

C L I F F O R D
C H A N C E

AI LEGISLATION TO WATCH IN 2023-2024

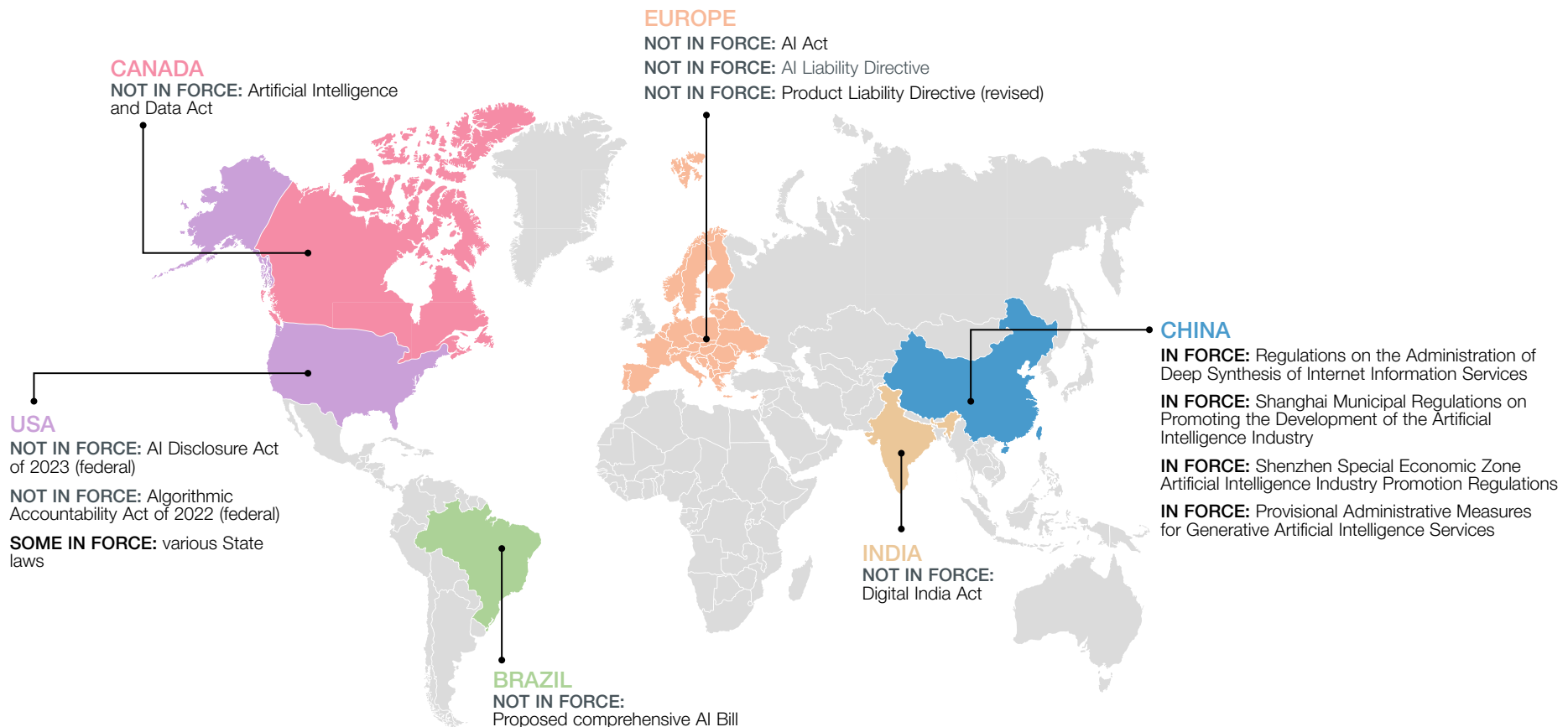
AI LEGISLATION TO WATCH IN 2023-2024

As Artificial Intelligence (AI)-powered technologies advance and proliferate, countries around the globe are responding by evolving their AI legislation, policies and strategies. A range of existing laws already apply to the development and use of AI, including privacy, cyber, intellectual property, antitrust, consumer protection and employment laws, as well as sector-specific and technology-targeting legislation. More recently, countries have begun adopting laws, proposals and bills that specifically focus on regulating AI.

