Artificial Intelligence & Technology Law Updates

Newsletter [October-November'24]

NOVEMBER

International Law Updates

1. First Treaty on Artificial Intelligence Governance Reaches 37 Signatories

November 10, 2024

The Council of Europe has opened the world's first legally binding treaty on artificial intelligence, the Framework Convention on AI and Human Rights, Democracy, and the Rule of Law, for signature on September 5, 2024. Signed by several nations, including the UK, USA, and EU, the treaty ensures AI development aligns with human rights, democracy, and the rule of law through a comprehensive, technology-neutral framework covering the entire AI lifecycle. Negotiated by 46 Council of Europe members, the EU, and 11 non-members with input from various sectors, the treaty aims to promote innovation while mitigating risks. It will come into force once ratified by at least five signatories, including three Council of Europe member states. The treaty reached 37 signatories as of November 10, 2024.

Link - https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225

National Legal Updates (International Countries)

2. EU Published the General Purpose AI Draft Code

November 15, 2024

The European Union has published its first draft of a Code of Practice for General Purpose AI (GPAI) models, which provides guidelines for managing risks and compliance, with the aim of preventing penalties. This code is written by independent experts. The draft, which will be finalized by May 2025, targets advanced AI models like those from OpenAI, Google, Meta, and Anthropic (and possibly others in the future). Key areas covered include transparency (e.g., disclosing web crawlers used for training), copyright compliance, risk assessment (addressing concerns like cyber offenses, discrimination, and loss of control), and technical/governance risk mitigation. The code also emphasizes accountability within organizations, requiring ongoing risk assessments and consultation with external experts. Violations could result in penalties of up to €35 million or 7% of global annual profits. Stakeholders can submit feedback until November 28, 2024, to help shape the final regulations.

Link - https://digital-strategy.ec.europa.eu/en/library/first-draft-general-purpose-ai-code-practice-published-written-independent-experts

3. European Commission - Consultation on AI Act Prohibitions and AI System Definition Application of AI Systems and Prohibited AI Practices

November 13, 2024

On November 13, 2024, the European Commission launched a consultation process to develop guidelines on defining AI systems and prohibited practices under the EU AI Act (AIA), with the aim of helping businesses comply ahead of the Act's provisions coming into effect on February 2, 2025. The consultation focuses on prohibited AI practices like harmful manipulation, social scoring, and certain biometric uses, to protect individual autonomy and ensure consistent enforcement across the EU. Stakeholders, including AI providers, businesses, national authorities, and civil society, are invited to submit input, which will help shape the guidelines. The consultation is open until December 11, 2024, and the final guidelines are expected in early 2025.

Link - https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-ai-act-prohibitions-and-ai-system-definition

3. European Commission Announced Establishment of AI Factories

November 11, 2024

On November 11, 2024, the European Commission announced it had received seven proposals to establish AI factories across the EU, aimed at boosting AI innovation. These factories will utilize the EU's High-Performance Computing (HPC) network to create an ecosystem for training advanced AI models and solutions, integrating computing power, data, and talent. The proposals, submitted by 15 EU Member States and 2 associated states, reflect a strong interest in leveraging supercomputers for AI development. Key countries involved include Finland, Germany, Spain, and Italy, among others. An expert panel will evaluate the proposals, with the final selection expected in December 2024, and the AI factories are set to launch in early 2025.

Link - https://digital-strategy.ec.europa.eu/en/news/commission-receives-seven-proposals-ai-factories-which-will-boost-ai-innovation-eu

4. Texas Proposed Responsible AI Governance Bill – Inspired from EU AI Act

November 8, 2024

On November 8, 2024, Texas State Representative proposed the Texas Responsible AI Governance Act (TRAIGA), which aims to regulate high-risk AI systems (HRAIS). Inspired by the EU AI Act and Colorado's AI legislation, TRAIGA sets a framework for developers, distributors, and deployers of HRAIS to mitigate algorithmic discrimination risks. Key provisions include semi-annual impact assessments, detailed record-keeping, AI literacy training, consumer disclosures, and an AI risk management policy. The bill also proposes the creation of the Texas Artificial Intelligence Council to oversee AI ethics and governance. TRAIGA is set to be formally introduced in the 2025 legislative session and, if passed, would take effect on September 1, 2025.

Link - https://ibat.informz.net/ibat/data/images/AI-Bill.pdf

5. Canada Announced the Creation of Canada Artificial Intelligence Safety Institute
November 12, 2024

November 12, 2024

On November 12, 2024, Canada announced the creation of the Canadian Artificial Intelligence Safety Institute (CAISI), focused on improving AI safety and promoting responsible use. CAISI will address AI risks like disinformation, cybersecurity breaches, and election interference, as part of a broader CAD 2.4 billion investment in responsible AI development. The institute will collaborate with national and international partners, including the National Research Council and the Canadian Institute for Advanced Research, conducting research on AI risks and safety measures. This initiative complements Canada's existing AI strategies, including the Artificial Intelligence and Data Act and the Voluntary Code of Conduct.

