

RỦI RO PHÁP LÝ TRONG SỬ DỤNG DỮ LIỆU NGHIÊN CỨU ĐỂ PHÁT TRIỂN VÀ ỨNG DỤNG TRÍ TUỆ NHÂN TẠO TẠI CƠ SỞ GIÁO DỤC ĐẠI HỌC

Nguyễn Công Ước, Đoàn Thành Nhân, Nguyễn Hoàng Yến
Ban Đảm bảo chất lượng và Pháp chế, Học viện Nông nghiệp Việt Nam
Email: ncuoc@vnua.edu.vn

Tóm tắt: Việc sử dụng dữ liệu nghiên cứu để huấn luyện và vận hành trí tuệ nhân tạo tại các cơ sở giáo dục đại học đặt ra yêu cầu về bảo vệ dữ liệu cá nhân, sở hữu trí tuệ, an ninh mạng và trách nhiệm AI. Bài viết phân tích khung pháp luật Việt Nam có hiệu lực đến 9/9/2026, đồng thời đối chiếu với pháp luật và chuẩn mực quốc tế. Kết quả cho thấy Việt Nam đã hình thành khung pháp lý tương đối toàn diện nhưng còn thiếu quy định thống nhất về dữ liệu nghiên cứu, khai thác văn bản và dữ liệu cho AI, quyền đối với bộ dữ liệu, mô hình và đầu ra AI. Bài viết đề xuất mô hình quản trị theo vòng đời nhằm đảm bảo sử dụng dữ liệu hợp pháp, minh bạch và có trách nhiệm.

Từ khóa: Dữ liệu nghiên cứu; trí tuệ nhân tạo; cơ sở giáo dục đại học; khai thác văn bản và dữ liệu; dữ liệu cá nhân; sở hữu trí tuệ.

LEGAL RISKS IN USING RESEARCH DATA FOR ARTIFICIAL INTELLIGENCE DEVELOPMENT AND APPLICATION IN HIGHER EDUCATION INSTITUTIONS

Abstract: The deployment of research data to train and operate artificial intelligence (AI) systems in higher education institutions introduces complex legal risks across personal data protection, intellectual property, cybersecurity, and AI accountability. This article examines Vietnam's legal framework as of September 2026, comparing it with regulatory approaches in the European Union, the United States, the United Kingdom, and Japan. The analysis shows that while Vietnam has established core legal pillars, regulatory gaps persist regarding the status of research data, text and data mining exceptions for AI, rights over datasets, models, and outputs, and liability allocation across the AI value chain. The authors propose a lifecycle governance model to ensure legal, transparent, and responsible data utilization.

Keywords: research data, artificial intelligence; legal risks; higher education institutions; personal data; intellectual property.

Nhận bài: 15/09/2026

Phản biện: 15/10/2026

Duyệt đăng: 18/10/2026

I. ĐẶT VẤN ĐỀ

Trong hoạt động nghiên cứu khoa học tại cơ sở giáo dục đại học, dữ liệu không chỉ là bảng số liệu được công bố kèm theo bài báo mà còn bao gồm dữ liệu thô, dữ liệu trung gian, bản ghi phỏng vấn, hình ảnh, âm thanh, mã nguồn, siêu dữ liệu và các bộ dữ liệu hình thành từ nhiều nhiệm vụ nghiên cứu. Cùng với sự phát triển của trí tuệ nhân tạo (AI), những nguồn dữ liệu này ngày càng được sử dụng để huấn luyện, tinh chỉnh, kiểm thử mô hình, xây dựng hệ thống truy xuất tăng cường, phát hiện quy luật và tạo ra dự báo khoa học.

