI ethics.
- Some ministries issued guidelines of applying AI techs in their fields:
  - The Ministry of Industry and Information Technology and the Ministry of Transportation issued guidelines and rules of on-road auto pilot test and auto pilot services.
- The legislation department will continue to push forward legislation in the AI space in 2025.

Data protection law and guidance

- The three fundamental laws governing cyber security and data protection (i.e., the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law) generally apply in the AI space.
- Key principles include transparency, fairness and the prohibition of unreasonable differential treatment. Personal information protection impact assessment is also required for implementing automated decision-making.
- The CAC (being the major governing authority in the data protection space), together with various other governmental agencies, form a joint force to regulate the AI space and has issued various lower-level regulations to specifically regulate algorithms/deepfake/generative AI with an emphasis on personal information protection.
- Various local governments have issued measures to promote and embrace AI technologies.
- The National Technical Committee 260 on Cybersecurity of Standardization Administration of China (known as TC260) has issued and will issue various national standards (soft law) to provide guidelines in development and use of AI technologies. It is anticipated that over 50 national standards and sectoral standards will be issued in the near future in this area.
- The enforcement cases currently focus on the misuse of AI to spread illegal information and failure to file the necessary registration for algorithms. There are no significant fines at the moment. Using AI to conduct illegal activities may attract criminal liability, depending on the specific circumstances.

HR, employment, and discrimination

- Currently, there is no specific guidance on AI discrimination in an employment context, although certain provisions on equal rights, non-discrimination, etc. can be found in the relevant labour laws.
- The Provisions on the Management of Algorithmic Recommendations for Internet Information Services issued by the CAC provides that where algorithmic recommendation service providers provide work scheduling services to workers, they shall protect the lawful rights and interests of workers in obtaining labour compensation, rest and vacation. They must also establish and improve algorithms such as for the assigning of orders on the platform, the composition and payment of remuneration, working hours, rewards and punishments, etc.

Medical devices / healthcare

- Central and local governments have issued policies and measures to embrace and promote integration of AI technologies with pharmaceutical/healthcare sector.
- The National Health Commission (together with other governmental agencies) has issued guidelines for applying AI technology to different use cases in the healthcare sector.
- Medical devices (including software) are subject to the Medical Devices Supervision and Management Regulations, which impose a range of safety and conformity obligations.
- The National Medical Products Administration (NMPA) has issued a few guidelines relating to AI including those, for example, on categorization of AI-based medical software products, and registration review of AI-based medical devices. NMPA has also issued sectoral standards to regulate the application of AI-related technology in the healthcare space.

Financial services regulation and guidance

- The current regulatory landscape of China's financial services sector emphasizes aspects of risk control, transparency and reasonableness of AI models or algorithms, as well as data privacy/security protections.
- The Administrative Measures for Data Security of Banking and Insurance Institutions released by the National Financial Regulatory Administration (NFRA, being one of the financial services regulators in China) on 27 December 2024 (became effective on the same date) require that:
    1. If a banking/insurance institution carries out automated decision-making analysis or model or algorithm development, it shall ensure the transparency of data handling and the fairness and reasonableness of the results.

2. Before a model or algorithm is put into use, a banking/insurance institution shall perform a data security review, and examine the reasonableness, legitimacy and interpretability of the use of data and models, as well as the impact of the use of data on the legitimate rights and interests of the relevant subjects, ethical and moral risks and the effectiveness of prevention and control measures.
3. When using AI technology to carry out business, a banking/insurance institution shall explain and disclose the impact of data on the decision-making results and establish risk mitigation measures for AI applications.

- The People's Bank of China (PBOC) has also issued several industry standards for the financial services sector relating to utilisation of AI algorithm applications. It recommends that financial institutions in China conduct a compliance audit over their financial applications based on AI algorithm and disclose relevant audit results/reports online, such as through their official website.
- The regulatory environment in China for the financial services sector has been supportive in terms of deployment of AI services and development of AI applications, whilst the authorities continue to strike a balance between the technology innovation and the increasing regulatory complexity alongside the development of AI technology.

AI in France

Overview

- The current French administration prioritizes 'digital sovereignty' as a national policy, aiming to foster the growth of a domestic AI industry, particularly by supporting start-ups that develop and utilize innovative AI technologies, including with the law.
- Initiated in 2018, France's National AI Strategy aims to position the country as a global leader in AI by 2030 with in investment of almost EUR 2.5 billion. The strategy has evolved through multiple phases, with the latest phase launched in February 2025 to strengthen computing infrastructure, attract and train AI talent, accelerate AI applications and build trustworthy AI.
- In February 2025, the French Government announced the creation of the National Institute for the Evaluation and Safety of Artificial Intelligence (INESIA) dedicated to the evaluation and safety of AI and aimed at guaranteeing national security in the AI domain.

AI Laws

- The EU AI Act has applied from 2 February 2025.
- As of now, France does not have jurisdiction-specific laws exclusively governing AI.
- However, AI applications are subject to existing regulations such as data protection laws (see below) and a patchwork of sector-specific regulations.
- For instance, Law No. 2019-486 of 22 May 2019 ("Pacte Law") sets out the conditions for autonomous vehicles to travel on the roads and clarifies the criminal liability regime applicable in the event of an accident involving such a vehicle.
- Law No. 2023-451 of 9 June 2023, requires that influencers clearly indicate the label "virtual images" on any photos or videos that have been digitally generated using AI to ensure transparency for their audience.
- Law No. 2024-449 of 21 May 2024, introduces a new criminal offence under Article 226-8-1 of the French Criminal Code, punishing the non-consensual dissemination of sexually explicit content generated by AI (deepfakes). The law also mandates educational measures in secondary schools to raise awareness about AI-generated content.