Link - https://www.canada.ca/en/innovation-science-economic-development/news/2024/11/canada-launches-canadian-artificial-intelligence-safety-institute.html

6. South Korea Launches AI Safety Institute

November 27, 2024

On November 27, 2024, South Korea officially launched its AI Safety Institute in Pangyo, following the AI Seoul Summit in May, where nations including Korea and Britain adopted a joint declaration on safe, innovative, and inclusive AI. The institute will focus on researching risks related to AI, such as abuse and loss of control, while serving as a hub for collaboration between industry, academia, and research institutes. It will also engage in the international network of AI safety institutes to promote global discussions. The inaugural director is Kim Myuhng-joo, a professor at Seoul Women's University, who emphasized that the institute will support AI companies to minimize risks and enhance global competitiveness, rather than acting as a regulatory body. A consortium of 24 entities, including major tech companies like Naver, KT, and Kakao, as well as leading universities, will collaborate on AI safety research and policymaking. South Korea is also collaborating with Japan and Singapore to study AI behavior across different languages and cultural contexts.

Link - https://www.koreaherald.com/view.php?ud=20241127050025

OCTOBER

International Law Updates

1. OECD - G7 Toolkit for Artificial Intelligence in the Public Sector

October 15, 2024

On October 15, 2024, OECD published a Toolkit for Artificial Intelligence in the Public Sector. The toolkit is a guide to help policymakers and public sector leaders implement principles for safe and trustworthy AI. It highlights AI's potential to enhance public sector efficiency, policymaking, service responsiveness, and transparency while addressing associated risks. The guide provides practical insights, ethical considerations, and good practices for AI use in the public sector.

Link - https://www.oecd.org/en/publications/g7-toolkit-for-artificial-intelligence-in-the-public-sector_421c1244-en.html

ASEAN Region Updates

2. Singapore – "Guidelines and Companion Guide on Securing AI Systems"

October 15, 2024

In Singapore, The Cyber Security Agency of Singapore (CSA) released guidelines to secure AI systems, addressing cybersecurity risks like adversarial attacks and supply chain threats. The guidelines promote securing AI by design and default throughout its lifecycle, from planning to end-of-life. The Companion Guide, a community-driven resource, provides practical security measures, controls, and best practices from industry and academia. It emphasizes identifying and mitigating risks, fostering confidence in AI systems, and encouraging business leaders and AI practitioners to adopt these measures to ensure safe and effective AI use.

Link - https://www.csa.gov.sg/Tips-Resource/publications/2024/guidelines-on-securing-ai

National Legal Updates (International Countries)

3. European Union AI Act – Joint Research Centre Published Harmonized Standards for The European AI Act

October 24, 2024

On October 24, 2024, the European Commission's Joint Research Centre released a Science for Policy Brief outlining key quality attributes for harmonized AI standards under the AI Act, such as risk prioritization, lifecycle coverage, clarity, and cross-sector applicability. It details necessary deliverables including risk management, record-keeping, human oversight, robustness, data governance, and cybersecurity, and emphasizes the fast-tracked drafting process for 37 standardization activities, aiming for high-risk AI system compliance by August 2026. The AI Act, adopted in August 2024, will apply provisions for high-risk AI systems after a transition period of 2-3 years. Once harmonized standards are published in the EU Official Journal, AI systems developed according to them will be legally presumed compliant. CEN and CENELEC are leading the drafting of these standards, as requested by the European Commission, to support the AI Act's implementation.

Link - https://publications.jrc.ec.europa.eu/repository/handle/JRC139430

4. WEF White Paper on Governance In The Age Of Generative AI

October 8, 2024

The World Economic Forum (WEF) published a white paper titled 'Governance in the Age of Generative AI: A 360º Approach for Resilient Policy and Regulation' in collaboration with Accenture. This paper discusses the need for governments to address regulatory gaps, engage multiple stakeholders, and prepare for future generative AI risks. It proposes a comprehensive governance framework, urging governments to assess and adapt existing regulations to tackle challenges introduced by generative AI, while coordinating across various policy objectives. It emphasizes the importance of cultivating a whole-of-society approach to AI governance, involving stakeholders from industry, civil society, and academia, and fostering interdisciplinary knowledge-sharing. The paper highlights the necessity for governments to plan for the future by developing agile strategies, investing in AI upskilling, conducting foresight exercises, and promoting international cooperation to manage emerging AI risks and advancements.