This table identifies key laws, proposals and bills focused on AI in a range of jurisdictions.

Note: This table is not an exhaustive overview of AI-focused laws, proposals or bills and it is not globally comprehensive. In particular, the table does not include: (i) laws that can apply to AI but do not focus on AI specifically or primarily, such as privacy laws; (ii) legislation that relates to the use of AI solely in the context of specific technologies (for example, automated driving systems or recommender systems) or in specific sectors (such as legislation that regulates AI use in healthcare only); (iii) laws that establish AI task forces or working groups; (iv) laws that apply only to governmental bodies or state agencies; (v) policy documents, consultations, white papers, ethical frameworks, and similar; (vi) aspirational or non-binding commitments and codes of conduct, (such as commitment by the G7 group of leading democratic countries to create an international code of conduct for AI); or (vii) in-progress initiatives, which may lead to legislation but do not currently involve a legislative proposal, such as the U.S. Congressional hearings in September 2023. For the U.S., the table includes a sample of legislation which is not representative of, or in proportion to, the full spectrum of proposed and enacted bills, particularly for the more active states such as California, New York, New Jersey and Illinois. For the EU, the table includes only EU-wide legislation, and not Member State initiatives.

AI-FOCUSED LAWS AND BILLS – GLOBAL MAP OF KEY EXAMPLES



AI-FOCUSED LAWS AND BILLS – US: EXAMPLES OF FEDERAL, STATE, AND LOCAL AI LEGISLATION

FEDERAL

NOT IN FORCE: AI Disclosure Act of 2023

NOT IN FORCE: Algorithmic Accountability Act of 2022

COLORADO

IN FORCE: INSURANCE (S. 21-169, GEN. ASSEMB., 2021 – 2022 REG. SESS. (COLO. 2021))

NEW YORK

NOT IN FORCE: EMPLOYMENT (S. 5641, 2023–2024 Leg. Sess. (N.Y. 2023))

IN FORCE: EMPLOYMENT (Local Law No. 144 of 2021, N.Y.C.)

NOT IN FORCE: EMPLOYMENT (Gen. Assemb. A7859, 2023-2024 (N.Y. 2023))

VERMONT

NOT IN FORCE: EMPLOYMENT (H. 114, Gen. Assemb., 2023–2024 Sess. (Vt. 2023))

MASSACHUSETTS

NOT IN FORCE: TECHNOLOGY (S. 31, 193rd Gen. Ct. (Mass. 2023))

NOT IN FORCE: EMPLOYMENT (H. 1873, 193rd Gen. Ct. (Mass. 2023))

PENNSYLVANIA

NOT IN FORCE: TECHNOLOGY (H. 49, Gen. Assemb., 2023–2024 Reg. Sess. (Pa. 2023))

NEW JERSEY

NOT IN FORCE: FINANCIAL SERVICES, HEALTHCARE, AND INSURANCE (S. 1402, 220th Leg., 2022–2023 Sess. (N.J. 2022))

NOT IN FORCE: EMPLOYMENT (A4909 and S1926, 220th Leg., Gen. Assemb., 2022-2023 Sess (N.J. 2022))

WASHINGTON, DC

NOT IN FORCE: TECHNOLOGY (B. 25-114, 2023 Council (D.C. 2023))

MARYLAND

IN FORCE: EMPLOYMENT (H. 1202, 2020 Gen. Assemb., Reg. Sess. (Md. 2020))

ILLINOIS

IN FORCE: EMPLOYMENT (Artificial Intelligence Video Interview Act)

NOT IN FORCE: EMPLOYMENT (H. 3773, 103rd Gen. Assemb. (Ill. 2023))

CALIFORNIA

NOT IN FORCE: CIVIL RIGHTS; EMPLOYMENT AND HOUSING (Assemb. B. 331, 2023–2024 Leg., Reg. Sess. (Cal. 2023))

