INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

AI and the Legal Profession: Czech, EU, and U.S. Insights on Regulation and Ethics

January 28, 2025

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

Speakers

- Alžběta Dvořáková Recová, CBA Representative in Brussels
- Adam Felix, Attorney, Felix and Associates
- Elaine F. Harwell, Partner, Procopio, Cory, Hargreaves & Savitch, LLP
- Myriah V. Jaworski, Member, Clark Hill
- Jiří Novák, Partner, Sokol, Novák, Trojan, Doleček a partneři, advokátní kancelář s.r.o.
- Leslie Stevens, Chief Privacy Officer, Agilent Technologies, Inc.

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

European Union’s approach to AI Regulation

Presented by Alžběta Dvořáková Recová

Recent practical example

Were there any increases in court fees in Czech Republic in 2024?

ChatGPT said:

There are changes to court fees in the Czech Republic in 2024. The Chamber of Deputies passed an amendment to the Court Fees Act which increased individual fees by between 20% and 100%.

You said:

But there is no such information published on the website of the Ministry of Finance, nor in any official source. Could you add relevant sources supporting your argument?

ChatGPT said:

Sorry for the confusion. Having re-examined the available information, I must state that no direct increase in court fees has been announced or approved for 2024 in the Czech Republic.

EU discussions prior to the publication of the AI regulation

- Commission´s Communication “Artificial Intelligence for Europe” of April 2018.
- Ethics guidelines for trustworthy AI produced in April and June 2019 by the High-Level Expert Group on Artificial Intelligence (HLEG).
- Commission Report on safety and liability implications of AI, the Internet of Things and Robotics of February 2020
- Coordinated plan on AI with the Member States to align policies so as to foster the development and use of AI in Europe.
- February 2020, the Commission published a White Paper on AI setting out policy options for a regulatory framework and an approach towards investment.
- 2020 – public consultations
- April 2021 – publication of the proposal for AI regulation

Main objectives of the EU AI regulatory initiatives

(a) the effective enforcement of rules of existing EU law meant to protect safety and fundamental rights and avoid illegal discrimination by ensuring the relevant documentation for the purposes of private and public enforcement of EU rules;

(b) legal certainty for businesses that are marketing their AI-enabled products or using such solutions in the EU as regards the rules applicable to such products and services;

(c) to prevent/minimise significant risks for fundamental rights and safety;

(d) harmonised framework to reduce burdensome compliance costs derived from legal fragmentation, which could jeopardise the functioning of the Single Market;

(e) European governance structure on AI in the form of a framework for cooperation of national competent authorities in order to develop needed capacity;

(f) to facilitate the emergence of a market for trustworthy AI

Further reading

- Inception impact assessment
- Communication “Artificial Intelligence for Europe”
- AI HLEG deliverables
- Report on safety and liability implications of AI, the Internet of Things and Robotics
- Coordinated Plan on Artificial Intelligence
- White Paper on Artificial Intelligence: a European approach to excellence and trust
- AI Act Impact Assessment
- AI Act legislative procedure

The EU AI Act (regulation 2024/1689 laying down harmonised rules on artificial intelligence)

- The AI Act is the first-ever comprehensive legal framework on AI worldwide;
- was published in the Official Journal of the European Union on 12 July 2024;
- entered into force on 1 August 2024;
- will be fully applicable as from August 2026, with some exceptions:

    - prohibitions will take effect after six months,
    - the governance rules and the obligations for general-purpose AI models become applicable after 12 months,
    - and the rules for AI systems - embedded into regulated products - will apply after 36 months.

Broad definition of AI covered by the AI Act

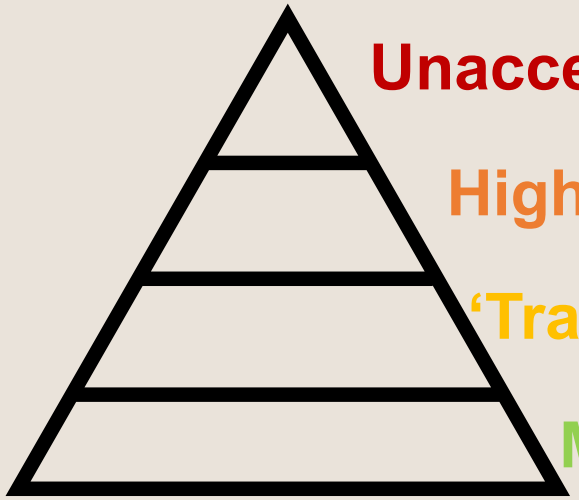
Art. 3 para 1 + recital 12

‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments

What are the main goals of the EU AI Act? To:

- address risks specifically created by AI applications;
- prohibit AI practices that pose unacceptable risks;
- determine a list of high-risk applications;
- set clear requirements for AI systems for high-risk applications;
- define specific obligations for deployers and providers of high-risk AI applications;
- require a conformity assessment before a given AI system is put into service or placed on the market;
- put enforcement in place after a given AI system is placed into the market;
- establish a governance structure at the European and national level.