Sự thay đổi này đặt ra những vấn đề pháp lý vượt ra ngoài tính hợp pháp của việc thu thập dữ liệu. Một bộ dữ liệu được thu thập hợp pháp cho một đề tài chưa chắc đã được phép sử dụng cho mục đích mới như huấn luyện AI. Tương tự, việc cơ sở giáo dục đại học có quyền quản lý kết quả nghiên cứu không đồng nghĩa với quyền sao chép mọi tác phẩm có trong dữ liệu, chuyển dữ liệu của đối tác cho nhà cung cấp AI hoặc cho phép nền tảng AI tái sử dụng dữ liệu. Đây là vấn đề cần được

nhìn nhận đầy đủ trong bối cảnh các trường đại học đẩy mạnh chuyển đổi số và phát triển AI.

Ở Việt Nam, khung pháp luật liên quan đã có những thay đổi trong giai đoạn 2025–2026. Luật Dữ liệu năm 2024, Luật Khoa học, công nghệ và đổi mới sáng tạo năm 2025, Luật Bảo vệ dữ liệu cá nhân năm 2025, Luật Trí tuệ nhân tạo năm 2025 và Luật sửa đổi, bổ sung một số điều của Luật Sở hữu trí tuệ năm 2025 tạo nên các lớp điều chỉnh mới. Tuy nhiên, các văn bản này điều chỉnh từng khía cạnh của dữ liệu và AI, chưa hình thành một chế độ pháp lý riêng, thống nhất cho dữ liệu nghiên cứu tại cơ sở giáo dục đại học.

Từ thực tiễn trên, bài viết tập trung phân tích các rủi ro pháp lý phát sinh khi dữ liệu nghiên cứu được sử dụng để phát triển, huấn luyện, tinh chỉnh, kiểm thử và ứng dụng AI tại cơ sở giáo dục đại học. Trên cơ sở phân tích quy phạm pháp luật, tổng quan tài liệu và so sánh pháp luật, bài viết đề xuất một số định hướng quản trị phù hợp với điều kiện pháp luật Việt Nam hiện nay.

II. DỮ LIỆU NGHIÊN CỨU VÀ CÁC TÀNG QUYỀN PHÁP LÝ

2.1. Khái niệm dữ liệu nghiên cứu

Pháp luật Việt Nam hiện chưa thiết lập một định nghĩa chung và chế độ pháp lý riêng cho “dữ liệu nghiên cứu”. Luật Dữ liệu số 60/2024/QH15 điều chỉnh các hoạt động xây dựng, bảo vệ, quản trị, xử lý và sử dụng dữ liệu số, trong khi Luật Khoa học, công nghệ và đổi mới sáng tạo số 93/2025/QH15 điều chỉnh nhiệm vụ, kết quả và tài sản hình thành từ hoạt động nghiên cứu.

Trong phạm vi bài viết, dữ liệu nghiên cứu được hiểu là dữ liệu được thu thập, tạo lập, quan sát, đo lường, mô phỏng, tổng hợp hoặc xử lý nhằm hình thành, kiểm chứng, giải thích hoặc tái lập kết quả nghiên cứu khoa học. Cách tiếp cận theo chức năng phù hợp hơn việc liệt kê theo định dạng, bởi cùng một dữ liệu có thể thay đổi vai trò trong vòng đời nghiên cứu và tiếp tục được sử dụng làm dữ liệu đầu vào cho hệ thống AI.

2.2. Một bộ dữ liệu có thể đồng thời chịu nhiều chế độ pháp lý

Không tồn tại một quyền sở hữu tuyệt đối và đơn nhất đối với mọi dữ liệu. Một bộ dữ liệu có thể đồng thời chứa dữ liệu cá nhân, tác phẩm được bảo hộ, bí mật kinh doanh, thông tin chịu nghĩa vụ bảo mật, kết quả của nhiệm vụ sử dụng ngân sách nhà nước hoặc dữ liệu mà cơ sở giáo dục đại học chỉ được cấp quyền truy cập.