THE WIDER GLOBAL AI LEGAL AND POLICY ENVIRONMENT

AI-RELEVANT RULES AND GUIDANCE ARE INCREASING GLOBALLY... HERE ARE SOME EXAMPLES

EU

- Various member state national AI strategies and legislative proposals/consultations
- AI Pact / AI Code of Conduct (EU-US)
- Digital Services Act
- Proposed Cyber Resilience Act
- GDPR

UK

- National AI Strategy, Action Plan and White Paper
- AI Standards Hub
- National Data Strategy and UK data protection laws
- ICO AI and Data Protection Toolkit
- AI Safety Summit (November 2023)

USA

- White House Office of Science and Technology Policy: Blueprint for an AI Bill of Rights
- Senate Majority Leader Chuck Schumer / Center for Strategic and International Studies: SAFE Innovation Framework
- Senators Blumenthal and Hawley bipartisan framework for AI
- National Institute of Standards and Technology: AI Risk Management Framework
- Federal Trade Commission: AI guidance and proposed rulemaking
- California Consumer Privacy Act, as amended by the California Privacy Rights Act

MIDDLE EAST

- UAE National AI Strategy
- Saudi Arabia SDAIA AI Ethics Principles
- Digital Dubai Authority AI Ethics Principles & Guidelines

CHINA

- Personal Information Protection Law
- Cybersecurity Law
- National Information Security Standardisation Technical Committee (TC260) guidelines on AI ethics
- Office of the State Council Opinion on Strengthening the Ethics and Governance of Science and Technology

JAPAN

- Social Principles of Human-Centric AI
- AI Governance in Japan Report by Ministry of Economy, Trade and Industry

SINGAPORE

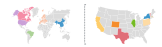
- MAS's Veritas Toolkit 2.0 and Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of AI and Data Analytics
- PDPC's Model AI Governance Framework
- IMDA's AI Verify
- Personal Data Protection Act

AUSTRALIA

- Safe and Responsible AI in Australia consultation and discussion paper
- Australia's AI Action Plan

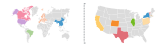
MULTI-JURISDICTIONAL

- G7 "Hiroshima" process on regulatory cooperation (in progress)
- UNESCO Recommendation on AI Ethics
- OECD Recommendation on AI
- APEC Business Advisory Council report on AI
- African Commission on Human and Peoples' Rights (ACHPR) Resolution on AI



Legislation/ Bill	Applicability	Summary*	In force?
Europe			
<p>EU</p> <p><u>AI Regulations (the EU AI Act)</u>¹</p>	<ul style="list-style-type: none"> Providers placing on the market or putting into service AI systems in the EU (even if a provider is not established in the EU), and third country providers where their systems' output is used in the EU. Users of AI systems located in the EU, and third country users where their systems' output is used in the EU. Potentially, providers placing on the market or putting into service outside the EU "prohibited" AI systems, where the provider (or distributor) is located in the EU (Parliament's position). Other actors throughout the AI value chain, such as importers and distributors of AI systems, authorised representatives in the EU etc., with specific provisions also defining when another operator / person should be deemed the provider. 	<ul style="list-style-type: none"> Regulates the placing on the market, putting into service and use of certain AI systems in the EU (with certain specific exclusions, e.g., systems developed or used exclusively for military purposes, and cases of very limited application). Contains rules aimed at ensuring the development and deployment of human-centric, secure, trustworthy and ethical AI, including, e.g., rules around AI systems' safety, transparency and data governance. Follows a risk-based approach, e.g.: <ul style="list-style-type: none"> Prohibits certain AI uses/practices. Imposes specific requirements for 'high-risk' AI systems (including conformity assessment, risk and quality management, data governance, documentation and record-keeping, registration, transparency, human oversight, accuracy, robustness and cybersecurity, and potentially such matters as a 'fundamental rights impact assessment'). Sets out specific transparency requirements for certain AI systems. Also, there are discussions and developments on the specific regulation of 'general purpose AI systems' / 'foundation models' / 'generative AI' systems, as well as around potential general principles for AI systems. Sets out other rules regarding market monitoring, market surveillance, regulatory sandboxes, governance, registration on a database, etc. Provides for significant penalties in case of infringement. 	No

¹ This is the initial proposal of the European Commission (21 April 2021). Please see [here](#) for the Council's 'General Approach' (6 December 2022) and [here](#) for the Parliament's position (14 June 2023). Trilogues began in June 2023 and are ongoing, as the EU lawmakers negotiate and seek to agree a final text. The information in the table is mainly based on the Commission's initial proposal.