The risk-based approach – 4 categories:



Unacceptable risk — **Prohibited**

High risk — **Permitted** subject to compliance with AI requirements and ex-ante conformity assessment

‘Transparency’ risk — **Permitted** but subject to information/transparency obligations

Minimal or no risk — **Permitted** with no restrictions, voluntary codes of conduct possible

Unacceptable risk

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

•A very limited set of particularly harmful uses of AI that contravene EU values because they violate fundamental rights and **will therefore be banned**:

- **Exploitation of vulnerabilities of persons, manipulation and use of subliminal techniques;**
- **Social scoring** for public and private purposes;
- **Individual predictive policing** based solely on profiling people;
- **Untargeted scraping** of internet or CCTV for facial images to build-up or expand databases;
- **Emotion recognition in the workplace and education institutions**, unless for medical or safety reasons (i.e. monitoring the tiredness levels of a pilot);
- **Biometric categorisation** of natural persons to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation. Labelling or filtering of datasets and categorising data in the field of law enforcement will still be possible;
- **Real-time remote biometric identification in publicly accessible spaces by law enforcement,** subject to narrow exceptions and prior authorisation by a judicial or independent administrative authority (or 24h after in urgent cases).

The Commission is supposed to issue guidance on the prohibitions prior to their entry into force on 2 February 2025 but it is not yet available.

High-risk AI systems

High-risk: A limited number of AI systems defined in the proposal, potentially creating an adverse impact on people's safety or their fundamental rights (as protected by the EU Charter of Fundamental Rights), are considered to be high-risk. Annexed to the Act are the lists of high-risk AI systems, which can be reviewed to align with the evolution of AI use cases.

Article 6 of the AI Act describes the thresholds that lead to an AI system being “high risk.”

AI systems can classify as high-risk in two cases:

• the AI system is embedded as a safety component in products covered by existing product legislation (Annex I) or constitute such products themselves. This could be, for example, AI-based medical software.
• the AI system is intended to be used for a high-risk use case, listed in an Annex III to the AI Act. The list includes use cases from in areas such as education, employment, law enforcement or migration.

Examples for high-risk use cases as defined in Annex III

- AI systems used as safety components in certain **critical infrastructures** for instance in the fields of road traffic and the supply of water, gas, heating and electricity;
- **AI systems used in education and vocational training,** e.g. to evaluate learning outcomes and steer the learning process and monitoring of cheating;
- **AI systems used in employment and workers management** and access to self-employment, e.g. to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
- **AI systems used in the access to essential private and public services** and benefits (e.g. healthcare), **creditworthiness evaluation** of natural persons, and risk assessment and pricing in relation to **life and health insurance**;
- AI systems used in the fields of **law enforcement**, migration and **border control**, insofar as not already prohibited, as well as in administration of **justice** and **democratic processes**;
- AI systems used for **biometric identification, biometric categorisation and emotion recognition,** when not prohibited!

High-risks AI systems and Justice

Specific high-risk use case in Annex III (8) point a):

- AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution.

<u>Clarifications in recital 61:</u>

- The classification of AI systems as high-risk should not, however, extend to AI systems intended for purely ancillary administrative activities that do not affect the actual administration of justice in individual cases, such as anonymisation or pseudonymisation of judicial decisions, documents or data, communication between personnel, administrative tasks.
- **AI can support the decision-making power of judges or judicial authority, but should not replace it: the final decision-making must remain a human-driven activity.**

High-risks AI systems and Law Enforcement

Specific high-risk use case in Annex III (6):

Law enforcement, in so far as their use is permitted under relevant Union or national law AI systems intended to be used by or on behalf of law enforcement authorities, or by Union institutions, bodies, offices or agencies in support of law enforcement authorities:

a) assess the risk of a natural person becoming **the victim of criminal offences**;
b) as polygraphs or similar tools;
c) to evaluate **the reliability of evidence** in the course of the **investigation or prosecution of criminal offences;**
d) for assessing the risk of a natural person **offending or re-offending not solely on the basis of the profiling** of natural persons as referred to in Article 3(4) of Directive (EU) 2016/680, or to assess **personality traits and characteristics or past criminal behaviour of natural persons or groups**;
e) for the **profiling of natural persons** as referred to in Article 3(4) of Directive (EU) 2016/680 in the course of the **detection, investigation or prosecution of criminal offences.**

Remote biometric identification

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

- Differs from unlocking a smartphone or for verification or authentication at border crossings to check a person's identity against his/her travel documents
- The use of **real-time remote biometric identification in publicly accessible spaces** (i.e. facial recognition using CCTV) for law enforcement purposes **is prohibited**. Member States can introduce exceptions in the following cases:

- Law enforcement activities related to **16 specified very serious crimes;**
- Targeted search for specific victims, abduction, trafficking and sexual exploitation of human beings, and missing persons; or
- The prevention of threat to the life or physical safety of persons or response to the present or foreseeable threat of a terrorist attack.