Vì vậy, khi đưa dữ liệu vào hệ thống AI, cần phân biệt năm lớp quyền và nghĩa vụ: (i) quyền tiếp cận dữ liệu; (ii) quyền và căn cứ xử lý dữ liệu cá nhân; (iii) quyền sao chép hoặc khai thác đối tượng sở hữu trí tuệ; (iv) quyền công bố, chia sẻ hoặc chuyển giao theo hợp đồng và quy định về nhiệm vụ khoa học; và (v) quyền sử dụng dữ liệu để phát triển AI. Có quyền ở một lớp không mặc nhiên tạo ra quyền ở các lớp còn lại.

2.3. Địa vị pháp lý của cơ sở giáo dục đại học trong chuỗi AI

Theo Luật Trí tuệ nhân tạo số 134/2025/QH15, tùy từng hoạt động, cơ sở giáo dục đại học có thể là nhà phát triển, nhà cung cấp, bên triển khai hoặc người sử dụng đầu ra AI. Trong pháp luật về dữ liệu cá nhân, cơ sở giáo dục cũng có thể là bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu hoặc bên xử lý, tùy thuộc vào việc quyết định mục đích và phương tiện xử lý.

Việc thuê dịch vụ AI không làm mất trách nhiệm của cơ sở giáo dục đối với tính hợp pháp của dữ liệu đầu vào. Tương tự, việc nhóm nghiên

cứ sử dụng tài khoản cá nhân trong thực hiện nhiệm vụ không đồng nghĩa với việc mọi trách nhiệm tổ chức được chuyển sang cá nhân. Do đó, vai trò và trách nhiệm pháp lý cần được xác định theo từng công đoạn của dự án.

III. KHUNG PHÁP LUẬT VIỆT NAM LIÊN QUAN ĐẾN DỮ LIỆU NGHIÊN CỨU VÀ AI

3.1. Pháp luật về dữ liệu và khoa học, công nghệ, đổi mới sáng tạo

Luật Dữ liệu số 60/2024/QH15 tạo nền tảng pháp lý chung cho quản trị, khai thác và sử dụng dữ liệu tại Việt Nam. Luật Khoa học, công nghệ và đổi mới sáng tạo số 93/2025/QH15 tiếp tục đặt vấn đề quản lý, khai thác và thương mại hóa kết quả nghiên cứu trong khuôn khổ mới.

Tuy nhiên, cần phân biệt giữa kết quả nghiên cứu đã hoàn thiện với dữ liệu thô, dữ liệu trung gian và dữ liệu hình thành trong quá trình nghiên cứu. Quyền đối với kết quả của một nhiệm vụ khoa học không nhất thiết đồng nhất với quyền đối với mọi dữ liệu được sử dụng để tạo ra kết quả đó. Vì vậy, việc cơ sở giáo dục đại học quản lý một nhiệm vụ khoa học không đồng nghĩa với quyền tự do chuyển toàn bộ dữ liệu cho doanh nghiệp phát triển AI.

3.2. Bảo vệ dữ liệu cá nhân

Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, có hiệu lực từ ngày 01/01/2026, điều chỉnh hoạt động xử lý dữ liệu theo phạm vi rộng, bao gồm thu thập, phân tích, tổng hợp, khử nhận dạng, cung cấp và chuyển giao. Các nguyên tắc xử lý yêu cầu mục đích rõ ràng, phạm vi phù hợp, bảo đảm tính chính xác, thời hạn lưu giữ và biện pháp bảo vệ cần thiết.

Đối với AI, vấn đề đáng lưu ý là sự khác biệt giữa mục đích thu thập ban đầu và mục đích sử dụng tiếp theo. Sự đồng ý của chủ thể dữ liệu cho một nghiên cứu cụ thể không mặc nhiên cho phép chuyển dữ liệu sang hệ thống AI phục vụ mục đích khác.

Bên cạnh đó, việc xóa thông tin nhận diện trực tiếp không phải lúc nào cũng loại bỏ nguy cơ tái nhận dạng khi kết hợp nhiều nguồn dữ liệu. Vì vậy, việc đưa dữ liệu cá nhân vào hệ thống AI cần được xem xét ngay từ khâu thiết kế nghiên cứu, đồng thời dưới góc độ pháp lý, đạo đức nghiên cứu và an toàn thông tin.