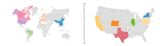
Legislation/ Bill	Applicability	Summary*	In force?
EU <u>AI Liability Directive</u> ²	Providers and users of certain AI systems (each as defined in the EU AI Act – see above), including operators / persons deemed to be the provider under the EU AI Act.	<ul style="list-style-type: none"> • Aims to harmonise certain EU Member State rules on compensation for damages caused by an AI system. It is a ‘minimum harmonisation’ directive. Being a directive, it needs to be transposed by the EU Member States into national law. • Applies to non-contractual fault-based civil liability claims for compensation of the damage caused by an AI system. • Seeks to facilitate the access to relevant information and substantiation of claims by requiring Member States to empower courts to order the disclosure of evidence re a high-risk AI system suspected of having caused damage in certain circumstances. • Establishes a conditional and rebuttable presumption of causality between the defendant’s fault (as further described in the proposed directive) and the output produced by an AI system or the failure of an AI system to produce an output. • Includes a review process, notably to consider possible future no-fault (strict) liability rules for claims against the operators of certain AI systems and the need for specific insurance coverage. • Closely connected to the proposed EU AI Act (see above). 	No

² This is the initial proposal of the European Commission (28 September 2022). Pending the EU Council’s and the European Parliament’s respective positions, and ensuing trilogues. At this stage, the information in the table is essentially based on the Commission’s initial proposal.



Legislation/ Bill	Applicability	Summary*	In force?
<u>EU Product Liability Directive (revised)</u> ³	<ul style="list-style-type: none"> Manufacturers of defective products and manufacturers of components of defective products including an economic operator having substantially modified the product. Possibly EU importers and EU authorised representatives of manufacturers, fulfilment service providers, distributors, online platforms etc. 	<ul style="list-style-type: none"> Revises the 1985 Product Liability Directive to update it and address technological developments, including re AI. Being a directive, it needs to be transposed by EU Member States into national law. Sets out common rules on the liability of operators for certain damage suffered by natural persons caused by 'defective products', i.e. material losses resulting from: (a) death or personal injury; (b) harm to or destruction of property (with exceptions, e.g., re the defective product itself or property used exclusively for professional purposes); or (c) loss or corruption of data not used exclusively for professional purposes (although point (c) has reportedly been one of the discussion points). Updates key notions to reflect the digital age and developments, for instance re AI, e.g.,: 'product', to explicitly cover software and digital manufacturing files; 'component', to include digital services integrated in or interconnected with a product; and 'defectiveness', to take account of the ability of products to continue learning after deployment or questions of interconnectedness. Seeks to ensure there is always an EU business that can be held liable for products bought from non-EU manufacturers and includes provisions to define when a given operator qualifies as the manufacturer. Requires Member States to empower courts to order the disclosure of relevant evidence for plausible claims. Also seeks to ease the burden of proof through rebuttable presumptions of 'defectiveness' or causal link e.g., where a claimant faces excessive difficulties due to technical or scientific complexity. Provides certain defences / exemptions from liability but adapts them to take account of the capacity of products to change after being placed on the market or put into service (e.g., an operator should not be exempted on the ground that the defectiveness did not exist at that point or came into being afterwards where the defectiveness is due to software, including updates or upgrades – or a lack of updates or upgrades necessary to maintain safety – or to certain 'related services' within the 'manufacturer's control'); provides restrictions on contractual limitations of liability, envisages the potential joint and several liability of economic operators, details specific limitation periods, etc. 	No

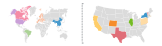
³ This is the initial proposal of the European Commission (28 September 2022). Please see [here](#) for the position reportedly adopted by the Council and constituting its mandate for negotiations with the European Parliament (position adopted on 14 June 2023). Pending the Parliament's position, and ensuing trilogues. At this stage, the information in the table is essentially based on the Commission's initial proposal.