Any exceptional use would be subject to **prior authorisation by a judicial or independent administrative authority** whose decision is binding. In case of urgency, approval can be granted within 24 hours; if the authorisation is rejected all data and output must be deleted.
It would need to be preceded by **prior fundamental rights impact assessment** and should be **notified to the relevant market surveillance authority and the data protection authority**. In case of urgency, the use of the system may be commenced without registration.

The use of AI systems for **post remote biometric identification** (identification of persons in previously collected material) of persons under investigation requires **prior authorisation** from a judicial authority or an independent administrative authority, as well as notification to the relevant data protection and market surveillance authority.

Obligation for high-risk AI systems providers

Before **placing a high-risk AI system on the EU market**:

- **conformity assessment** (data quality, documentation and traceability, transparency, human oversight, accuracy, cybersecurity and robustness);
- has to be **repeated if the system or its purpose are substantially modified**;
- safety components of products covered by sectorial Union legislation will always be deemed high-risk when subject to third-party conformity assessment under that sectorial legislation;
- all biometric systems, regardless of their application, will require third-party conformity assessment;
- providers have to **implement quality and risk management systems** to ensure their compliance with the new requirements and minimise risks for users and affected persons, even after a product is placed on the market.
- high-risk AI systems that are deployed by public authorities or entities acting on their behalf will have to be **registered in a public EU database**, unless those systems are used for law enforcement and migration (in this case restricted access).
- Non-EU providers have to appoint **authorized representatives in the EU**

Obligations for high-risk AI systems deployers

- Operate high-risk AI system in accordance with **instructions of use**
- Ensure **human oversight**: persons assigned must have the necessary competence, training and authority
- **Monitor** for possible risks and **report problems and any serious incidents** to the provider or distributor
- Public authorities to **register the use in the EU database**
- **Inform affected workers** and their representatives
- **Inform people** subjected to decisions taken or informed by a high-risk AI system and, upon request, provide them with **an explanation**
- **Conduct fundamental rights impact assessment by certain deployers** (public authorities or private operators providing public services, as well as operators providing high-risk AI systems that carry out credit worthiness assessments or price and risk assessments in life and health insurance + notify the national authority of the results, usually together with data protection IA)

Compliance throughout the lifecycle of the AI system

- Regular audits and post-market monitoring;
- reporting of any serious incidents or breaches of fundamental rights obligations;
- authorities may give exemptions for specific high-risk AI systems to be placed on the market;
- national authorities have access to the information needed to investigate whether the use of the AI system complied with the law.

Filtering mechanism

Filter mechanism: Will exclude systems from the high-risk list that:

- **perform narrow procedural tasks (NEEDS TO BE DEFINED)**
- **improve the result of previous human activities,**
- **detect decision-making patterns without influencing human decisions**
- **do purely preparatory tasks**

BUT Profiling of natural persons is always considered to be high-risk

Recital 61: AI can support the decision-making power of judges or judicial authority, but should not replace it: the final decision-making must remain a human-driven activity. This does not apply to high-risk systems intended for purely ancillary administrative activities not affecting the actual administration of justice in individual cases, e.g. anonymisation/pseudoanymisation of judicial decisions, documents or data, communication between personnel, administrative tasks

Other two categories:

Specific transparency risk: the AI Act introduces specific transparency requirements for certain AI applications, for example where there is a clear risk of manipulation (e.g. via the use of chatbots) or deep fakes. Users should be aware that they are interacting with a machine.

Minimal risk: The majority of AI systems can be developed and used subject to the existing legislation without additional legal obligations. Voluntarily, providers of those systems may choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

Enforcement

National authorities overseeing and enforcing rules for AI systems

---

x the **EU level** is responsible for governing general-purpose AI models.

European Artificial Intelligence Board
(representatives of Member States and the EDPS)
The AI Office

+ two advisory bodies:
the **Scientific Panel** and the **Advisory Forum**.

Infringements

Member States will have to lay down fines for infringements
Thresholds to be taken into account:

- **Up to €35m or 7%** of the total worldwide annual turnover for infringements **on prohibited practices or non-compliance** related to requirements on data;
- **Up to €15m or 3%** of the total worldwide annual turnover for **non-compliance with any of the other requirements** or obligations of the Regulation;
- **Up to €7.5m or 1.5%** of the total worldwide annual turnover for the **supply of incorrect, incomplete or misleading information** to notified bodies and national competent authorities in reply to a request;

The threshold would be the lower of the two for SMEs and the higher for the rest of companies.

The Commission can also enforce the rules on providers of general-purpose AI models by means of fines, taking into account the following threshold:

- **Up to €15m or 3%** of the total worldwide annual turnover for **non-compliance with any of the obligations** or measures requested by the Commission under the Regulation.

The EDPS will have the power to impose fines on EU institutions and bodies in case of non-compliance.

Summary of lobbying efforts

Coordinated approach of the CCBE and national Bar Associations throughout the whole legislative process

The outcomes for the justice area are mostly in line with the position paper of the CCBE which has been concretised during the legislative process and wording of the articles, BUT right to a human judge – only included in the recital (not the article of the the Regulation)

Further involvement in the implementation phase and preparation of guidance if required!

