

IDVN

Viet Nam International Law Firm

LEGAL UPDATE

Legal Tech



PHÁP LUẬT VỀ TRÍ TUỆ NHÂN TẠO TỪ 2026 TRỞ ĐI

Trịnh Nguyên Hoàng

Vào ngày 14/06/2025, văn bản Luật Công nghiệp công nghệ số (“**Luật CNCNS**”) chính thức được thông qua bởi Quốc hội và sẽ có hiệu lực vào ngày 01/01/2026. Ngoài các nội dung quan trọng như công nghiệp công nghệ số, công nghiệp bán dẫn, tài sản số, quyền và trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan... Luật CNCNS cuối cùng đã đề cập đến chủ đề quan trọng nhất trong mảng LegalTech của thế giới kể từ năm 2022 đến giờ: **Trí tuệ nhân tạo** (Artificial Intelligence).

1. Về định nghĩa của trí tuệ nhân tạo

Tại Điều 3.9 của Luật CNCNS, trí tuệ nhân tạo được định nghĩa như sau:

“9. Hệ thống trí tuệ nhân tạo là hệ thống dựa trên máy móc được thiết kế để hoạt động với các mức độ tự chủ khác nhau và có khả năng thích ứng sau khi triển khai nhằm đạt được những mục tiêu rõ ràng hoặc ngầm định, suy luận từ dữ liệu đầu vào mà hệ thống này nhận được để tạo ra dự đoán, nội dung, khuyến nghị, quyết định có thể ảnh hưởng đến môi trường thực hoặc môi trường điện tử. Hệ thống trí tuệ nhân tạo là sản phẩm công nghệ số tích hợp giữa phần cứng, phần mềm và dữ liệu.”

Có thể thấy, quy định này được sao chép toàn bộ từ Điều 3.1 của Luật Trí tuệ nhân tạo Liên minh Châu Âu (EU)¹, cho thấy Việt Nam đã học hỏi kinh nghiệm quốc tế khi xây dựng khái niệm này. Khái niệm này cũng tương đồng với khuyến nghị của OECD² và Viện Đo lường Quốc gia Hoa Kỳ.³ Các khái niệm này đều ghi nhận rằng trí tuệ nhân tạo là “hệ thống dựa trên máy móc” (machine-based) và có mức độ tự chủ khác nhau (varying levels of autonomy).

Tuy nhiên, một điểm mà Việt Nam đã bổ sung thêm so với các khái niệm quốc tế nêu trên đó là “*Hệ thống trí tuệ nhân tạo là sản phẩm công nghệ số tích hợp giữa phần cứng, phần mềm và dữ liệu*”. Các khái niệm của OECD, EU và NIST không ghi nhận rõ ràng rằng trí tuệ nhân tạo là sản phẩm tích hợp giữa phần cứng, phần mềm và dữ liệu, mà chỉ thể hiện rằng nó là phần cứng (machine-based). Sự khác biệt này có thể đem đến hệ quả khác biệt về vấn đề đánh thuế và phân loại hàng hóa (tiêu chuẩn quốc gia) khi nhập khẩu vào Việt Nam.

2. Chính sách của nhà nước đối với trí tuệ nhân tạo

Điều 4 của Luật CNCNS đưa ra một số chính sách phát triển trí tuệ nhân tạo như:

(i) Đưa trí tuệ nhân tạo trở thành phương thức sản xuất mới;

¹ Xem thêm tại: <https://artificialintelligenceact.eu/article/3/>

² Xem thêm tại Phần I của khuyến nghị: https://weccglobal.org/uploads/2019/07/2019_OECD_Recommendations-AI.pdf

³ Xem thêm tại: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf>

(ii) Thúc đẩy mạnh mẽ năng lực nội sinh quốc gia, tạo ra những mô hình kinh tế mới với năng suất và giá trị vượt trội.

(iii) Thúc đẩy nghiên cứu, phát triển, triển khai, sử dụng trí tuệ nhân tạo (với chính sách ưu đãi cao nhất từ nhà nước tại Điều 28).

Với sự phát triển của Tác nhân trí tuệ nhân tạo (AI Agent) sắp tới thì việc các doanh nghiệp, tổ chức, cá nhân như FPT, VinAI research, Viettel, VNPT, VNG... phát triển theo định hướng nói trên của nhà nước sẽ trở thành một mô hình kinh doanh mới với năng suất và giá trị vượt trội (nhưng cũng dẫn đến hệ quả là rất nhiều công việc và nhân sự sẽ bị đào thải và thay thế bởi AI.