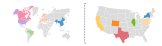
Legislation/ Bill	Applicability	Summary*	In force?
Americas			
USA Federal <u>Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022)</u>	“Covered entities” (persons, partnerships, or corporations under the jurisdiction of the FTC) that deploy an “augmented critical decision process and/or exceed certain revenue or equity value thresholds or possess / use above a certain volume of identifying information of consumers, households, or consumer devices.”	<ul style="list-style-type: none"> • Would direct the FTC to develop regulations and provide guidance on performing impact assessments of “automated decision systems” (including “any system, software, or process (including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques and excluding passive computing infrastructure) that uses computation, the result of which serves as a basis for a decision or judgment”) used by “covered entities” to make “critical decisions” affecting a consumer’s life. • Would require transparency and annual reporting by covered entities. • Would require covered entities to attempt to eliminate or mitigate “likely material negative impacts”. 	No
USA Federal <u>AI Disclosure Act of 2023</u>	<ul style="list-style-type: none"> • Generative artificial intelligence. 	<ul style="list-style-type: none"> • Generative artificial intelligence will include on any output it generates the following: “Disclaimer: this output has been generated by artificial intelligence.” • Violation of this requirement will be deemed a violation of FTC regulations regarding unfair or deceptive acts or practices. • The FCT will be able to impose penalties under the Federal Trade Commission Act for any violations. 	No
USA California <u>Assembly Bill 331</u>	<ul style="list-style-type: none"> • Deployers (entities that use an automated decision tool (“ADT”) to make a “consequential decision”). • Developers of ADTs. 	<ul style="list-style-type: none"> • Would require deployers and developers of ADTs to perform an impact assessment, including among other things an analysis of potential adverse impacts (on the basis of protected characteristics) and a description of safeguards to address “reasonably foreseeable” risks of algorithmic discrimination. • Would require deployers to notify natural persons re ADTs being used to make, or being a controlling factor in making, “consequential decisions”. • Would require deployers and developers to establish and maintain a governance program with respect to risks of algorithmic discrimination. 	No



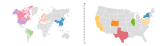
Legislation/ Bill	Applicability	Summary*	In force?
USA Colorado <u>Senate Bill 21-169</u> <u>(Protecting Consumers from Unfair Discrimination in Insurance Practices)</u>	Insurers authorized to do business in the State of Colorado.	<ul style="list-style-type: none"> Prohibits insurers from using any external consumer data and information source, algorithm or predictive model in a way that results in unfair discrimination (against protected categories) in insurance practices. Directs the regulator to work with stakeholders, then adopt rules for how insurers test their 'big data' systems for unfair discrimination, demonstrate such testing, and remedy any unfairly discriminatory impact. 	Yes
USA Washington, DC <u>B25-114 (Stop Discrimination by Algorithms Act of 2023)</u>	Service providers, data brokers, individuals and other "covered entities" that make or rely on algorithmic determinations by a service provider and that exceed certain revenue thresholds or possess or control above a certain volume of personal information of D.C. residents.	<ul style="list-style-type: none"> Would prohibit use of algorithmic decision-making (utilizing AI, machine learning or similar techniques) on the basis of protected traits in a discriminatory manner or otherwise makes "important life opportunities" unavailable. Would require annual audit and reporting of such algorithmic determinations and related practices and implementation of "reasonable measures" to address risks of an "unlawful disparate impact" (based on discrimination). Would require notice to individuals about the use of personal information in such algorithmic determinations. For violations, would provide for civil penalties (monetary fines) and punitive damages in a civil action. 	No
USA Illinois <u>Public Act 101-0260; House Bill 2557 (Artificial Intelligence Video Interview Act)</u>	Employers that use AI to analyze video interviews of applicants for employment positions based in Illinois.	<ul style="list-style-type: none"> Requires disclosure by employers to applicants of use of AI analysis and obtaining consent from applicants to such use. Limits video-sharing and requires video deletion upon request by applicants. Requires collection and annual reporting of demographic data from employers relying solely on AI analysis for selection of applicants for an in-person interview. 	Yes