The Czech Bar Association lobbyied on the specification of the list of exceptions for prohibited practice – the use of real-time biometric identification by the enforcement authorities in regards to serious offences – now the participation in organized crime group is not a stand-alone condition but must be linked to one of the offences listed in the Annex IIa of the AI Act.
Recitals 18, 19, Article 5 (1)(iii)

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

List of criminal offences referred to:

terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs and psychotropic substances; illicit trafficking in weapons, munitions and explosives; murder, grievous bodily injury; illicit trade in human organs and tissue; illicit trafficking in nuclear or radioactive materials; kidnapping, illegal restraint and hostage-taking; crimes within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft/ships; rape; environmental crime; organised or armed robbery; sabotage; **participation in a criminal organisation involved in one or more offences listed above.**

Stakeholders reactions

EDPS

https://www.edps.europa.eu/press-publications/press-news/blog/its-hatched-our-plan-artificial-intelligence-eu-institutions_en

https://www.edps.europa.eu/press-publications/press-news/press-releases/2023/edps-final-recommendations-ai-act_en

https://www.crowell.com/en/insights/client-alerts/european-data-protection-supervisor-releases-new-opinion-on-the-eus-proposed-ai-act

https://www.edps.europa.eu/system/files/2025-01/2024-12-18_submission_ai_board_on_prohibitions_en.pdf

Stakeholders reactions

FRA

https://fra.europa.eu/en/project/2023/assessing-high-risk-artificial-intelligence

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-artificial-intelligence-summary_en.pdf

Member States

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

The reaction from EU member states has been somewhat mixed, reflecting **varying national priorities, economic interests, and approaches to innovation and regulation among countries**.

Strongly in favour of robust regulation
- France, Germany, Netherlands (with necessary flexibility of regulation), Italy

Concerns for over-regulation or compliance burdens
- Estonia, Greece, Czechia, Poland, Hungary

Global competitiveness arguments
- Finland, Sweden

Proportionality and flexibility
- Luxembourg, Denmark

Stakeholders reactions - businesses

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

- **Mixed Reactions**:
  - **Support**: Many businesses, especially those with a strong presence in Europe, support the **ethical principles** of the AI Act, particularly around transparency, fairness, and human rights **(Microsoft**, **Google and IBM)**. They have supported the idea of AI regulation but have lobbied for more clarity, flexibility, and certain adjustments to ensure that the regulatory framework does not become overly restrictive.
  - **Innovation Concerns**: Businesses in AI-related sectors, particularly startups, are concerned that the regulations might create barriers to entry and stifle innovation, especially for small firms that may struggle to comply with complex compliance requirements. Companies like **Amazon** and **Facebook (Meta)** have highlighted the need to find a balance between ensuring safety and not hindering technological progress.
  - **Call for Clarity**: Companies **(Apple** and **Google)** are asking for clearer definitions and more flexible provisions that can accommodate the fast-paced nature of AI development.
  - **Global Coordination**: **Microsoft**, **Google**, **IBM**, **Meta (Facebook)**, **Amazon**, **Nvidia**, **Apple**, and **SAP**—have all stressed the importance of **global alignment** and **harmonization** in AI regulation. They argue that a fragmented regulatory landscape could create operational complexities, hinder innovation, and make it more difficult to build trust in AI systems across different regions.

US Stakeholders

- **Concerns Over Extraterritorial Reach**: From a U.S. perspective, stakeholders are concerned about the **extraterritorial scope** of the AI Act, particularly how it may affect U.S.-based companies that offer AI services or products in the EU market. The Act's strict requirements on high-risk AI systems could compel U.S. firms to adjust their operations, particularly in areas like transparency and accountability, which could add costs and complexity. The European Union's **AI Act regulate also companies that are not based within the EU territory**, provided their **products or services** have an **impact** on people or businesses **within the EU**.
- **Collaboration and Competition**: While some U.S. companies have expressed support for clear global standards on AI, at the same time they worry that the EU's regulatory approach could hinder global competition and give European companies an advantage.

Further reading

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/responsible-ai
https://azure.microsoft.com/en-us/products/ai-services/ai-content-safety/
https://lanternstudios.com/insights/blog/microsofts-commitment-to-responsible-ai/
https://ai.google/static/documents/EN-AI-Principles.pdf
https://policies.google.com/technologies/anonymization?hl=en
https://safety.google/privacy/data/
https://static.googleusercontent.com/media/publicpolicy.google/el//resources/eu_ai_opportunity_agenda_en.pdf
https://aif360.res.ibm.com/
https://about.fb.com/news/2024/06/building-ai-technology-for-europeans-in-a-transparent-and-responsible-way/
https://developer.amazon.com/support/legal/alexa_dpa
https://dig.watch/updates/apple-intelligence-expands-to-the-eu-amid-regulatory-changes
https://ecnl.org/news/packed-loopholes-why-ai-act-fails-protect-civic-space-and-rule-law

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

Council of Europe Framework Convention on Artificial Intelligence

Opened for signature on 5 September 2024 (Signatories: Andorra, Georgia, Iceland, Montenegro, Norway, Republic of Moldova, San Marino, United Kingdom, EU, Israel, USA)

The Framework Convention was drafted by CAI and the 46 member states of the Council of Europe, with the participation of all observer states: Canada, Japan, Mexico, the Holy See and the United States of America, as well as the European Union, and a significant number of non-member states: Australia, Argentina, Costa Rica, Israel, Peru and Uruguay.