3.3. Sở hữu trí tuệ và khai thác văn bản, dữ liệu

Luật số 131/2025/QH15 sửa đổi, bổ sung một số điều của Luật Sở hữu trí tuệ, có hiệu lực từ ngày 01/4/2026, ghi nhận nguyên tắc cho phép sử dụng

văn bản và dữ liệu về đối tượng quyền sở hữu trí tuệ đã được công bố hợp pháp và công chúng được phép tiếp cận để nghiên cứu khoa học, thử nghiệm, huấn luyện AI, với điều kiện không ảnh hưởng bất hợp lý đến quyền và lợi ích hợp pháp của tác giả, chủ sở hữu.

Nghị định số 134/2026/NĐ-CP tiếp tục cụ thể hóa các điều kiện sử dụng văn bản và dữ liệu được bảo hộ quyền tác giả, quyền liên quan, bao gồm nguồn tiếp cận hợp pháp, mục đích không nhằm thương mại, quyền bảo lưu của chủ thể quyền và trách nhiệm lưu giữ hồ sơ, dữ liệu huấn luyện.

Tuy nhiên, ngoại lệ này không đồng nghĩa với việc mọi dữ liệu có thể truy cập đều được tự do sử dụng để huấn luyện AI. Khi hệ thống hoặc kết quả nghiên cứu được khai thác thương mại, các nghĩa vụ về quyền tác giả và tiền bản quyền cần tiếp tục được xem xét. Ngoại lệ sở hữu trí tuệ cũng không loại bỏ nghĩa vụ bảo vệ dữ liệu cá nhân, bí mật kinh doanh và hạn chế theo hợp đồng. Vì vậy, “dữ liệu công khai” không nên được đồng nhất với “dữ liệu tự do sử dụng”.

3.4. Luật Trí tuệ nhân tạo và quản trị dữ liệu huấn luyện

Luật Trí tuệ nhân tạo số 134/2025/QH15, có hiệu lực từ ngày 01/3/2026, thiết lập cách tiếp cận quản lý theo rủi ro. Việc thu thập, xử lý và sử dụng dữ liệu để phát triển, huấn luyện, kiểm thử hoặc vận hành AI phải tuân thủ pháp luật về dữ liệu, dữ liệu cá nhân, sở hữu trí tuệ và an ninh mạng.

Đối với hệ thống rủi ro cao, các nghĩa vụ quản trị dữ liệu huấn luyện, kiểm thử, lập hồ sơ kỹ thuật, lưu nhật ký, giám sát của con người và trách nhiệm giải trình được đặt ra chặt chẽ hơn. Nghị định số 142/2026/NĐ-CP tiếp tục quy định chi tiết một số điều và biện pháp thi hành Luật Trí tuệ nhân tạo.

Tuy nhiên, một hệ thống AI có mức độ rủi ro tác động thấp vẫn có thể sử dụng dữ liệu nhạy cảm hoặc tài sản trí tuệ có giá trị cao. Vì vậy, phân loại rủi ro của hệ thống không thể thay thế việc đánh giá mức độ nhạy cảm của dữ liệu đầu vào.

IV. NHỮNG NHÓM RỦI RO PHÁP LÝ CHỦ YẾU TẠI CƠ SỞ GIÁO DỤC ĐẠI HỌC

Rủi ro pháp lý trong sử dụng dữ liệu nghiên cứu để phát triển và ứng dụng AI không tập trung ở một công đoạn mà trải dài theo toàn bộ vòng đời dữ liệu, chủ yếu gồm năm nhóm sau:

Thứ nhất, rủi ro về quyền sử dụng dữ liệu đầu vào. Dữ liệu nghiên cứu có thể bao gồm tác phẩm được bảo hộ, dữ liệu của đối tác và kết quả nhiệm

vụ khoa học với phạm vi quyền sử dụng khác nhau. Việc tiếp cận hợp pháp không đồng nghĩa với quyền tự do sao chép hoặc sử dụng để huấn luyện AI. Nếu không lưu giữ nguồn gốc, giấy phép và điều kiện khai thác, cơ sở giáo dục đại học có thể gặp khó khăn khi chứng minh quyền sử dụng dữ liệu hoặc giải quyết tranh chấp.