Data protection law and guidance

- The GDPR applies to any AI use involving personal data.
  - Key principles include fairness, transparency, accuracy and accountability.
  - There is a default prohibition on solely automated decisions with significant effects.
- In May 2023, the CNIL released its AI action plan addressing the rapid development of generative AI and large language models.
- As part of its efforts to encourage and lead the development of soft law in AI, since 2022 the CNIL has also published various guidance, including:
  - A self-assessment guide including a series of checklists with explanations to assist providers or users of AI systems in complying with data protection obligations.
  - Recommendations for AI system development (10 factsheets), clarifying the intersection of AI with GDPR, and supplemented by two additional factsheets focusing on informing individuals and facilitating their rights.
  - Recommendations on the use of public data and open data distributors to ensure the lawful reuse of personal data databases.
  - FAQs on the EU AI Act and its relationship with the GDPR.
  - FAQs regarding the deployment of GenAI systems, emphasizing key points to ensure compliance with the GDPR and the EU AI Act.
- On 20 October 2022, the CNIL issued a penalty of 20 million euros and ordered the company Clearview AI Inc. to stop collecting and using, without legal basis, the data of individuals in France and to delete those already collected. The CNIL is also participating in the EU task force on ChatGPT to investigate on the compliance of their data protection practices following the various complaints received by EU data protection authorities, including the CNIL.

HR, employment, and discrimination

- Under Article L. 1132-1 of the French Labour Code, employees and job applicants in the private sector are protected against discrimination. More generally, discrimination is an offence defined in the French Criminal Code under Articles 225-1 et seq.
- The Economic, Social and Environmental Council (CESE) has issued a cross-cutting opinion on AI and its impacts on labour and employment.
- On November 2024, the CNIL published a guide regarding the use of AI-augmented cameras in freight vehicles to monitor employees for safety purposes.

Medical devices / healthcare

- The EU Medical Devices Regulation and AI Act affect players who intend to implement AI in medical devices or healthcare. In addition, the new EU Product Liability directive makes it easier for consumers to bring claims for defective products and AI medical devices.
- The Bioethics law of 2021 first brought the concept of AI into the French public health Code. Also, both the AI Act and the Medical Device Regulation (2017/745) are applicable to medical devices using AI in France.
- In November 2022, the national ethics committee (CCNE) and the national digital ethics committee (CNPEN) issued a joint guidance on the AI systems applied to medical diagnostic which can be essential to the patient's care.
- In 2023, the CNIL launched a sandbox with healthcare companies. Some projects used AI, and the CNIL provided informal guidance on data protection during AI training and deployment.
- On 11 February 2025, during the AI Summit, the French Minister for health announced the launch of work on a national roadmap for AI in healthcare, highlighting AI's strategic importance in this area.

Financial services regulation and guidance

- Under the French administrative order (*Arrêté*) of 3 November 2014 on the internal control of entities in the banking, payment services and investment services sectors, AI systems used in internal controls in the financial sector must be supervised by qualified personnel.
- Article L.533-10-3 of the French Monetary and Financial Code, which transposes Directive 2014/65 (MiFID II), establishes a regulatory framework for algorithmic and high-frequency trading. In May 2024, the Financial Market Authority (AMF) underlined governance duties and algorithm accountability in high-frequency contexts.
- The French banking authority (ACPR) and the AMF regularly publish guidance on the use of AI in the financial sector in the form of good practices, research and news item, such as on the explainability of AI (eg. with AI based-credit risk predictive models or robot-advisor). The AMF also warned investors in April 2025 against relying solely on AI tools for investments decisions, emphasizing that these tools do not guarantee returns and may be exploited in scams.

Several enforcement measures have been taken against entities found to have breached French rules in relation with algorithmic trading. For example, the AMF fined a British high-frequency trading firm EUR 400,000 for allowing technical failures to persist, leading to order book pollution on several CAC 40 stocks (AMF, Commission des sanctions, 8 July 2016).

AI in Germany

Overview

- Due to a lack of a competent authority, the AI Act has so far remained less important in Germany.
- Under the GDPR, the conference of German data protection authorities *(Datenschutzkonferenz – DSK)* has provided extensive guidance on choosing and using AI.

AI Laws

- The EU AI Act has applied from 2 February 2025.
- The German Government released a draft bill for a law implementing the European AI Regulation AI Market Surveillance Act (*KI-Marktüberwachungsgesetz*) in January 2025, which addresses the competent authorities under the EU AI Act:
  - Existing market surveillance and notifying authorities will also oversee compliance with the EU AI Act (e.g. the German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*).
  - In areas where no supervisory authority exists, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways (*Bundesnetzagentur*) serves as the market surveillance authority and notifying authority.

Data protection law and guidance

- The GDPR applies to any AI use involving personal data.
  - Key principles include fairness, transparency, accuracy and accountability.
  - There is a default prohibition on solely automated decisions with significant effects.
- Several state data protection authorities and the DSK have published guidance on the selection and usage of AI from a privacy perspective.
- The guidance by the Conference of Data Protection Authorities contains detailed guidance on setting up and using AI from a privacy perspective and the requirements which operators should consider when choosing an AI system to use.

HR, employment, and discrimination

- The General Act on Equal Treatment (*Allgemeines Gleichbehandlungsgesetz* – AGG) includes protection against discrimination (direct and indirect), as well as harassment and victimization – protected characteristics:
  - Race or ethnic origin
  - Gender
  - Religion or belief

  - Disability
  - Age
  - Sexual orientation
- The Federal Anti-Discrimination Agency published a detailed legal opinion on The General Equal Treatment Act and protection against discrimination by algorithmic decision-making systems.
- Also, the DSK guidance on AI contains a brief section on avoiding discrimination when using AI systems.
- In certain cases, using AI systems in companies may also trigger co-determination of the works council. When simply allowing the usage of AI, this can be prevented by not allowing the employer to access users' prompts.