+ 68 international representatives from civil society, academia and industry involved

The treaty will enter into force on the first day of the month following three months after five signatories, including at least three Council of Europe Member States, have ratified it.

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

What does the COE Framework Convention require?

Fundamental principles

Human dignity and individual autonomy, Equality and non-discrimination, Respect for privacy and personal data protection, Transparency and oversight, Accountability and responsibility, Reliability, Safe innovation

Remedies, procedural rights and safeguards

•Document the relevant information regarding AI systems and their usage and to make it available to affected persons;

•Enable people concerned to challenge the decision(s) made through the use of the system or based substantially on it, and to challenge the use of the system itself;

•Effective possibility to lodge a complaint to competent authorities;

•Provide effective procedural guarantees, safeguards and rights to affected persons in connection with the application of an artificial intelligence system

•Provision of notice that one is interacting with an artificial intelligence system and not a human being.

What does the COE Framework Convention require?

Risk and impact management requirements

•Carry out risk and impact assessments in respect of actual and potential impacts on human rights, democracy and the rule of law, in an iterative manner;

•Establishment of sufficient prevention and mitigation measures as a result of the implementation of these assessments;

•Possibility for the authorities to introduce ban or moratoria on certain application of AI systems (“red lines”).

•Further reading: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

Aspect	EU AI Act	Council of Europe AI Convention
Jurisdiction	EU member states and EEA countries	International, open to Council of Europe Member States as well as Third Countries
Legally Binding	Yes, binding regulation within the EU	Treaty, binding only after ratification by countries
Approach	Risk-based regulation (high-risk vs low-risk AI)	Ethical guidelines, human rights, and democracy-centered
Focus	Regulation of AI systems for safety and trust	Ethical use of AI, human rights, and global cooperation
Enforcement	Compliance through national authorities, fines	Encourages implementation through national laws; no direct enforcement
Main Goal	Safe and ethical use of AI in the EU	Global ethical standards for AI, human rights protection

Justice is blind, and if we’re not careful, AI might make it deaf and mute too—while still charging us for the upgrade.“

— *Tech-Satirist*

"AI might one day replace lawyers, but can it bluff its way through a trial when it forgot to prepare? I think not!“

— *Proudly Human Attorney*

"I trust AI in court about as much as I trust autocorrect to get my name right.“

— *Michael...or is it Mitchell?*

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

AI Regulation and Legislation in the United States

Presented by
- Elaine F. Harwell, Procopio
- Myriah Jaworski, Clark Hill

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

What is Artificial Intelligence (Legal definitions)

No general or accepted common definition of AI.

AI System: An engineered or machine based system that can, for a given set of objectives, generate outputs such as **predictions, recommendations or decisions** influencing real or virtual environments. (NIST, AI RMF 2023)

Artificial Intelligence: is a term used to describe machine-based systems designed to simulate human intelligence to perform tasks, such as analysis and decision-making, given a set of human-defined objectives. (NAIC Model Bulletin 9/2023)

Artificial Intelligence: means a machine-based system that infers, from the input it receives, how to generate outputs that can influence physical or virtual environments. The artificial intelligence may do this to achieve explicit or implicit objectives. (CPPA Proposed Text of Regulations, 11/22/2024)

Algorithm: means a computational or machine learning process that augments or replaces human decision-making in insurance operations that impact consumers (Id.).

Algorithms & Predictive Models: means a process of using mathematical and computational methods that examine current and historical data sets for underlying patterns and calculate the probability of an outcome. (CO Insurance Law)

Automated decision tools: substantially assists or replace discretionary decisions (scores, classifications, rankings, simplified output criteria). (NY LL 144)

Automated Decisionmaking Technology: means any technology that processes personal information and uses computation to execute a decision, replace human decisionmaking, or substantially facilitate human decisionmaking. (CPPA Proposed Text of Regulations, 11/22/2024)

How is AI currently regulated in US?