Thứ hai, rủi ro về xử lý dữ liệu cá nhân. Việc đưa dữ liệu nghiên cứu vào hệ thống AI có thể làm thay đổi mục đích xử lý, mở rộng phạm vi tiếp cận và gia tăng nguy cơ tái nhận dạng. Đặc biệt, việc sử dụng nền tảng AI nước ngoài có thể làm phát sinh nghĩa vụ liên quan đến chuyển dữ liệu xuyên biên giới theo quy định pháp luật.

Thứ ba, rủi ro về bảo mật và khả năng bảo hộ kết quả nghiên cứu. Việc đưa dữ liệu thử nghiệm, quy trình kỹ thuật hoặc thông tin chưa công bố lên nền tảng AI bên ngoài có thể vi phạm nghĩa vụ bảo mật, ảnh hưởng đến khả năng bảo hộ sáng chế hoặc bí mật kinh doanh. Rủi ro còn phụ thuộc vào quyền tiếp cận, sử dụng dữ liệu của nhà cung cấp theo điều khoản dịch vụ.

Thứ tư, rủi ro về sai lệch dữ liệu, đầu ra AI và trách nhiệm pháp lý. AI có thể tạo ra thông tin không chính xác, nguồn trích dẫn không tồn tại hoặc kết quả phân tích sai lệch. Khi đầu ra được sử dụng trong nghiên cứu, tư vấn hoặc quyết định quản lý, thiệt hại có thể liên quan đến nhiều chủ thể. Việc xác định trách nhiệm phụ thuộc vào vai trò, mức độ kiểm soát, lỗi và quan hệ nhân quả giữa các bên.

Thứ năm, rủi ro chuyển dữ liệu xuyên biên giới và “AI ngầm”. Việc sử dụng nền tảng AI nước ngoài hoặc tài khoản cá nhân ngoài hệ thống được phê duyệt có thể khiến cơ sở giáo dục khó kiểm soát địa điểm lưu trữ, phạm vi tiếp cận và thời hạn lưu giữ dữ liệu. Vì vậy, cần quy định rõ công cụ AI được phép sử dụng và loại dữ liệu được đưa vào từng hệ thống.

V. KINH NGHIỆM VÀ BÀI HỌC TỪ NƯỚC NGOÀI

5.1. Liên minh châu Âu

Liên minh châu Âu thiết lập cấu trúc tương đối rõ giữa bảo vệ dữ liệu, khai thác văn bản và dữ liệu, và quản trị AI. Quy định chung về bảo vệ dữ liệu (GDPR) đặt ra các nguyên tắc về căn cứ xử lý, giới hạn mục đích, tối thiểu hóa dữ liệu và bảo vệ dữ liệu trong nghiên cứu khoa học. Chỉ thị (EU) 2019/790 quy định ngoại lệ khai thác văn bản và dữ liệu cho tổ chức nghiên cứu và tổ chức di sản văn hóa trong điều kiện luật định, đồng thời

có cơ chế bảo lưu quyền trong một số trường hợp. Đạo luật AI năm 2024 tiếp tục đặt ra yêu cầu về quản trị dữ liệu, hồ sơ kỹ thuật, lưu nhật ký và giám sát con người đối với hệ thống rủi ro cao.

Kinh nghiệm đáng chú ý đối với Việt Nam là cách tiếp cận phân tầng: ngoại lệ nghiên cứu không đồng nghĩa với miễn trừ các nghĩa vụ pháp lý khác; hoạt động khai thác thương mại cần được xem xét trong khuôn khổ quyền và nghĩa vụ tương ứng.