Medical devices / healthcare

- The EU Medical Devices Regulation and AI Act affect players who intend to implement AI in medical devices or healthcare. In addition, the new EU Product Liability directive makes it easier for consumers to bring claims for defective products and AI medical devices.
- Medical devices (including software) are subject to the Medical Devices Regulation (Regulation (EU) 2017/745), which impose a range of safety and conformity obligations.
- The German Federal Institute for Drugs and Medical Devices (*Bundesinstitut für Arzneimittel und Medizinprodukte* – BfArM) is currently exploring ways of using AI in the health care space. For example, Health Data Lab of the BfArM is currently working on a project to use AI to generate synthetic health data to be used for medical research.

Financial services regulation and guidance

- The German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – BaFin) has been actively publishing guidance on AI for the last couple of years.
- Its Principles for the Use of Algorithms in Decision-Making Processes from 2021 laid down four principles for using AI in the finance and insurance sector:
  - Clear responsibility of management
  - Adequate risk and outsourcing management
  - Avoidance of bias
  - Prevention of legally prohibited discrimination
- Since then, the BaFin has published several pieces of guidance on the matter with the main focus being risk management of using AI systems and ensuring fair and non-discriminatory usage.

AI in Hong Kong

Overview

- The government has adopted an internal AI guideline, "Ethical Artificial Intelligence Framework" to assist government bureaux/departments in planning, designing and implementing AI and big data analytics in their IT projects and services.
- The government is not proposing to introduce comprehensive AI legislation.
- The data protection regulator, the Office of the Privacy Commissioner for Personal Data (PCPD), has published "Guidance on the Ethical Development and Use of Artificial Intelligence".

AI Laws

- No comprehensive AI law proposed.
- The government has proposed to amend the Copyright Ordinance to introduce a text and data mining (TDM) exception.
- Various authorities including the PCPD, Hong Kong Monetary Authority (HKMA), Securities and Futures Commission (SFC), Financial Services and the Treasury Bureau (FSTB), Department of Health and the Judiciary issued industry-specific guidelines on AI.

Data protection law and guidance

- The key principles of the Personal Data (Privacy) Ordinance (PDPO) include fairness in the collection of personal data, informed consent to the use of data for direct marketing, openness and transparency, as well as accuracy and security of data.
- The PCPD published the Guidance on the Ethical Development and Use of Artificial Intelligence in 2021, recommending the three Data Stewardship Values (respectful, beneficial and fair) and adopting the seven Ethical Principles for AI:
    4. Accountability
    5. Human oversight
    6. Transparency and interpretability
    7. Data privacy
    8. Fairness
    9. Beneficial AI
    10. Reliability, robustness and security

- The "Guidance on the Ethical Development and Use of Artificial Intelligence" published by PCPD in 2024 provides a set of recommendations on the best practices for any organisations procuring, implementing and using any type of AI systems that involve the use of personal data.
- Human oversight is not compulsory but is recommended to mitigate the risks of AI systems.
- The PCPD also issued guidance notes on collection and use of fingerprint and biometric data.
- In the enforcement space, the PCPD investigated an employer for unnecessary and excessive collection of fingerprint data and issued a warning letter (Case No.:2008C04).

HR, employment, and discrimination

- The four anti-discrimination laws in Hong Kong are:
  - Sex Discrimination Ordinance
  - Disability Discrimination Ordinance
  - Family Status Discrimination Ordinance
  - Race Discrimination Ordinance
- The Equal Opportunities Commission (EOC) has not issued any formal guidance regarding AI, but in an interview the EOC Chairperson acknowledged the potential impact of AI and automated decision-making system on inequalities and discrimination.

Medical devices / healthcare

- There is no specific law in Hong Kong regulating medical devices, but depending on the nature of the product it may be regulated by other laws such as the Pharmacy and Poisons Ordinance, the Radiation Ordinance, the Telecommunications Ordinance and the Electrical Products (Safety) Regulation.
- A voluntary Medical Device Administrative Control System (MDACS) is available for registration of medical devices.
- The Department of Health issued a technical note on the requirements for listing of AI medical devices on the MDACS.

Financial services regulation and guidance

- A number of guidelines are published by HKMA, SFC and FSTB:
  - Generative Artificial Intelligence in the Financial Services Space (HKMA, 2024).
  - Use of Artificial Intelligence for Monitoring of Suspicious Activities (HKMA, 2024).
  - Consumer Protection in respect of Use of Generative Artificial Intelligence (HKMA, 2024).
  - High-level Principles on Artificial Intelligence (HKMA, 2019).
  - Circular to licensed corporations - Use of generative AI language models (SFC, 2024).
  - Policy Statement on Responsible Application of Artificial Intelligence in the Financial Market (FSTB, 2024).
- HKMA and the Hong Kong Cyberport initiated a Generative AI Sandbox program in which participants (including 10 banks and four technology companies) are developing and testing AI systems for enhancing risk management, anti-fraud measures and customer experience.

Intellectual Property

- The government launched a public consultation in July 2024 regarding potential amendments to the Copyright Ordinance in view of AI technology.
- At the end of the consultation, the government concluded that the existing Copyright Ordinance already contains applicable provisions to protect the copyright of AI-generated works, and are sufficient to address copyright infringement cases involving AI-generated works.

The government also suggested to introduce a TDM exception to allow reasonable use of copyright works for computational data analysis and processing.

AI in Italy

Overview

In recent years, the Italian government has developed a structured and forward-looking approach to the regulation of AI, based on the guidelines of the European Commission's White Paper on AI.

- This approach is based on two main strands. The first involves the government's commitment, which began in 2020 with the development of a National AI Strategy under the Ministry of Enterprise and Made in Italy. This strategy is part of the broader European Coordinated Plan on AI and is designed to be implemented through joint efforts between EU member states and institutions.
- The Italian Strategy for Artificial Intelligence 2024-2026 was published on 22 July 2024, identifying three strategic macro-objectives, namely, (i) supporting the implementation and adoption of AI applications to support management practices, production models, and innovation projects; (ii) promoting functional and applied scientific research activities; (iii) enhancing human capital through training and the development of talent with the necessary skills.
- The second strand is at the Parliament level and consists of the intensive fact-finding work carried out during this legislative term by various bodies of the Chamber of Deputies.
- In parallel, the Italian Data Protection Authority (IDPA) has been at the forefront of AI oversight, having already issued several decisions and fines aimed at ensuring compliance with data protection standards in the development and deployment of AI systems.