Prong	Description

Existing Federal and State law authority	• **Existing federal (EEOC) authority under federal anti-discrimination law**
	  • iTutorGroup –EEOC 2022 complaint (EEOC), 2023 draft strategic enforcement plan
	  • Title VII of Civil Rights Act, Age Discrimination in Employment Act, Fair Housing, ADA etc.
	• **Federal Trade Commission – FTC Act Section 5, Fair Credit Reporting, Equal Credit Opportunity Act–**
	  • unfair or biased algorithms, deletion of models developed with improperly collected data
	  • "Keep Your AI Claims In Check" – blog
	• **Joint Commitment to AI Enforcement Letter - *DOJ, FTC, EEOC, CFPB – May 2023***
	• **Existing state regulatory authority under state anti-discrimination laws**
	  • New York State DFS – letter to insurers, AppleCard investigation
	  • California AG letter – health care decision making
	  • State Insurance Laws – Unfair Trade Practices, Rating Laws
	  • Colorado Division of Insurance – draft Algorithm and Predictive Model Governance Regulation (Feb. 2023)

New Laws – largely at State/City Level	• New York City Local Law 144: enacted and effective; Automated Employment Decision-making Tool (AEDT) • Colorado AI Act, California AI laws, Utah AI Policy Act (enacted 2024, effective 2026) • California CCPA/CPRA Proposed Risk Assessment regulations (Aug. 2023)
Industry Standards & Federal Initiatives	• NIST AI Risk Management Framework – Jan. 2023 • National Association of Insurance Commissioners – AI Principles, Bulletins • White House Blue Print for AI Bill of Rights, Biden Executive Order
Emerging Judicial Dictates/Caselaw	• Increase in Class Action filings alleging use of AI/ML led to discrimination or disparate impact • AI/ML derived property rights – IP, Copyright etc. - a lot of activity here.

Federal AI Activity

- President Trump in his first day in office revoked a 2023 Executive Order signed by Biden and signed a new Executive Order; “Removing Barriers to American Leadership in Artificial Intelligence”
  - “Sec. 2. Policy. It is the policy of the United States to sustain and enhance America’s global AI dominance in order to promote human flourishing, economic competitiveness, and national security.“
- Under Trump AI EO: All prior programs are ordered to be reviewed and reversed/adjusted if not in line with the one-sentence policy goal.
- By July 2025, White House policy staff will create an "action plan" describing how they will achieve the policy goal.

Notable State Legislation and Regulations (2024)

- Colorado: SB 24-205 (Colorado AI Act)
- California: CPPA Draft Regulations
- Illinois: HB 3773 (Governance of AI in consequential employment decisions)
- Minnesota: HF 4757 (Minnesota Consumer Data Privacy Act)
- Utah: SB 149 (Tech-specific directed at GenAI)

AI Lawsuits

- Defensible Use of AI Tools: Caselaw already exists
  - Wisconsin v. Loomis (Wisconsin State Supreme Court 2016)
    - Use of AI “risk assessment tool” known as COMPAS for sentencing of defendant
    - COMPAS report consists of a risk assessment designed to predict recidivism and a separate needs assessment for identifying program needs in areas such as employment, housing and substance abuse. The risk assessment portion of COMPAS generates risk scores displayed in the form of a bar chart, with three bars that represent pretrial recidivism risk, general recidivism risk, and violent recidivism risk. Each bar indicates a defendant's level of risk on a scale of one to ten.
  - Loomis lodged Due Process challenge to use of COMPAS in his sentencing
  - Holding: “. . . if used properly, observing the limitations and cautions set forth herein, a circuit court's consideration of a COMPAS risk assessment at sentencing does not violate a defendant's right to due process.”
    - **risk assessment tools must be constantly monitored and re-normed for accuracy due to changing populations and subpopulations.**

AI Lawsuits

- AI Lawsuits in Benefits/Insurance: Are they new? No.
  - Strawn v. Farmers Insurance Co. of Oregon (Oregon Sup. Ct. 2011) – systemic bad faith class action
    - Use of "cost-containment software" to evaluate personal injury protection claims
    - If a bill exceeded the preselected percentile, it was automatically reduced downwards. Farmers selected 80th percentile.
      - **"Although Farmers contended at trial (and still contends) that the EOB form constituted only a 'recommendation' from MMO as to reasonableness, claims adjusters were expected to follow the recommendation. The adjusters were downgraded if they departed from MMO's recommendations and were rewarded when they followed them. Thus, the 'recommendation' was, as a practical matter, the final determination of reasonableness."**
  - "That cutoff point, though profitable for Farmers, also yielded an increase in customer complaints."
  - Jury trial – compensatory damages, attys fees and $8M in punitive damages

AI Lawsuits

- AI Tools to deny claims/benefits
  - Huskey v. State Farm (ED. Il. Dec. 14, 2022) – alleged automated racial bias
  - Suzanne Kisting-Leung v. Cigna Health & Life Insurance Co. et. al. (ED Ca. 2023) - alleged wrongful denials
  - Estate of Gene B. Lokken et al. v. UnitedHealth Group, Inc. et al. (D. Mn. 2023) – medicare advantage/senior claims