5.2. Hoa Kỳ

Hoa Kỳ chưa có ngoại lệ thống nhất ở cấp liên bang dành riêng cho khai thác văn bản và dữ liệu để huấn luyện AI. Việc sao chép để huấn luyện thường được xem xét theo nguyên tắc sử dụng hợp lý (fair use), dựa trên mục đích, tính chất sử dụng, bản chất tác phẩm, lượng sử dụng và ảnh hưởng đến thị trường. Cách tiếp cận này tạo tính linh hoạt nhưng phụ thuộc vào hoàn cảnh cụ thể và án lệ.

Về quản trị, Khung quản lý rủi ro AI của Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST AI Risk Management Framework) gồm bốn chức năng Govern, Map, Measure và Manage, nhấn mạnh an toàn, bảo mật, minh bạch, quyền riêng tư và quản lý thiên lệch. Đây là khuôn khổ tham khảo hữu ích cho cơ sở giáo dục đại học nhưng không trực tiếp tạo ra nghĩa vụ pháp lý.

5.3. Vương quốc Anh và Nhật Bản

Vương quốc Anh cho phép khai thác văn bản và dữ liệu phục vụ nghiên cứu phi thương mại trong những điều kiện nhất định theo Copyright, Designs and Patents Act 1988. Phạm vi ngoại lệ này đặt ra vấn đề đối với nghiên cứu có tài trợ doanh nghiệp hoặc khả năng thương mại hóa.

Nhật Bản có cách tiếp cận tương đối rộng tại Điều 30-4 Luật Bản quyền, cho phép khai thác tác phẩm trong những trường hợp không nhằm hưởng thụ tư tưởng hoặc cảm xúc được thể hiện, với điều kiện không gây phương hại bất hợp lý đến lợi ích của chủ thể quyền. Việc áp dụng phụ thuộc vào mục đích, cách thức sử dụng và tác động đến thị trường.

5.4. Bài học tham khảo

Không có mô hình nước ngoài nào có thể sao chép nguyên trạng. Tuy nhiên, có thể rút ra một số nguyên tắc chung: dữ liệu phải được tiếp cận hợp pháp; quyền và nghĩa vụ cần được quản trị theo vòng đời; ngoại lệ nghiên cứu phải đi cùng biện pháp bảo vệ; hoạt động AI cần có khả năng truy nguyên, minh bạch tương xứng với rủi ro và trách nhiệm được phân bổ theo khả năng kiểm soát của từng chủ thể.

VI. KHOẢNG TRỐNG PHÁP LÝ VÀ NHỮNG VẤN ĐỀ CẦN TIẾP TỤC NGHIÊN CỨU

Mặc dù pháp luật Việt Nam đã có những bước phát triển đáng kể, việc sử dụng dữ liệu nghiên cứu cho AI vẫn còn một số vấn đề cần tiếp tục làm rõ.

Trước hết, pháp luật chưa hình thành một chế độ pháp lý thống nhất đối với dữ liệu nghiên cứu. Một bộ dữ liệu có thể đồng thời chịu sự điều chỉnh của pháp luật về dữ liệu, dữ liệu cá nhân, sở hữu trí tuệ, bí mật nhà nước, tài sản công và hợp đồng. Sự phân tán này tạo ra khó khăn cho cơ sở giáo dục đại học trong việc xác định quyền và trách nhiệm đối với từng tập dữ liệu.

Tiếp theo, ranh giới giữa khai thác văn bản và dữ liệu phục vụ nghiên cứu với hoạt động huấn luyện AI có tính thương mại cần được làm rõ. Việc được tiếp cận dữ liệu hợp pháp không đồng nghĩa với quyền tự do thu thập, sao chép và xử lý dữ liệu cho mọi mục đích.