AI Laws

- The EU AI Act has applied from 2 February 2025.
- The Italian Parliament is working on a draft law on AI. The proposal sets out principles governing the research, testing, development, adoption, and application of AI systems and models.
- The aim of the bill is to promote proper, transparent, and responsible use of AI in an anthropocentric context, with a view to seizing the opportunities it offers. It will ensure oversight of the economic and social risks and the impact of AI on fundamental rights.
- The provisions included in the draft law shall be interpreted and applied in accordance with the EU AI Act.

Data protection law and guidance

- The GDPR applies to any AI use involving personal data.
  - Key principles include fairness, transparency, accuracy and accountability.
  - There is a default prohibition on solely automated decisions with significant effects.
- The IDPA has been active on AI enforcement:
  - On 20 December 2024 the IDPA imposed a fine of 15 million EUR against OpenAI in relation to its ChatGPT service. The IDPA alleged that OpenAI had breached various obligations under the GDPR, including its transparency and information obligations and the requirement to identify an appropriate lawful basis. The IDPA also alleged it had failed to implement age verification to protect children. OpenAI is appealing the fine and was granted an interim suspension on the IDPA's fining decision by the Court of Rome while the appeal is ongoing.
  - On 19 May 2025, the IDPA imposed a 5 million EUR fine on the US-based company Luka Inc., which manages the chatbot Replika. Alleged breaches included failing to identify an appropriate lawful basis, breaches of transparency and information obligations, and failure to implement age verification mechanisms. The IDPA also launched a further investigation to assess whether personal data are being properly processed by the generative AI system behind the service.
  - On 30 January 2025, the IDPA ordered Hangzhou DeepSeek Artificial Intelligence and Beijing DeepSeek Artificial Intelligence, the Chinese companies that provide the DeepSeek chatbot service, to stop processing Italian users' data, as a matter of urgency and with immediate effect.

HR, employment, and discrimination

- The Italian legal framework on HR, employment and discrimination is composed of a patchwork of legislation:
  - Article 3 of the constitution establishes the principle of equality of all citizens before the law, stipulating that everyone has equal social dignity without distinction of sex, race, language, religion, political opinion, personal, or social conditions.
  - The Workers' Statute (Law No. 300 of 20 May 1970) establishes rules on the protection of workers' freedom and dignity, freedom of association and trade union activity in the workplace, and rules on employment.
  - The Code of Equal Opportunities (Legislative Decree No. 198 of 11 April 2006) brings together the existing state legislation on gender equality in the political, social, and economic contexts. The Law No. 162 of 5 November 2021 amended the Code of Equal Opportunities and introduced gender equality certification and incentive tools for the most compliant companies.
  - Law No. 4 of 15 January 2021, regarding the ratification and implementation of

the International Labor Organization Convention No. 190 on the elimination of violence and harassment in the workplace, adopted in Geneva on 21 June 2019.

- The draft law on AI mentioned above includes specific provisions on the use of AI in the field of employment and possible related discrimination. It examines the specific case of the use of AI in the areas of organization and management of employment relationships. In this regard, the provision stipulates that, when using AI, the fundamental rights of individuals must be guaranteed, avoiding forms of discrimination based on sex, age, ethnic origin, religious belief, sexual orientation, political opinions, and personal, social, and economic conditions, in accordance with European Union law.
- Moreover, the draft bill includes a specific provision to set up an Observatory on the adoption of AI systems in the employment market within the Ministry of Labor and Social Policies, in order to mitigate the risks arising from the use of AI systems in the workplace.

Medical devices / healthcare

- The EU Medical Devices Regulation and AI Act affect players who intend to implement AI in medical devices or healthcare. In addition, the new EU Product Liability directive makes it easier for consumers to bring claims for defective products and AI medical devices.
- The healthcare sector could also be affected by the draft law on AI mentioned above. In fact, the bill includes several provisions aimed at regulating the use of AI in the healthcare sector.
- In particular, it provides that AI systems in healthcare shall serve as support in prevention, diagnosis, treatment, and therapeutic choice processes, without prejudice to the decision, which must always be left to healthcare professionals.
- It also establishes that AI systems in healthcare and the related data used must be reliable, periodically verified, and updated, with a view to minimizing the risk of errors and improving patient safety.
- The draft bill also includes prohibitions on conditioning access to healthcare services on discriminatory criteria using AI tools.

Financial services regulation and guidance

- The Bank of Italy is active within the space of AI and regularly publish guidance and papers on the topic, to provide information and analysis on various aspects at the intersection between AI and financial services regulation. For instance, in May 2025 it published a paper on the exploration of large language models (LLM) alignment in finance.

AI in the Netherlands

Overview

- Regulators are applying existing regulations to AI applications, focusing on transparency, explainability and risk management.
- The Dutch Data Protection Authority (AP) is working on guidelines for the use of AI in line with the AVG, focusing mainly on preventing discrimination and ensuring data protection.
- The Dutch government supports initiatives such as the Innovation Centre for Artificial Intelligence (ICAI) to promote cooperation between academic institutions and industry in developing reliable
  AI applications.
- The Dutch DPA uses fines to enforce the GDPR.

AI Laws

- The EU AI Act has applied from 2 February 2025.
- No AI-specific laws in the Netherlands. The regulation of AI is done within existing legal frameworks, such as the GDPR (AVG), the Financial Supervision Act (Wft), and the Healthcare Quality, Complaints and Disputes Act (Wkkgz).

Data protection law and guidance

- The GDPR applies to any AI use involving personal data.
  - Key principles include fairness, transparency, accuracy and accountability.
  - There is a default prohibition on solely automated decisions with significant effects.
- The Dutch DPA is producing and updating online content aimed at organizations to help them comply with the GDPR, such as guidance on DPIA's, privacy in annual reports, and guidelines for supervisory boards (RvC & RvT) of organizations.
- The Dutch DPA is actively enforcing the GDPR in the Netherlands through fines and formal warnings. Multiple fines have been imposed to companies including Clearview AI.

HR, employment, and discrimination

- The Dutch General Equal Treatment Act (*Algemene wet gelijke behandeling*) sees on the equal treatment of persons irrespective of religion, belief, political affiliation, race, sex, nationality, heterosexual or homosexual orientation or marital status.

- In addition, there are a number of more specific laws, such as the Equal Treatment of Man and Women Act (WGB), the Equal Treatment on the Grounds of Disability or Chronic Illness Act (WGBH/CZ) and the Equal Treatment on the Basis of Age in Employment Act (WGBL).
- The Dutch Ministry of the Interior and Kingdom Relations has provided guidance on 'non-discrimination by design' for the leading questions and principles that apply when developing and deploying an AI-system. More recently, the government published an E-learning on non-discrimination in algorithms and data for government organizations.
- The Dutch benefits scandal (*toeslagenaffaire*) involved the Tax Administration using a self-learning algorithm to detect fraud in childcare benefit applications. This algorithm disproportionately flagged families with dual nationalities or foreign-sounding names as high-risk, leading to false accusations of fraud and severe financial hardship for thousands of families. The scandal highlighted the dangers of unregulated algorithmic profiling and resulted in the resignation of the Dutch government in 2021. The Dutch DPA imposed a fine of €2.75 million on the Dutch Tax administration.

Medical devices / healthcare

- The EU Medical Devices Regulation and AI Act affect players who intend to implement AI in medical devices or healthcare. In addition, the new EU Product Liability directive makes it easier for consumers to bring claims for defective products and AI medical devices.
- The Dutch Health and Youth Inspectorate (IGJ) calls on healthcare providers to introduce generative AI in their own organization carefully and with attention to any risk. It states that healthcare providers must realise that the usage of AI applications must comply with the MDR and the AI Act.
- The IGJ published a Digital Care Assessment Framework which consists of standards and associated assessment criteria based on different laws and regulations.

Financial services regulation and guidance

- De Nederlandse Bank (DNB) and the AFM (the Dutch financial supervisory organizations) published guidance on the impact of AI on the financial sector, and general principles for the use of AI by financial institutions. In addition to this, the Dutch Financial supervision Act (Wft) and the EU AI Act are important for the usage of AI by financial institution and the supervision.

AI in Singapore

Overview

- Singapore has opted for a 'soft law', industry-led approach to AI governance, preferring advisory guidelines, toolkits, and frameworks over binding AI-specific legislation. Regulatory agencies have proactively published comprehensive and, in many cases, prescriptive guidance – including for key industries and business sectors (as elaborated on below).
- As a general approach, the Singapore regulators continue to emphasise a risk-based, pragmatic approach, balancing innovation with robust governance measures.
- Regional cooperation is also part of Singapore's strategy, as seen in its key role in developing and endorsing the *ASEAN Guide on AI Governance and Ethics,* promoting consistent and ethical AI deployment across Southeast Asia.

AI Laws

- Singapore does not currently have AI-specific legislation in place. The government has adopted a 'soft law' strategy of focusing on governance first and legislating later if needed.
- The Infocomm Media Development Authority (IMDA) has been particularly active, spearheading initiatives in collaboration with the AI Verify Foundation such as the *Model AI Governance Framework for Generative AI* (May 2024) and *Global AI Assurance Pilot* (February 2025). These efforts promote voluntary testing, transparency, and good practice through frameworks aligned with global standards.

Data protection law and guidance

- Singapore's Personal Data Protection Act 2012 (PDPA) is principles-based and technology-neutral. Organisations are generally required to notify individuals of the purposes of data collection and obtain consent, except in limited circumstances. While the PDPA does not ban automated decision-making, organisations should inform individuals and ensure transparency, especially in AI-related contexts.
- The Personal Data Protection Commission (PDPC) has introduced multiple frameworks and guidelines to strengthen AI governance, including the Artificial Intelligence Governance Framework in collaboration with the IMDA and an Implementation and Self-Assessment Guide for Organisations to assess their AI governance processes. In March 2024, the PDPC released the *Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems*, which provide practical guidance on how core obligations under the PDPA (e.g. consent, purpose limitation, and notification) apply when organisations use AI to make personalised recommendations or decisions.

- The PDPC has taken enforcement action and issued fines in cases of data breaches or other instances where data protection obligations are contravened. The PDPA also provides for potential civil claims to be brought by impacted individuals against organisations for damages suffered as a result of breaches of the PDPA.
- In relation to cybersecurity, Singapore's Cyber Security Agency (CSA) released the *Guidelines on Securing AI Systems* and a complementary companion guide in October 2024 to support the secure design and use of AI technologies. These documents adopt a lifecycle approach, outlining practical security considerations across five stages: planning and design, development, deployment, operations and maintenance, and end-of-life.
- While non-binding, the guidelines are intended to help organisations integrate security "by design and by default" into AI systems, and the Companion Guide provides concrete measures and best practices drawn from industry and research. The CSA views these as living documents, to be updated as the AI threat landscape evolves.

HR, employment, and discrimination

- Singapore's approach to workplace discrimination has recently moved from a guidance-based model to a formal legal framework with the introduction of the Workplace Fairness Act 2025, which gives legal force to certain anti-discrimination protections and fair employment practices. Previously, safeguards were outlined in the non-binding *Tripartite Guidelines on Fair Employment Practices*.
- There is growing attention on the use of AI in hiring. The government have encouraged responsible AI use, including in HR contexts, highlighting the importance of transparency, explainability, and accountability when AI tools are used in employment decisions. However, there is no sector-specific regulation yet that directly governs the use of AI in hiring or employment.

Medical devices / healthcare

- The Ministry of Health (MOH) and Health Sciences Authority (HSA) have developed and published the Artificial Intelligence in Healthcare Guidelines.
- AI in medical devices is regulated by the HSA. AI-powered tools that meet the definition of a medical device under the Health Products Act 2007 are subject to regulatory oversight, including registration and quality assurance requirements.
- The HSA has published the *Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach*, including how AI/ML-based tools are classified and assessed. Singapore is also exploring the regulatory sandbox approach to facilitate innovation while managing risks.

Financial services regulation and guidance

- The Monetary Authority of Singapore (MAS) has issued AI-specific guidance for the financial sector, notably the FEAT principles—Fairness, Ethics, Accountability and Transparency—for the use of AI and data analytics in financial services. While not legally binding, these principles help firms assess and manage AI risks, including in areas like credit scoring, fraud detection, and customer profiling.
- In March 2024, MAS also published an information paper on Cyber Risks Associated with Generative AI, highlighting risks like data leakage, prompt injection attacks, model hallucination, and over-reliance on Gen AI outputs. The paper provides risk mitigation strategies such as enhanced governance, prompt controls, and monitoring mechanisms, and underscores the importance of human oversight.
- MAS supports responsible AI use through the Veritas Initiative, which provides toolkits and methodologies to help financial institutions implement FEAT principles in a measurable and verifiable manner. Key deliverables include fairness assessment metrics, ethics and accountability implementation checklists, and model governance frameworks. The initiative aims to promote trust in AI by operationalising responsible AI practices, encouraging consistency across the industry, and enabling firms to demonstrate that their AI-driven decisions are fair and transparent. One such example is Project MindForge, which focuses on the risks and opportunities of Generative AI (Gen AI) in financial services. Its goals are to create a framework for the responsible use of Gen AI and to promote innovation that tackles industry challenges and improves risk management.

AI in South Africa

Overview

- The South African government (spearheaded by the Department of Communications and Digital Technologies) has published a *National Artificial Intelligence Policy Framework (October 2024)*, aiming to position South Africa as a leader in AI innovation while promoting responsible and inclusive use of AI. The policy emphasises ethical AI systems, talent development, and leveraging AI to address developmental challenges.
- South Africa has endorsed the Africa Declaration on Artificial Intelligence (2025), which emphasises ethical and inclusive AI principles, including references to data sovereignty, ethics, and diverse cultural contexts across Africa.
- The Film and Publication Board (FPB) has conducted research on regulating generative AI for misinformation/disinformation but has not published final regulations.
- South Africa's G20 Presidency has placed national emphasis on digital inclusion, ethical AI, and digital public infrastructure, reflecting its broader commitment to global digital equity as well as strong governmental support for AI-driven economic development and the need for inclusive digital infrastructure.

AI Laws

- South Africa does not currently have a standalone, overarching AI law.
- Governance relies on a combination of sectoral regulations (healthcare, financial services), the Protection of Personal Information Act (POPIA), E*lectronic Communications and Transactions Act* (ECTA), and common law principles.
- The National Artificial Intelligence Policy Framework (2024) proposes guiding principles on issues such as data governance, transparency, ethics, and fair competition and is intended as a precursor to more formal legislative or regulatory measures.

Data protection law and guidance

- Data protection in South Africa is primarily governed by the Protection of Personal Information Act, 2013 (POPIA):
  - Key principles include lawfulness, minimality, transparency, and accountability in processing personal information, which is broadly defined and includes both natural and juristic persons (i.e. incorporated entities such as companies).
  - POPIA limits solely automated decision-making with legal consequences or substantial effects (section 71). Certain automated decisions may require additional safeguards or justification, though further guidance is still evolving.
- The Information Regulator oversees POPIA enforcement. Organisations developing or utilising AI must comply with POPIA's requirements on obtaining consent or other lawful justifications, protecting data, and upholding data subject rights such as access and objection.
- Enforcement has primarily been through compliance notices and recommendations rather than fines, however, no action by the Information Regulator for AI usage has been publicised to date.

HR, employment, and discrimination

- The Constitution of South Africa prohibits unfair discrimination. Discrimination protection is robustly addressed by the *Employment Equity Act*, and *Promotion of Equality and Prevention of Unfair Discrimination Act*, collectively protecting against discrimination on grounds including race, gender, disability, sexual orientation, religion, culture, and language.
- No specific regulatory guidance on AI in the employment and discrimination context has yet been issued, but the use of AI in recruitment, staff management, or automated performance assessments must ensure compliance with existing discrimination laws and regulations.

Medical devices / healthcare

- South Africa's health sector is broadly overseen by the National Department of Health.
- Where AI-powered software or devices meet the definition of a "medical device", they may fall under the *Medicines and Related Substances Act* and need licensing or registration (enforced through the South African Health Products Regulatory Authority).
  - It is not yet fully clear how SAHPRA classifies and evaluates "software as a medical device" or advanced AI solutions.
- The Health Professions Council of South Africa (HPCSA) sets standards of professional conduct for healthcare practitioners. The HPCSA's *draft Ethical Guidelines on the Use of Artificial Intelligence* (2024) outline proposed expectations for safety, accountability, and patient-centricity. The draft Guidelines:
  - Provide that AI must be patient-centred and integrated responsibly into clinical workflows, minimising risks of over-reliance on automated tool
  - Stress the importance of patient confidentiality, safe deployment, oversight by qualified professionals, and compliance with privacy legislation, and, once final, may require informed patient consent for AI-driven diagnostic or treatment support systems
  - Urges caution regarding biases in training data

Financial services regulation and guidance

- The financial sector is regulated by various laws as well as the Financial Sector Conduct Authority (FSCA) and the Prudential Authority (a division of the South African Reserve Bank (SARB)).
- No standalone AI-specific regulatory instrument exists, however, standard consumer protection duties will apply. Institutions using AI must comply with broad obligations set out in, for example, the *Financial Advisory and Intermediary Services (FAIS) Act, Financial Intelligence Centre Act* (FICA), and POPIA's data protection requirements. "Treating Customers Fairly" principles mean AI systems must not result in discriminatory or unfair customer outcomes.
- The FSCA has highlighted AI-driven risks (such as model bias, explainability gaps, and data privacy concerns) in its consumer protection work.
- The FSCA and PA have confirmed they are working on a joint standard looking at AI use by financial institutions as part of their regulatory roadmap.

AI in the United Kingdom

Overview

- The government is taking forward a number of recommendations from an AI Opportunities Action Plan that look to enable and embrace AI.
- The government is not proposing to introduce comprehensive AI legislation.
- The data protection regulator, the Information Commissioner's Office (ICO), has provided extensive guidance on developing and using AI.
- There has been some ICO enforcement but at present fines have been used sparingly.

AI Laws

- No comprehensive AI law has been proposed.
- The government may consult on a law to impose obligations on the most powerful models.
- The government has consulted on an exception to copyright law for text and data mining for commercial activities (including training generative AI models).
- The government has proposed making the creation of sexually explicit deepfakes of adults a criminal offence (the law already covers creating images of children)
- Regulation-making powers to make rules for products with intangible components (like AI) are likely to be introduced.
- The Automated Vehicles Act 2024 will create an authorisation regime for automated vehicles when brought into force.

Data protection law and guidance

- The UK GDPR remains very close to the EU GDPR:
  - Key principles include fairness, transparency, and accuracy.
  - A lawful basis is needed for any processing of personal data, and a specific condition must be met to process special category data.
  - There is currently a default prohibition on solely automated decisions with significant effects.
- The ICO has looked to provide a range of resources to help organisations innovate responsibly, including an innovation advice service.
- The ICO has published guidance on AI and data protection, an AI and data protection risk toolkit, guidance on explaining decisions made with AI, and guidance on biometric data.

- Enforcement has generally been limited to reprimands or enforcement notices – a fine has been issued to Clearview AI, which was successfully appealed (though a further appeal from the ICO is ongoing).

HR, employment, and discrimination

- Article 14 European Convention on Human Rights (protection from discrimination) (Human Rights Act allows ECHR rights to be enforced in the UK courts)
- Equality Act 2010 includes protection against discrimination (direct and indirect), as well as harassment and victimisation – the following characteristics are protected:
  - Age
  - Disability
  - Gender reassignment
  - Marriage and civil partnership
  - Pregnancy and maternity
  - Race
  - Religion or belief
  - Sex
  - Sexual orientation
- The Equality and Human Rights Commission has provided guidance on AI and equality for public sector bodies.
- Litigation has been brought alleging that facial recognition checks required to access a work app were racially discriminatory, while in a separate case, the Court of Appeal found police use of automated facial recognition breached human rights and equality laws.

Medical devices / healthcare

- Medical devices (included software) are subject to the Medical Devices Regulations 2002, which impose a range of safety and conformity obligations.
- The Medicines & Healthcare products Regulatory Agency (MHRA) has provided updated guidance on software and AI as a medical device.
- The MHRA launched an 'AI Airlock' to provide a specific regulatory sandbox for AI as a Medical Device.

Financial services regulation and guidance

- The Financial Conduct Authority (FCA) has set out how it will use the current regulatory framework to regulate AI – key regulation includes:
  - Overarching requirements such as the Principles for Business and Threshold Conditions
  - More specific rules and guidance such as the Senior Management Arrangements, Systems and Controls (SYSC) sourcebook
  - The cross-cutting Consumer Duty.
- The Prudential Regulation Authority has highlighted the potential implications of widespread AI adoption in financial services, particularly concerning financial stability.
- The FCA has launched an AI Lab, to provide a pathway for the FCA, firms and wider stakeholders to engage in AI-related insights, discussions and case studies.
- The Bank of England has also established an AI consortium to provide a platform for engagement on AI in UK financial services.

AI in the United States

Overview

- On 23 January 2025 President Trump issued an Executive Order (Removing Barriers to American Leadership) that rolled back all policies, directives, regulations, orders and other actions taken pursuant to Biden's Executive Order from October 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence).
- The policy stated in Trump's Executive Order is for the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security.
- Within 180 days of Trump's Executive Order (mid-July 2025), a task force is to develop and submit to Trump an action plan to achieve this policy.
- In the US, laws can be enacted at the Federal, State and local level, adding to the potential complexity of governing AI. The US does not have comprehensive AI legislation nor data privacy legislation at the Federal level. Generally, new laws are being enacted at the State-level.

AI Laws

- Colorado enacted the first broad AI law which is focused on algorithmic discrimination and imposes obligations on the AI developer and deployers for high-risk AI systems. The Colorado Attorney General will have exclusive authority to enforce it. Enacted in May 2024, it will be effective in February 2026, but there are indications that the law may be amended before going into effect.
- California has enacted a handful of laws related to AI, including a law that requires the developers of generative AI solutions to disclose the data used by the developer to train the solution. This law will take effect on 1 January 2026.
- The new federal law known as the TAKE IT DOWN Act makes it illegal to "knowingly publish" or threaten to publish intimate images without a person's consent, including AI-created "deepfakes." Websites and social media companies must remove such material within 48 hours of notice from a victim, and they must also take steps to delete duplicate content. Several states have adopted laws prohibiting "deep fakes," digital replicas and use of likeness, and transparency requirements, including California and Tennessee. In addition, several states have laws that require disclosures to consumers when interacting with AI systems or receiving other communications that are AI generated.

- At the Federal level, there are numerous existing laws that can be applied to AI use cases, especially as it relates to discrimination or consequential decisions related to consumers including those enforced (e.g., CFPB, DOJ, FTC, EEOC). Each AI use case, especially those impacting consumers, need to be reviewed against this backdrop. Currently enforcement has been limited.

Data protection law and guidance

- By the end of 2025, there will be 16 states that have comprehensive privacy laws in effect. Many of these laws continue the U.S. tradition of "opt-out" privacy, including a specific opt-out right with respect to the use of AI for certain rights (criminal justice, education, employment, financial services, health insurance, housing, and access to basic necessities such as food and water). Certain states, most notably California, continue to pursue legislation that impacts AI use cases in the name of data privacy.
- In addition to the state data privacy laws, the Health Insurance Portability and Accountability Act 1996 (HIPAA) also has an impact on the use of protected health information in certain AI use cases.

HR, employment, and discrimination

- There is no specific federal law regulating AI in the workplace. However, the existing employment laws remain applicable. In addition, several states have passed laws applicable to the use of AI in employment practices.
- At the local level, New York City Local Law 144 places limits on the use of automated employment decisions tools regulation, which requires posting of annual audits. There has been no enforcement action.
- There have been a few enforcement actions, including one instance where the employer's AI tool allegedly discriminated based on age and gender. Interestingly, the AI tool provider is also included in this suit and potentially faces liability – in addition to the employer.

Medical devices / healthcare

- The Food and Drug Administration (FDA) has proposed a framework for AI/ML enabled medical devices, and provides a list of AI/ML enabled medical devices that are authorized for marketing in the US.
- See also comments related to protected health information above.

Financial services regulation and guidance

- In the US, the insurance sector is governed by State law. As of March 2025, 24 states have adopted, in some form, the National Association of Insurance Commissioners' model AI bulletin (Use of Artificial Intelligence Systems by Insurers). Four other states have issued insurance-specific laws or regulations concerning AI use in the insurance industry. Several other states are considering or have laws pending also relevant to the insurance business with certain states focused on methods of testing the algorithms and data for unfairly discriminatory outcomes.
- As it relates to the broader financial services markets, the existing regulatory agencies (e.g., FINRA, SEC, Federal Reserve, OCC, FDIC) have been issuing guidance, and in some cases, there has been limited enforcement based on existing regulations.
- On 16 October 2024, the New York Department of Financial Services (DFS) issued guidance raising awareness about combatting cybersecurity risks arising from AI used by DFS licensees, such as insurers and virtual currency businesses.

Contacts

Australia

Lisa Fitzgerald
Partner, Melbourne
Tel +61 3 8686 6088
lisa.fitzgerald@nortonrosefulbright.com

Annie Haggar
Partner, Canberra
Tel +61 2 6110 3046
annie.haggar@nortonrosefulbright.com

Georgina Hey
Partner, Sydney
Tel +61 2 9330 8210
georgina.hey@nortonrosefulbright.com

Canada

Imran Ahmad
Senior Partner, Canadian Head of Technology and Canadian Co-Head of Cybersecurity and Data Privacy, Toronto
Tel +1 416 202 6708
imran.ahmad@nortonrosefulbright.com

China

Frank Liu
Partner
Tel +86 186 0218 2228
frank.liu@shanghaipacificlegal.com

Johnny Liu
Senior Associate, Shanghai
Tel +86 21 6086 0192
johnny.liu@shanghaipacificlegal.com

Xiaodi Ding
Senior Associate, Shanghai
Tel +86 21 608 60126
xiaodi.ding@shanghaipacificlegal.com

Shibin Zhao
Senior Associate, Shanghai
Tel +86 21 6137 7005
email@nortonrosefulbright.com

France

Nadege Martin
Partner, Paris
Tel +33 1 5659 5374
nadege.martin@nortonrosefulbright.com

Laura Helloco
Associate, Paris
Tel +33 1 5659 5058
laura.helloco@nortonrosefulbright.com

Germany

Christoph Ritzer
Partner, Frankfurt
Tel +49 69 5050 96241
christoph.ritzer@nortonrosefulbright.com

Natalia Filkina
Senior Associate, Frankfurt
Tel +49 69 5050 96270
natalia.filkina@nortonrosefulbright.com

Hong Kong

Justin Davidson
Partner, Hong Kong
Tel +852 3405 2426
justin.davidson@nortonrosefulbright.com

Stanely Ng
Associate, Hong Kong
Tel +852 3405 2337
stanley.ng@nortonrosefulbright.com

Italy

Veronica Pinotti
Partner, Milan
Tel +39 02 8635 9440
veronica.pinotti@nortonrosefulbright.com

Martino Sforza
Partner, Milan
Tel +39 02 8635 9441
martino.sforza@nortonrosefulbright.com

Patrizia Pedretti
Senior Associate, Milan
Tel +39 02 8635 9442
patrizia.pedretti@nortonrosefulbright.com

The Netherlands

Jurriaan Jansen
Partner, Amsterdam
Tel +31 20 462 9381
jurriaan.jansen@nortonrosefulbright.com

Singapore

Jeremy Lua
Special Counsel, Singapore
Tel +65 6309 5336
jeremy.lua@nortonrosefulbright.com

Terence De Silva
Associate, Singapore
Tel +65 6309 5331
terence.desilva@nortonrosefulbright.com

South Africa

Allison Williams
Director, Durban
Tel +27 31 582 5655
allison.williams@nortonrosefulbright.com

Tristan Marot
Senior Associate, Johannesburg
Tel +27 11 685 8915
tristan.marot@nortonrosefulbright.com

United Kingdom

Marcus Evans
Partner, London
Tel +44 20 7444 3959
marcus.evans@nortonrosefulbright.com

Rosie Nance
Senior Knowledge Lawyer, London
Tel +44 20 7444 5615
rosie.nance@nortonrosefulbright.com

United States

Chuck Hollis
Head of Artificial Intelligence, United States, St. Louis
Tel +1 404 443 2147
chuck.hollis@nortonrosefulbright.com

Sue Ross
Senior Counsel, New York
Tel +1 212 318 3280
susan.ross@nortonrosefulbright.com

NORTON ROSE FULBRIGHT

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 3500 lawyers and other legal staff based in Europe, the United States, Canada, Latin America, Asia, Australia, Africa and the Middle East.

nortonrosefulbright.com