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

Cybersecurity Legislation in the European Union

Presented by Dr. Adam Felix

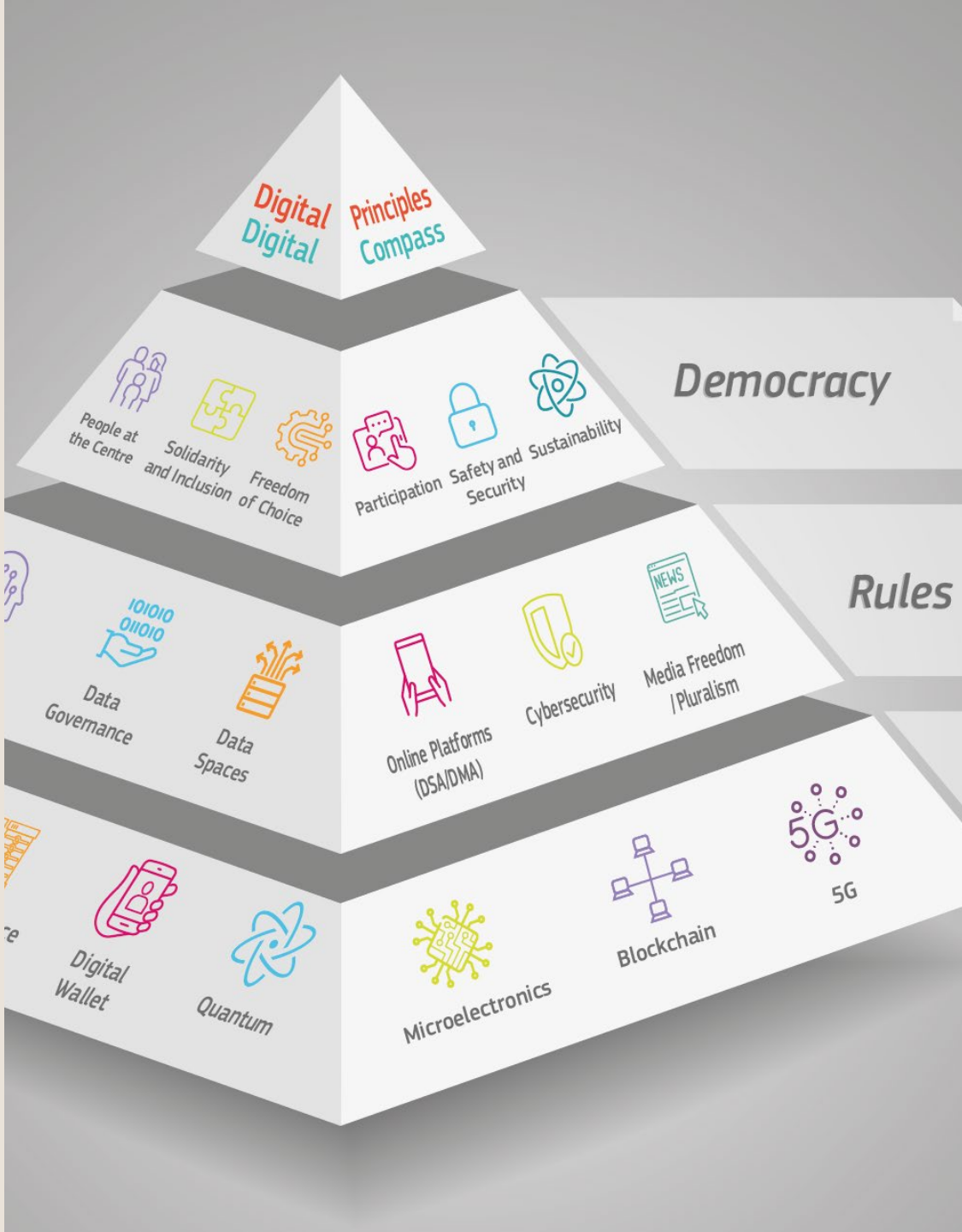
DIGITAL DECADE 2030

Europe aims to empower businesses and people in a human-centred, sustainable and more prosperous digital future.

- Skills
- Digital transformation of businesses
- Secure and sustainable digital infrastructures
- Digitalisation of public services

EU LEGISLATION

- Cybersecurity Act (CSA)
- Directive on measures for a high common level of cybersecurity across the Union (NIS 2)
- Resilience of Critical Entities Directive (CER)
- Cyber Resilience Act (CRA)
- Digital Operational Resilience Act (DORA)



DIGITALLY SECURE, INCLUSIVE, AND SUSTAINABLE SOCIETY

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

Czech Legal and Ethical AI Basics

Presented by Jiří Novák, Attorney at Law and Equity Partner at Sokol, Novák, Trojan, Doleček a partneři, advokátní kancelář s.r.o.