3. Các hành vi bị cấm đối với hệ thống trí tuệ nhân tạo

Các công nghệ AI đi đầu như Qwen, Sora, DeepSeek, Wan 2.5, Kling 2.5... việc sửa chữa ảnh và video đã trở nên phổ biến và đơn giản hơn bao giờ hết. Mọi cá nhân, tổ chức đều có thể sửa chữa ảnh và video chỉ với một vài dòng chữ mô tả và một cú click chuột. Nếu được sử dụng với mục đích xấu, các công cụ này có thể xâm phạm nghiêm trọng đến quyền và lợi ích hợp pháp của tổ chức, cá nhân khác.

Điều 12.6 của Luật CNCNS cấm tổ chức, cá nhân sử dụng, cung cấp, triển khai hệ thống trí tuệ nhân tạo để xâm phạm lợi ích quốc gia, dân tộc, quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, lợi ích công cộng; quyền con người, quyền công dân, quyền và lợi ích hợp pháp của tổ chức, cá nhân và phá hoại thuần phong mỹ tục.

4. Nguyên tắc phát triển, cung cấp, triển khai sử dụng trí tuệ nhân tạo

Điều 41 của Luật CNCNS quy định về một số nguyên tắc, kim chỉ nam định hướng phát triển, cung cấp, triển khai sử dụng trí tuệ nhân tạo như sau:

- Phục vụ sự thịnh vượng và hạnh phúc của con người, lấy con người làm trung tâm, nâng cao năng suất, hiệu quả công việc, thúc đẩy thông minh hóa; tiếp cận bao trùm, linh hoạt, công bằng và không phân biệt đối xử; tôn trọng các giá trị đạo đức, dân tộc; quyền con người, quyền công dân, quyền và lợi ích hợp pháp của tổ chức, cá nhân;

- Bảo đảm minh bạch, trách nhiệm giải trình, khả năng giải thích được; bảo đảm không vượt qua tầm kiểm soát của con người;

- Bảo đảm an toàn, an ninh mạng;

- Bảo đảm tuân thủ quy định pháp luật về dữ liệu, bảo vệ dữ liệu cá nhân;

- Bảo đảm khả năng kiểm soát thuật toán, mô hình trí tuệ nhân tạo;

- Kiểm soát rủi ro **trong suốt vòng đời của hệ thống trí tuệ nhân tạo**;

- Bảo đảm tuân thủ pháp luật về bảo vệ quyền lợi người tiêu dùng và pháp luật khác có liên quan.

Một điểm đáng lưu ý chưa được định nghĩa trong Luật CNCNS đó là: “*Thế nào là vòng đời của hệ thống trí tuệ nhân tạo?*” Khi tham khảo khuyến nghị của OECD⁴, vòng đời của trí tuệ nhân tạo bao gồm 4 giai đoạn từ (i) thiết kế, dữ liệu và mô hình; (ii) xác minh và thẩm định; (iii) triển khai; cho đến (iv) vận hành và giám sát. Các giai đoạn này thường diễn ra một cách lặp đi lặp lại và không nhất thiết phải tuần tự.

⁴ Xem thêm tại Phần I của khuyến nghị: https://weccglobal.org/uploads/2019/07/2019_OECD_Recommendations-AI.pdf

Quyết định ngừng vận hành và phát triển một hệ thống AI có thể xảy ra tại bất cứ thời điểm nào trong giai đoạn 4 – vận hành và giám sát.

Ngoài ra, Điều 44.1 của Luật CNCNS quy định về dấu hiệu nhận dạng đối với hệ thống trí tuệ nhân tạo, yêu cầu chủ thể cung cấp, triển khai trí tuệ nhân tạo phải tạo ra các dấu hiệu cụ thể để người dùng có thể biết họ đang tương tác với trí tuệ nhân tạo hoặc sử dụng sản phẩm công nghệ số tạo ra bởi trí tuệ nhân tạo.

Trên đây là một số nội dung mà doanh nghiệp, tổ chức, cá nhân cần lưu ý khi phát triển, cung cấp, triển khai sử dụng AI kể từ ngày 01/01/2026 trở đi. Hàng loạt các văn bản quy định chi tiết và hướng dẫn sẽ được ban hành trong tương lai để quản lý chặt chẽ hơn về các khía cạnh như ưu đãi, hỗ trợ phát triển nghiên cứu, vấn đề xử phạt, vấn đề dấu hiệu nhận dạng hệ thống trí tuệ nhân tạo, các nguyên tắc cần lưu tâm v.v...