Ngoài ra, việc xác định và phân bổ quyền, lợi ích đối với dữ liệu, mô hình và đầu ra AI vẫn đặt ra những vấn đề pháp lý phức tạp. Nghị định số 134/2026/NĐ-CP đã bước đầu quy định điều kiện phát sinh quyền tác giả đối với sản phẩm có sử dụng AI, nhấn mạnh sự đóng góp đáng kể, mang tính quyết định của con người; sản phẩm hoàn toàn do AI tạo ra không làm phát sinh quyền tác giả, quyền liên quan. Tuy nhiên, khi mô hình được phát triển bởi nhóm nghiên cứu, sử dụng dữ liệu của trường và nền tảng công nghệ của doanh nghiệp, việc phân bổ quyền khai thác cần được giải quyết thông qua pháp luật sở hữu trí tuệ, pháp luật về khoa học, công nghệ, hợp đồng và quy chế nội bộ.

VII. ĐỊNH HƯỚNG QUẢN TRỊ RỦI RO TẠI CƠ SỞ GIÁO DỤC ĐẠI HỌC

Trong điều kiện pháp luật tiếp tục hoàn thiện, các cơ sở giáo dục đại học cần chủ động xây dựng cơ chế quản trị dữ liệu và AI trên cơ sở pháp luật hiện hành, thay vì chờ đợi một văn bản điều chỉnh toàn diện mọi tình huống.

Thứ nhất, cần xác minh nguồn gốc và phạm vi quyền sử dụng dữ liệu trước khi đưa vào hệ thống AI. Với mỗi dự án, nhóm nghiên cứu nên lập hồ sơ ghi nhận nguồn dữ liệu, chủ thể cung cấp, mục đích thu thập, điều kiện sử dụng, quyền sở hữu trí tuệ, dữ liệu cá nhân và các hạn chế theo hợp đồng. Hồ sơ cần được cập nhật trong suốt vòng đời dự án.

Thứ hai, cần phân loại dữ liệu theo mức độ nhạy cảm, từ dữ liệu công khai, dữ liệu nội bộ đến

dữ liệu cá nhân, thông tin mật và dữ liệu thuộc phạm vi bí mật nhà nước. Đồng thời, phải đánh giá mức độ rủi ro của hệ thống AI, bởi hệ thống có chức năng đơn giản vẫn có thể tạo ra rủi ro pháp lý lớn nếu xử lý dữ liệu đặc biệt nhạy cảm.

Thứ ba, đối với nền tảng AI bên ngoài, cần chuyển từ tư duy “mua phần mềm” sang “quản trị quan hệ xử lý dữ liệu”. Trước khi sử dụng, cơ sở giáo dục phải xem xét điều khoản về dữ liệu đầu vào, quyền sử dụng dữ liệu để huấn luyện, địa điểm lưu trữ, phạm vi tiếp cận, cơ chế xóa dữ liệu, thông báo sự cố và trách nhiệm khi xảy ra vi phạm.

Thứ tư, cần kiểm soát tình trạng “AI ngầm” bằng cách quy định rõ loại dữ liệu được phép đưa lên công cụ AI công cộng, dữ liệu chỉ được xử lý trên hệ thống nội bộ và dữ liệu không được chuyển cho nền tảng bên ngoài. Đồng thời, nhà trường cần cung cấp công cụ thay thế phù hợp để hạn chế việc sử dụng tài khoản cá nhân ngoài hệ thống quản trị.

Thứ năm, quản trị AI phải gắn với trách nhiệm của con người. Kết quả do AI tạo ra cần được kiểm tra trước khi sử dụng trong báo cáo khoa học, công bố, tư vấn chuyên môn hoặc quyết định quản lý. Đối với hệ thống có khả năng tác động đáng kể đến quyền và lợi ích của cá nhân, cần duy trì cơ chế giám sát và can thiệp của con người nhằm bảo đảm trách nhiệm giải trình.