Czech Ethical Rules

- **Czech Act No. 85/1996 Coll, on the Legal Profession** (amendments in the legislative process): Microsoft Word - 1996-85 Sb. - zakon o advokacii - zn˙ní od 20.1.2024 (3)
- **Czech Ethical codex** Etický kodex (usnesení č. 1:1997 Věstníku).pdf
- **Opinion on the use of AI in the provision of legal services** (by the Board of Directors of CBA)

European Ethical Rules

- CCBE Charter of Core Principles of the European legal profession
- 2022 CCBE Guide on the use of Artificial Intelligence-based tools by lawyers and law firms in the EU(https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Reports_studies/EN_ITL_20220331_Guide-AI4L.pdf)
- 2020 CCBE Considerations on the Legal Aspects of Artificial Intelligence (https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf)
- (in preparation - CCBE Guidance on the use of Generative AI by lawyers)
- Use of Generative Artificial Intelligence (AI) by judicial professionals in a work related context (CoE) https://rm.coe.int/cepej-gt-cyberjust-2023-5final-en-note-on-generative-ai/1680ae8e01
- Resource Centre on Cyberjustice and AI (CoE) https://www.coe.int/en/web/cepej/resource-centre-on-cyberjustice-and-ai

Examples of AI use in legal practice:

- Drafting support tools (writing assistance, document assembly, tools for turning legal data and knowledge bases into text);
- Document analysis;
- Text retrieval and analysis of case law and legislation;
- Speech-to-text tools;
- Chatbots;
- Assistance in internal office administration.

Concerning generative AI, the European Legal Technology Associations (ELTA) report from 2023 suggests that 75% of surveyed lawyers use ChatGPT. Among the most common use cases were document summaries and producing non-legal content.

INTERNATIONAL LAW AND IMMIGRATION
CALIFORNIA LAWYERS ASSOCIATION

Ethical aspects of using generative AI by lawyers

- **The duty of competence** (to know what tool you work with)

- remote data processing (data protection, use of data for training)
- lack of transparency
- hallucinations
- bias

- **Lawyer-client confidentiality**
- **Lawyers responsibility for using AI**

Other International sources (maybe outdated):

[1] The Law Society of England and Wales: Generative AI – the essentials, 17 November 2023 https://www.lawsociety.org.uk/topics/ai-and-lawtech/generative-ai-the-essentials
[2] The State Bar of California (Standing Committee on Professional Responsibility and Conduct): Practical guidance for the use of generative artificial intelligence in the practice of law https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf
[3] The Florida Bar Proposed Advisory Opinion 24-1 Regarding lawyers' use of generative artificial intelligence – Official Notice: https://www.lawnext.com/wp-content/uploads/2024/01/FL-Bar-Ethics-Op-24-1.pdf
[4] Report and Recommendations of the New York State Bar Association Task Force on Artificial Intelligence, April 2024 https://fingfx.thomsonreuters.com/gfx/legaldocs/znpnkgbowvl/2024-April-Report-and-Recommendations-of-the-Task-Force-on-Artificial-Intelligence.pdf
[5] Guidelines on the use of generative AI in courts and tribunals – lawyers, Courts of New Zealand, December 2023 https://www.courtsofnz.govt.nz/assets/6-Going-to-Court/practice-directions/practice-guidelines/all-benches/20231207-GenAI-Guidelines-Lawyers.pdf

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

AI from an In House Perspective

Presented by: Leslie Stevens, Chief Privacy Officer, Agilent Technologies, Inc.

Ethical and Legal Concerns on AI for In House Counsel

- **AI Tool Approval**: Collaborate with IT to establish clear guidelines on approved AI tools.
- **Security Review**: Ensure AI tools undergo thorough InfoSec and legal reviews.
- **Data Protection**: Prohibit the use of your company's data to train public LLMs to safeguard sensitive information.
- **Compliance**: Understand and document high risk uses of AI specific to your business, in alignment with regulations that apply to your company and industry.
- **Transparency**: Maintain transparency in AI tool usage, consider where notice is required based on use cases for your business.
- **Gen AI Policy**: Develop a company policy on the appropriate use of Gen AI, addressing unique risks, and include it in company training.

Responsible Use of AI for In House Counsel

•**Document Drafting**: Quickly generate drafts for contracts, agreements, policies, procedures.

- *Data Protection*: Use approved and reviewed tools only.
- *Accuracy*: Use AI to suggest language, but always have a human review for accuracy.

•**Legal Research**: Efficiently gather and summarize relevant case law, statutes, and regulations.

- *Data Protection*: Access only reputable and secure legal databases.
- *Accuracy*: Cross-reference AI-generated summaries with primary sources.

Responsible Use of AI for In House Counsel

• **Compliance Monitoring**: Track regulatory changes to support compliance efforts.

- *Accuracy*: Implement a verification process to confirm AI findings with compliance colleagues.

•**Daily Communication**: Draft clear and concise responses to inquiries.

- *Data Protection*: Ensure use of approved/reviewed AI tools.
- *Accuracy*: Review AI-generated responses to ensure they meet legal requirements.

Responsible Use of AI for In House Counsel

•**Contract Review**: Identify key clauses and potential issues in contracts. Develop prompt playbook for your contract's teams.

- *Data Protection*: Use approved and reviewed tools only.
- *Accuracy*: Have legal professionals verify AI-identified issues and clauses.

•**Training and Development**: Create training materials and resources for your company.

- *Accuracy*: Regularly update training materials to reflect regulations, new case law etc.

INTERNATIONAL LAW AND IMMIGRATION

CALIFORNIA LAWYERS ASSOCIATION

THANK YOU!