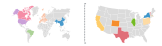
Legislation/ Bill	Applicability	Summary*	In force?
USA Illinois <u>House Bill 3773 (amends Illinois Human Rights Act and Consumer Fraud and Deceptive Business Practices Act)</u>	Employers that use predictive data analytics in employment decisions.	<ul style="list-style-type: none"> • Would prohibit consideration of an applicant's race (or zip code when used as a proxy) when employers use "predictive data analytics" (i.e., "automated machine learning algorithms for the purpose of statistically analyzing a person's behavior"), resulting in refusal to hire, harassment, or acting on the basis of unlawful discrimination, with respect to recruitment, hiring, promotion, privileges or conditions of employment, among other things. • Would prohibit the use of information that assigns specific risk factors to a consumer's race (or zip code) when persons or entities rely on predictive data analytics to determine the consumer's creditworthiness, resulting in rejection of credit. Would require procedures to be devised to ensure that such information is not considered. 	No
USA Maryland <u>House Bill 1202 (Labor and Employment – Use of Facial Recognition Systems – Prohibition)</u>	Employers that use facial recognition technology during employment interviews.	<ul style="list-style-type: none"> • Prohibits use of facial recognition services during employment interviews to create a "facial template" (without consent). • Requires signed applicant waivers to be obtained by employers. 	Yes
USA Massachusetts <u>Bill S.31 (Act drafted with the help of ChatGPT to regulate generative AI models like ChatGPT)</u>	Companies operating a "large-scale generative artificial intelligence model".	<ul style="list-style-type: none"> • Would require adherence to certain operating standards, such as "reasonable" security measures for training data, "regular" risk assessments, and informed consent from individuals for data collection/use/disclosure. • Would require registration with the Attorney General of the State of Massachusetts. 	No



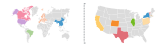
Legislation/ Bill	Applicability	Summary*	In force?
<p>USA Massachusetts</p> <p><u>Bill H.1873 (Act preventing a dystopian work environment)</u></p>	Employers, and vendors acting on behalf of employers.	<ul style="list-style-type: none"> • Would require notice to employees from employers or vendors (acting on behalf of employers) of use of “automated decision systems” (“ADSs”), “algorithmic impact assessments” for certain uses, and record-keeping of ADS. Would provide employee rights to request certain information from employers or vendors—including information about use of ADS. • Would require review and adjustment of employment-related decisions or ADS outputs based on inaccurate data. • Would prohibit certain uses of ADSs (e.g., outputs regarding a worker’s health must not be a basis for employment-related decisions). 	No
<p>USA New Jersey</p> <p><u>Bills No. A4909 and S1926</u></p>	Users and vendors of automated employment decision tools in the State of New Jersey.	<ul style="list-style-type: none"> • Would prohibit the sale (or offer for sale) of “automated employment decision tools” without a “bias audit” within the past year and ongoing, free annual bias audit services. • Would require notice to be provided to a candidate about use of automated employment decision tools to screen the candidate. • For violations, would provide for civil penalties (monetary fines). 	No
<p>USA New Jersey</p> <p><u>Bill No. S1402</u></p>	<ul style="list-style-type: none"> • Certain financial services institutions involved in loans / credit • Insurance companies licensed, registered, or authorized in the State of New Jersey. • Healthcare providers. 	<ul style="list-style-type: none"> • Would prohibit use of ADSs to discriminate against persons or groups in a protected class, in relation to participation or eligibility for certain loan / credit terms or conditions, certain insurance coverage terms, or healthcare services, in each case at a disproportionate rate to those who are not members of the protected class. 	No
<p>USA New York</p> <p><u>Assembly Bill A567 / Senate Bill S5641</u></p>	Employers implementing or using an automated employment decision tool to select job candidates within the State of New York.	<ul style="list-style-type: none"> • Would establish criteria for use of “automated employment decision tools,” including requirements for conducting and publishing an annual “disparate impact analysis” when such tools are used by employers to select job candidates. 	No