Link to the white paper –
https://www3.weforum.org/docs/WEF_Governance_in_the_Age_of_Generative_AI_2024.pdf

5. AI Policy for Financial Markets – Hongkong

October 28, 2024

The Hong Kong Government has issued a policy statement on the responsible application of AI in the financial market, emphasizing its commitment to fostering AI adoption while managing associated risks. The Financial Secretary, highlighted Hong Kong's unique position as an international financial hub, aiming to leverage AI to accelerate financial sector development, while addressing challenges like cybersecurity, data privacy, and intellectual property protection. The policy advocates for financial institutions to adopt AI governance strategies and risk-based approaches, with human oversight to mitigate potential risks. The Hong Kong University of Science and Technology will support the sector by providing AI models, computing resources, and training services. Financial regulators will continue updating guidelines to reflect AI advancements, while efforts to address AI-related cyber challenges and public education on AI risks will also be prioritized.

Link - https://www.info.gov.hk/gia/general/202410/28/P2024102800154.htm

6. Germany and France Publish Joint Recommendations for The Use of AI Programming Assistants

October 4, 2024

On October 4, 2024, the French Cybersecurity Agency and Germany's Federal Office for Information Security issued joint recommendations for the secure use of AI coding assistants. These recommendations state both the benefits and risks of AI tools in programming. While AI coding assistants can automate code generation, enhance productivity, and translate legacy code, they pose risks such as security vulnerabilities, inconsistent code quality, and the potential leakage of sensitive data. Specific concerns include automation bias, generation of flawed code, and susceptibility to adversarial attacks. To mitigate these risks, the agencies recommend cautious use of AI tools, implementing security measures, conducting risk assessments, and having experienced developers review AI-generated code to ensure reliability and protect sensitive information.

Link –
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/ANSSI_BSI_AI_Coding_Assistants.html

7. FINOS Releases Initial Draft of AI Governance Framework for Financial Institutions

October 1, 2024

On October 1, 2024, FINOS (the Fintech Open Source Foundation) released a draft AI Governance Framework for financial institutions at the Open Source in Finance Forum (OSFF) in New York. Developed by the AI Readiness Special Interest Group, the framework identifies 15 risks and 15 controls tailored to generative AI in financial services, aiming to ensure safe, compliant, and trustworthy AI adoption. The initiative has garnered strong support from industry leaders like NVIDIA, Protect AI, and Moody's, who joined FINOS as members. This collaborative, open-source effort invites participation from the financial services community to

refine the framework and operationalize AI governance, addressing challenges like regulatory compliance, automation risks, and customer trust in AI systems. The initiative reflects a broader commitment to leveraging open-source solutions for financial services' technological evolution.

Link - Press Release

8. US – Guidance of AI and Worker Well-being

October 16, 2024

On October 16, 2024, the U.S. Department of Labor (DOL) released Artificial Intelligence and Worker Well-Being: Principles and Best Practices for Developers and Employers. The rationale behind this is to develop a roadmap to enhance worker wellbeing through AI. This guidance builds on previously issued principles, emphasizing worker empowerment, ethical AI development, governance, transparency, labor rights protection, AI-driven worker enablement, support for those impacted by AI, and responsible data use. While the principles are non binding, they offer practical "Best Practices" for employers and developers, aligning with President Biden's Executive Order on trustworthy AI.

Link - https://www.dol.gov/newsroom/releases/osec/osec20241016

9. US – President Biden issued a National Security Memorandum on AI

October 24, 2024

On October 24, 2024, President Biden issued a National Security Memorandum (NSM) on Artificial Intelligence, emphasizing U.S. leadership in safe and trustworthy AI technologies while addressing risks like foreign espionage and supply chain vulnerabilities. It introduced a Framework for AI Governance and Risk Management in National Security, focusing on transparency, accountability, and alignment with democratic values and human rights. The NSM outlined prohibited AI uses, such as biased decision-making and profiling infringing on constitutional rights, and mandated risk assessments for high-impact AI applications. Agencies must maintain inventories of AI use cases and report on risk management practices, while standardized training for federal personnel on responsible AI usage was also mandated. The memorandum promotes international collaboration, building on efforts like the International Code of Conduct on AI, to establish globally responsible governance frameworks.

Link - https://ai.gov/wp-content/uploads/2024/10/NSM-Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf

10. AI Privacy guidelines by Australia

October 21, 2024

On October 21, 2024, the Australian Information Commissioner released guidance stating that the Privacy Act applies to AI products that process personal data. The guidance advises organizations to evaluate the purposes for which data is used, ensure data accuracy, and secure proper consent, particularly for sensitive data. Organizations must also be transparent about AI usage in privacy policies and adopt accountability measures. It emphasizes the need for continuous assurance, including staff training on privacy risks.

Link - https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products