Thứ sáu, có thể khái quát mô hình quản trị theo sáu giai đoạn: xác định mục tiêu và vai trò của dự án; xác minh nguồn gốc và quyền sử dụng dữ liệu; phân loại dữ liệu và đánh giá rủi ro; kiểm soát quá trình phát triển, thử nghiệm; giám sát khi triển khai; và lưu trữ, thu hồi quyền truy cập hoặc

xóa dữ liệu theo quy định. Cách tiếp cận này giúp chuyển từ xử lý sự cố sang kiểm soát rủi ro ngay từ khi thiết kế dự án.

VIII. KẾT LUẬN

Việc sử dụng dữ liệu nghiên cứu để phát triển và ứng dụng AI đang trở thành xu hướng trong hoạt động khoa học tại các cơ sở giáo dục đại học. Tuy nhiên, giá trị của dữ liệu cũng làm gia tăng yêu cầu xác định quyền sử dụng, bảo vệ thông tin và phân bổ trách nhiệm. Dữ liệu được thu thập hợp pháp không đồng nghĩa với quyền sử dụng cho mọi mục đích; quyền quản lý kết quả nghiên cứu cũng không mặc nhiên bao gồm quyền khai thác không hạn chế đối với toàn bộ dữ liệu cấu thành kết quả đó.

Qua phân tích pháp luật Việt Nam và kinh nghiệm quốc tế, có thể thấy các rủi ro chủ yếu phát sinh tại điểm giao thoa giữa quyền sử dụng dữ liệu đầu vào, bảo vệ dữ liệu cá nhân, sở hữu trí tuệ, bảo mật nghiên cứu, chuyển dữ liệu cho bên thứ ba và trách nhiệm đối với đầu ra AI. Mặc dù pháp luật Việt Nam giai đoạn 2024–2026 đã tạo lập những nền tảng quan trọng, việc thiếu cơ chế pháp lý thống nhất dành riêng cho dữ liệu nghiên cứu vẫn đặt ra yêu cầu tiếp tục hoàn thiện.

Ở cấp độ cơ sở giáo dục đại học, quản trị theo vòng đời là định hướng phù hợp, trong đó nguồn gốc dữ liệu, quyền sử dụng, mức độ nhạy cảm và rủi ro của hệ thống AI phải được xem xét ngay từ khâu thiết kế. Quản trị tốt rủi ro pháp lý không nhằm hạn chế phát triển AI mà tạo điều kiện để nhà khoa học khai thác dữ liệu và công nghệ mới một cách hợp pháp, có trách nhiệm, đồng thời bảo vệ quyền và lợi ích của các chủ thể liên quan.

TÀI LIỆU THAM KHẢO

- Quốc hội. (2024). Luật Dữ liệu số 60/2024/QH15 ngày 30 tháng 11 năm 2024.
- Quốc hội. (2025). Luật Khoa học, công nghệ và đổi mới sáng tạo số 93/2025/QH15 ngày 27 tháng 6 năm 2025.
- Quốc hội. (2025). Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26 tháng 6 năm 2025.
- Quốc hội. (2025). Luật Trí tuệ nhân tạo số 134/2025/QH15 ngày 10 tháng 12 năm 2025.
- Quốc hội. (2025). Luật số 131/2025/QH15 ngày 10 tháng 12 năm 2025 sửa đổi, bổ sung một số điều của Luật Sở hữu trí tuệ.
- Chính phủ. (2026). Nghị định số 134/2026/NĐ-CP ngày 06 tháng 4 năm 2026 sửa đổi, bổ sung một số điều của Nghị định số 17/2023/NĐ-CP về quyền tác giả, quyền liên quan.
- Chính phủ. (2026). Nghị định số 142/2026/NĐ-CP ngày 30 tháng 4 năm 2026 quy định chi tiết một số điều và biện pháp thi hành Luật Trí tuệ nhân tạo.
- European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation).
- European Parliament and Council of the European Union. (2019). Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market.
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence.
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1).
- United States Code. (n.d.). Title 17, § 107: Limitations on exclusive rights: Fair use.
- United Kingdom. (1988). Copyright, Designs and Patents Act 1988, Section 29A.
- Japan. (1970). Copyright Act, Article 30-4.