Legislation/ Bill	Applicability	Summary*	In force?
USA New York <u>Assembly Bill A7859</u>	Employers and employment agencies using automated employment decision tools ("AEDTs").	<ul style="list-style-type: none"> Requires employers and employment agencies using AEDTs (derived from "machine learning, statistical modeling, data analytics or artificial intelligence") for employment screening, to notify candidates about the use of AEDTs in their assessment or evaluation, the qualifications and characteristics used by AEDTs, the type of data collected, the source(s) of the data and the applicable data retention policy applicable to such AEDTs. The notice must be made no less than 10 business days before use of any AEDTs to allow candidates to request "an alternative selection process or accommodation". 	No
USA New York City <u>Local Law 144 of 2021 (Automated Employment Decision Tools)</u>	Employers and employment agencies using automated employment decision tools ("AEDTs").	<ul style="list-style-type: none"> Requires employers and employment agencies using AEDTs (derived from "machine learning, statistical modeling, data analytics or artificial intelligence") to conduct independent "bias audits" within one year prior to use and publish a summary of the results. The results must satisfy certain minimum criteria. Requires notice to candidates or employees residing in New York City about the use of AEDTs in assessments or evaluations for hiring or promotion. The notice must provide instructions to request "an alternative selection process or a reasonable accommodation under other laws, if available." For violations, provides a civil penalty. 	Yes (enforcement began July 2023).
USA Pennsylvania <u>House Bill 49 (Act providing for artificial Intelligence registry)</u>	Businesses operating artificial intelligence systems within the Commonwealth of Pennsylvania.	<ul style="list-style-type: none"> Would provide for the Department of State of the Commonwealth of Pennsylvania to establish both a hard copy and online registry for businesses that operate AI systems. 	No



Legislation/ Bill	Applicability	Summary*	In force?
<p>USA Vermont</p> <p><u>House Bill H.114 (Act restricting electronic monitoring of employees and employment-related automated decision systems)</u></p>	Employers that use electronic monitoring of employees or automated decision systems for employment-related decisions.	<ul style="list-style-type: none"> • Would prohibit certain uses of “automated decision systems” by employers (e.g., relying solely on outputs for employment-related decisions) and would prohibit any facial, gait or emotion recognition technology. • Would require impact assessments of automated decision systems. • Would provide employees with a right to request access to data related to employees that was produced or utilized by automated decision systems used by employers. 	No
<p>Canada</p> <p><u>Proposal for an Artificial Intelligence and Data Act (AIDA), part of Bill C-27</u></p>	Businesses operating in Canada.	<ul style="list-style-type: none"> • The Artificial Intelligence and Data Act (“AIDA”) aims to ensure accountability for risks associated with high-impact AI systems used in the course of international and interprovincial trade and commerce. • The following activities may be regulated: system design and development, making a system available for use, and managing the operations of a system. • The AIDA would create new criminal offences to directly prohibit and address specific behaviours of concern, such as using unlawfully obtained personal information to design an AI system, and making available an AI system that could cause harm or damage. It would establish a new AI and Data Commissioner, who would be empowered to ensure compliance. 	No
<p>Brazil</p> <p><u>Proposed comprehensive AI Bill</u></p>	Companies that develop, implement or use AI technology in Brazil.	<ul style="list-style-type: none"> • The proposed law is general in nature and sets out a wide range of rights and responsibilities for users and organisations developing and deploying AI systems in Brazil. • Its proposals include a requirement for risk assessments to be conducted before any AI system is put on the market in Brazil, creation of a new regulatory body to enforce the law, instating a list of high-risk systems and a prohibition of specific types of AI systems, imposition of an obligation on providers and users of AI systems to establish governance structures, creation of an obligation for reporting incidents and breaches and a protective system of civil liability. 	No



Legislation/ Bill	Applicability	Summary*	In force?
Asia-Pacific			
<p>China</p> <p><u>Regulations on the Administration of Deep Synthesis of Internet Information Services</u></p> <p>Translation from Chinalawtranslate here.</p>	Providers and users of deep synthesis services in China	<ul style="list-style-type: none"> • The regulations focus on ‘deep fake’-type use cases and generative AI-based chat services such as ChatGPT. Deep synthesis is defined as “technology utilising generative and/or synthetic algorithms, such as deep learning and virtual reality, to produce text, graphics, audio, video, or virtual scenes”. • Obligations for providers include verification of user identity and monitoring for certain types of information, prohibition of misinformation, facilitation of user appeals and complaints. App stores and other distribution platforms are required to review deep synthesis services for safety and to address violations. • Services that generate or edit biometric information, or certain services with implications for national security / national interests are subject to additional requirements including security assessments. Notification and consent are required where services edit biometric information. 	Yes
<p>China</p> <p><u>Shanghai Municipal Regulations on Promoting the Development of the Artificial Intelligence Industry</u></p> <p>Translation from Georgetown University here.</p>	Providers of AI products and services within the administrative divisions of Shanghai	<ul style="list-style-type: none"> • The regulations are wide-ranging. They set out a framework for industrial development, local governance and research, and obligations covering the inspection and testing, certification and accreditation of, and standards for, the AI industry, as well as quality supervision of related products. • The regulations adopt a risk-based approach, imposing more extensive scrutiny of high-risk AI products and services. However, it is not yet clear what categories of products and services will be classified as high-risk. • The regulations set out detailed prohibitions for entities that carry out AI R&D (for example, prohibiting the provision of products and services that endanger national security or infringe on personal privacy). 	Yes



Legislation/ Bill	Applicability	Summary*	In force?
<p>China</p> <p><u>Shenzhen Special Economic Zone Artificial Intelligence Industry Promotion Regulations</u></p> <p>Translation from Georgetown University here.</p>	<p>Within the Shenzhen Special Economic Zone</p>	<ul style="list-style-type: none"> The Shenzhen regulations provide for a wide range of industrial policy and R&D support measures. From a regulatory perspective, they adopt a risk-based approach where “<i>High-risk AI applications shall adopt a regulatory model of ex ante assessment and risk warning. Low and moderate-risk AI applications shall adopt a regulatory model of ex ante disclosure and post facto tracking.</i>” The regulations contain prohibitions, for example, regarding providing products and services that endanger national security or public interests, adversely affect commercial orders, or violate personal rights and interests, including privacy. 	<p>Yes</p>
<p>China</p> <p><u>Provisional Administrative Measures for Generative AI Services</u></p> <p>Translation from Stanford University here.</p>	<p>Any person who provides services to the public in China by utilising the generative AI products it develops and/or uses.</p>	<ul style="list-style-type: none"> The measures mandate steps to prevent algorithmic discrimination based on various characteristics and prohibit discriminatory content generation. The measures clarify how certain privacy and intellectual property protections apply to generative AI. The measures would require security assessment declarations to be submitted to the cyberspace administration authorities before services enabled by generative AI are offered publicly. 	<p>Yes</p>
<p>India</p> <p><u>Proposed Digital India Act, 2023</u></p>	<p>It will be possible to determine the DIA’s applicability once the draft text is published in the coming weeks / months.</p>	<ul style="list-style-type: none"> The Ministry of Electronics and Information Technology has published a proposal for a Digital India Act 2023 (“DIA”), which would replace the Information Technology Act 2000 and sit alongside the proposed Personal Data Protection Bill. The DIA proposal sets out to define and regulate high-risk AI systems through a rules-based and institutional quality testing framework, and to cover algorithmic accountability, AI-based ad targeting, content moderation and the ethical use of AI-based tools to protect the rights or choices of users. 	<p>No</p>

CLIFFORD CHANCE

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

Content relating to jurisdictions where Clifford Chance does not have an office is based on the firm's experience as international counsel representing clients in their business activities in such jurisdictions from the firm's international offices and should not be construed as constituting legal advice. Clifford Chance is not permitted to advise on such laws and should such advice be required Clifford Chance would work alongside a domestic law firm.

Content relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers.