

CÔNG NGHỆ SỐ VÀ CÔNG TÁC BẢO MẬT DỮ LIỆU TRONG HẠ TẦNG GIÁO DỤC SỐ

Bùi Thị Lự¹, Trần Thị Hương Lý¹, Đặng Thùy Hương¹
Email: builu@hou.edu.vn

Ngày tòa soạn nhận được bài báo: 20/08/2025

Ngày phản biện đánh giá: 10/10/2025

Ngày bài báo được duyệt đăng: 23/10/2025

DOI: 10.59266/houjs.2025.801

Tóm tắt: Sự phát triển mạnh mẽ của công nghệ số đã mở ra nhiều cơ hội đổi mới cho giáo dục, song cũng đặt ra thách thức lớn về bảo mật dữ liệu và an toàn thông tin. Bài báo phân tích cơ sở lý luận, chỉ ra nguy cơ rò rỉ dữ liệu cá nhân, tấn công mạng và xâm phạm quyền riêng tư khi triển khai giáo dục số. Trên cơ sở tổng hợp các công trình nghiên cứu, bài viết nhấn mạnh bảo mật dữ liệu không chỉ là yêu cầu kỹ thuật mà còn gắn liền với yếu tố tổ chức, chính sách và đạo đức giáo dục. Bài báo đã phân tích mối quan hệ giữa công nghệ số và công tác bảo mật dữ liệu, những nguy cơ và thách thức đối với vấn đề bảo mật dữ liệu, đồng thời đề xuất các nguyên tắc và định hướng bảo mật dữ liệu cũng như hàm ý quản trị và hoạch định chính sách bảo mật dữ liệu trong giáo dục số.

Từ khóa: công nghệ số, bảo mật dữ liệu, hạ tầng giáo dục số, an toàn thông tin, chuyển đổi số

I. Đặt vấn đề

Trong bối cảnh chuyển đổi số quốc gia đang được đẩy mạnh, giáo dục được xác định là một trong những lĩnh vực then chốt, đóng vai trò tiên phong trong việc ứng dụng công nghệ số để đổi mới hoạt động dạy học và quản lý. Sự phát triển của hạ tầng giáo dục số cùng các nền tảng học tập trực tuyến, hệ thống quản lý học tập (LMS), kho học liệu điện tử và công cụ đánh giá trực tuyến đã mở ra cơ hội lớn nhằm nâng cao chất lượng, mở rộng khả năng tiếp cận tri thức và thúc đẩy công

bằng trong giáo dục. Tuy nhiên, đi kèm với đó là những thách thức nghiêm trọng về an toàn và bảo mật dữ liệu. Việc lưu trữ và xử lý khối lượng lớn dữ liệu cá nhân, dữ liệu học tập và quản trị trên môi trường số tiềm ẩn nguy cơ rò rỉ, truy cập trái phép và tấn công mạng, có thể làm suy giảm niềm tin xã hội đối với giáo dục số.

Xuất phát từ thực tiễn đó, nghiên cứu này hướng đến mục tiêu làm rõ cơ sở lý luận về công nghệ số và bảo mật dữ liệu trong giáo dục số, nhận diện các nguy cơ và thách thức, đồng thời xác định các

¹ Trường Đại học Mở Hà Nội

nguyên tắc và định hướng bảo mật cơ bản nhằm góp phần xây dựng hạ tầng giáo dục số an toàn, bền vững. Về mặt lý luận, bài báo bổ sung góc nhìn tích hợp giữa công nghệ số và bảo mật dữ liệu, coi đây là hai thành tố gắn bó hữu cơ trong hệ sinh thái giáo dục số. Về mặt thực tiễn, nghiên cứu đưa ra các hàm ý cho quản lý nhà trường và hoạch định chính sách, đồng thời đề xuất định hướng nhằm nâng cao nhận thức, năng lực vận hành và khung pháp lý cho bảo mật dữ liệu trong giáo dục.

Điểm mới của nghiên cứu là tập trung phân tích mối quan hệ giữa công nghệ số và bảo mật dữ liệu trong giáo dục số từ cả khía cạnh kỹ thuật, quản trị và đạo đức, thay vì chỉ dừng lại ở khía cạnh công nghệ. Trên cơ sở đó, bản thảo được triển khai theo cấu trúc: làm rõ một số khái niệm cơ bản; tổng quan nghiên cứu liên quan; trình bày phương pháp nghiên cứu; phân tích kết quả và thảo luận về mối quan hệ công nghệ số - bảo mật dữ liệu, những thách thức, nguyên tắc định hướng, cùng các hàm ý chính sách và quản lý.

II. Cơ sở lý luận

2.1. Một số khái niệm cơ bản

2.1.1. Công nghệ số

Theo tác giả Nambisan (2017), công nghệ số có thể được hiểu là tập hợp các công cụ và hệ thống số như điện toán đám mây, phân tích dữ liệu, cộng đồng trực tuyến, mạng xã hội, in 3D cung cấp khả năng tính toán, truyền thông và hợp tác hỗ trợ hoạt động sáng tạo/kinh doanh.

Theo Luật công nghiệp công nghệ số (2025): Công nghệ số là tập hợp các phương pháp khoa học, quy trình công nghệ, công cụ kỹ thuật để sản xuất, truyền đưa, thu thập, xử lý, lưu trữ, trao đổi thông tin, dữ liệu số và số hóa thể giới thực.

Từ hai định nghĩa trên, có thể hiểu, Công nghệ số là tập hợp các công cụ, hệ thống và thiết bị dựa trên dữ liệu số, cho phép thu thập, lưu trữ, xử lý, truyền tải và tái tạo thông tin nhằm hỗ trợ hoặc thay đổi hoạt động của con người và tổ chức.

Về hình thức, công nghệ số bao gồm các phần cứng như máy tính, điện thoại, máy chủ, thiết bị IoT, phần mềm (ứng dụng) như nền tảng học tập trực tuyến, mạng xã hội, công cụ phân tích dữ liệu, trò chơi số và hạ tầng số như internet, điện toán đám mây, blockchain.

Công nghệ số giúp biến đổi dữ liệu thành thông tin hữu ích, hỗ trợ ra quyết định, kết nối giao tiếp, tạo ra sản phẩm và dịch vụ mới.

Công nghệ số giữ vai trò nền tảng trong giáo dục số khi vừa là công cụ hỗ trợ vừa là động lực đổi mới. Nó giúp thay đổi phương pháp dạy và học thông qua lớp học ảo, hệ thống quản lý học tập, phần mềm tương tác, từ đó tăng tính chủ động và cá nhân hóa cho người học. Đồng thời, công nghệ số mở rộng khả năng tiếp cận tri thức, cho phép học tập mọi lúc, mọi nơi và kết nối với cộng đồng học tập toàn cầu. Ngoài ra, việc ứng dụng công nghệ số trong quản lý giáo dục giúp số hóa dữ liệu, phân tích quá trình học tập, đánh giá trực tuyến, góp phần nâng cao hiệu quả điều hành. Nhờ vậy, công nghệ số trở thành chìa khóa xây dựng một hệ sinh thái giáo dục số hiện đại, linh hoạt và hội nhập.

2.1.2. Bảo mật dữ liệu

Bảo mật dữ liệu (data security) thường được hiểu dựa trên mô hình CIA (Confidentiality - Integrity - Availability), tức là bảo đảm tính bí mật, toàn vẹn và sẵn sàng của thông tin (Chai & Zolkipli, 2021; Stallings, 2019).

Khái niệm này không chỉ giới hạn trong kỹ thuật, mà còn bao gồm yếu tố con

người, tổ chức và luật pháp. Trong giáo dục trực tuyến, bảo mật dữ liệu được hiểu là bảo vệ dữ liệu học tập và quản lý khỏi truy cập, sử dụng hoặc phá hủy trái phép, đồng thời bảo đảm quyền riêng tư và an toàn cho người học

Từ đó, có thể khái quát rằng: Bảo mật dữ liệu trong giáo dục số là tập hợp các biện pháp kỹ thuật, tổ chức và pháp lý nhằm bảo vệ dữ liệu học tập và quản lý khỏi truy cập, tiết lộ hoặc thay đổi trái phép, bảo đảm bí mật, toàn vẹn và sẵn sàng của thông tin.

Bảo mật dữ liệu giữ vai trò đặc biệt quan trọng trong giáo dục số, thể hiện ở ba khía cạnh then chốt. Trước hết, bảo mật dữ liệu giúp bảo vệ quyền riêng tư, ngăn chặn việc rò rỉ hay sử dụng trái phép thông tin cá nhân của người học và nhà giáo, từ đó đảm bảo an toàn cho mỗi cá nhân trong môi trường trực tuyến. Tiếp đến, bảo mật tốt góp phần duy trì sự ổn định của hệ thống giáo dục số, hạn chế các sự cố gián đoạn hay tấn công mạng có thể làm gián đoạn hoạt động dạy học. Quan trọng hơn, việc đảm bảo an toàn dữ liệu còn tạo dựng niềm tin cho người học, phụ huynh và toàn xã hội, củng cố sự tin cậy đối với các dịch vụ giáo dục số, qua đó thúc đẩy sự phát triển bền vững của mô hình này.

2.1.3. Giáo dục số

Theo University of Edinburgh (2023), giáo dục số là việc sử dụng sáng tạo các công cụ và công nghệ kỹ thuật số trong dạy và học, thường được gọi là học tập tăng cường bằng công nghệ (Technology Enhanced Learning) hoặc e-Learning.

Lynn và cộng sự (2022) định nghĩa giáo dục số là việc sử dụng và phát triển các công nghệ số cho dạy học trong giáo dục chính quy và phi chính quy, cùng với hạ tầng cần thiết để hỗ trợ việc triển khai.

Từ các quan niệm trên, trong nghiên cứu này, giáo dục số được hiểu là quá trình dạy và học ứng dụng công nghệ số, gắn với hạ tầng và nguồn lực số nhằm nâng cao chất lượng và khả năng tiếp cận giáo dục.

2.2. Lược khảo nghiên cứu liên quan

Trong những năm gần đây, vấn đề bảo mật dữ liệu trong giáo dục số được quan tâm ở cả khía cạnh lý luận và thực tiễn.

Một luồng nghiên cứu nổi bật tập trung vào vấn đề quyền riêng tư và bảo vệ dữ liệu trong learning analytics. Hoel (2018) nhấn mạnh cần thiết phải xác định các nguyên tắc đạo đức/giáo dục để điều chỉnh thu thập và xử lý dữ liệu học tập, nhằm cân bằng giữa khai thác dữ liệu phục vụ cải tiến giảng dạy và bảo vệ quyền lợi người học. Tiếp đó, tổng quan hệ thống của Liu và Khalil (2023) hệ thống hóa tám vấn đề xuyên suốt liên quan đến quyền riêng tư và bảo vệ dữ liệu trong học phân tích (learning analytics), bao gồm minh bạch, mục đích sử dụng, quyền truy cập và quản trị dữ liệu - cung cấp một khung phân tích hữu ích để đánh giá rủi ro và yêu cầu quản trị. Tác giả Phạm (2024) trong bài viết “Vai trò của dữ liệu số và những vấn đề đặt ra đối với dữ liệu số trong giáo dục, đào tạo” đã khẳng định “Bảo đảm quyền riêng tư và bảo mật của dữ liệu số là điều cần thiết để duy trì sự tin cậy và tuân thủ các quy định bảo vệ dữ liệu”. Tác giả đề xuất các nhà trường phải triển khai những biện pháp mạnh mẽ để bảo vệ thông tin và trao đổi minh bạch như: phân chia nhiệm vụ (SoD) để ngăn gian lận, xác thực hai yếu tố để chặn xâm nhập trái phép, và hợp tác với đơn vị chuyên trách an ninh mạng nhằm bảo đảm hệ thống an toàn, tránh rò rỉ dữ liệu.

Về khía cạnh kỹ thuật, nhiều nghiên cứu phân tích các rủi ro liên quan đến nền tảng học trực tuyến và LMS chạy trên nền

đám mây, đồng thời đề xuất giải pháp kỹ thuật như mã hóa, xác thực mạnh, kiểm soát truy cập và sao lưu an toàn. Chatterjee và cộng sự (2023) cung cấp đánh giá chi tiết về các lỗ hổng trên LMS đám mây và các mô hình bảo mật khả thi (cryptographic & steganographic approaches) để giảm thiểu rủi ro rò rỉ và tấn công. Những giải pháp kỹ thuật này thường được kết hợp với quy trình quản trị để đạt được hiệu quả bảo mật toàn diện. Tác giả Trịnh và Nguyễn (2024) đã nghiên cứu, trình bày cách mà blockchain có thể tích hợp vào quy trình bảo mật bài thi đối với một số môn thi thực hành tại phòng máy tính, nhấn mạnh vào việc xác thực danh tính, bảo vệ dữ liệu, chống gian lận và quản lý thông tin kết quả.

Về khung chính sách và quản trị, có những đề xuất khung tổng thể kết hợp chính sách, công nghệ và quy trình vận hành; Trong bài viết, “An ninh, bảo mật dữ liệu của học sinh và giáo viên: kinh nghiệm quốc tế và khuyến nghị” tác giả Hồng Anh (2024) đã nhấn mạnh các bài học về chính sách bảo vệ dữ liệu cá nhân, luật pháp và công nghệ như mã hóa, bảo vệ quyền riêng tư, từ đó đưa ra các khuyến nghị cho Việt Nam về xây dựng tiêu chuẩn bảo mật cho LMS, cải thiện hành lang pháp lý và nâng cao nhận thức người dùng. Ở cấp quốc gia, khung pháp luật và chiến lược an ninh mạng cũng ngày càng hoàn thiện, ví dụ các văn bản, kế hoạch hành động về an toàn-an ninh mạng và bảo vệ dữ liệu cá nhân tại Việt Nam (Bộ Thông tin và truyền thông, 2023; Chính phủ, 2022; Chính phủ, 2023), tạo bối cảnh pháp lý cần tính đến khi triển khai giải pháp kỹ thuật và quản trị trong trường đại học

III. Phương pháp nghiên cứu

Trong nghiên cứu này, tôi sử dụng phương pháp nghiên cứu lý luận, tập trung vào việc thu thập, phân tích và tổng hợp

các tài liệu, công trình khoa học, văn bản pháp lý và các nguồn tư liệu liên quan. Từ đó, nghiên cứu tiến hành hệ thống hóa cơ sở lý luận, làm rõ các khái niệm, nguyên tắc và mối quan hệ giữa công nghệ số và công tác bảo mật dữ liệu trong giáo dục số. Việc phân tích, so sánh và khái quát hóa các nguồn tư liệu giúp hình thành khung lý thuyết, đồng thời tạo nền tảng khoa học để rút ra kết luận và đề xuất các hàm ý quản lý, chính sách phù hợp.

IV. Kết quả nghiên cứu và thảo luận

4.1. Mối quan hệ giữa công nghệ số và bảo mật dữ liệu trong giáo dục số

Công nghệ số vừa mở ra cơ hội đổi mới, vừa tạo ra thách thức nghiêm trọng về bảo mật dữ liệu. Các nền tảng học tập trực tuyến, kho học liệu điện tử và hệ thống thi trực tuyến giúp quản lý hiệu quả hơn, cá nhân hóa học tập và mở rộng khả năng tiếp cận tri thức. Nhưng đồng thời, việc thu thập, lưu trữ và xử lý khối lượng lớn dữ liệu cá nhân và học tập trên môi trường số khiến nguy cơ rò rỉ, truy cập trái phép hoặc tấn công mạng gia tăng. Như vậy, bảo mật dữ liệu trở thành điều kiện tiên quyết để đảm bảo tính bền vững và giữ vững niềm tin vào giáo dục số.

4.2. Những nguy cơ và thách thức đặt ra

Trong bối cảnh giáo dục số, một trong những nguy cơ lớn nhất là tình trạng rò rỉ dữ liệu cá nhân và học tập của học sinh, sinh viên và giảng viên. Các dữ liệu này thường bao gồm thông tin định danh, điểm số, kết quả kiểm tra, thậm chí cả lịch sử học tập và trao đổi trực tuyến. Khi bị lộ thông tin, chúng có thể bị sử dụng trái phép vào mục đích thương mại hoặc gian lận học thuật, gây tổn hại đến quyền riêng tư và uy tín của người học.

Bên cạnh đó, các hệ thống quản lý học tập (LMS), kho học liệu điện tử và hạ tầng điện toán đám mây cũng thường xuyên phải đối mặt với nguy cơ tấn công mạng. Các cuộc tấn công từ chối dịch vụ (DDoS), xâm nhập bất hợp pháp hoặc cài đặt mã độc có thể làm gián đoạn quá trình dạy - học, thậm chí phá hủy cơ sở dữ liệu quan trọng. Theo báo cáo của EDUCAUSE (2021), số lượng sự cố an ninh mạng trong giáo dục đại học toàn cầu đã gia tăng đáng kể trong giai đoạn dịch COVID-19, khi các trường đồng loạt chuyển sang môi trường trực tuyến.

Bên cạnh đó, phần mềm mã hóa dữ liệu tổng tiền, lừa đảo trực tuyến và lây nhiễm phần mềm độc hại, mất an toàn từ các mối đe dọa sẵn có như thiết bị không được bảo mật, sử dụng mật khẩu yếu... đều là những nguy cơ đe dọa cho an toàn thông tin trong bối cảnh giáo dục số (Lê, 2024)

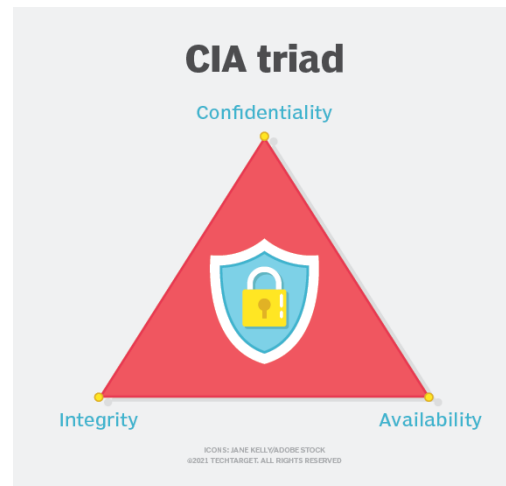
Ngoài yếu tố kỹ thuật, thiếu hụt nhận thức và kỹ năng bảo mật của người dùng cũng là một thách thức lớn. Nhiều giảng viên và sinh viên chưa được đào tạo bài bản về cách sử dụng mật khẩu an toàn, phát hiện email giả mạo (phishing) hay bảo vệ thiết bị cá nhân, dẫn đến việc vô tình tạo ra lỗ hổng cho kẻ xấu khai thác.

Cuối cùng, cần nhấn mạnh đến sự chưa đồng bộ của chính sách và hành lang pháp lý. Tại nhiều quốc gia, bao gồm cả Việt Nam, các quy định về bảo mật dữ liệu trong giáo dục vẫn còn phân tán, thiếu chuẩn thống nhất áp dụng cho LMS, hệ thống thi trực tuyến hay kho học liệu số. Điều này dẫn đến sự khó khăn trong triển khai đồng bộ các biện pháp bảo mật, cũng như hạn chế khả năng hợp tác quốc tế trong lĩnh vực này (Liu & Khalil, 2023).

4.3. Nguyên tắc và định hướng bảo mật dữ liệu trong giáo dục số

Từ các công trình nghiên cứu, có thể rút ra các nguyên tắc cơ bản và định hướng:

- Nguyên tắc CIA: đảm bảo dữ liệu bí mật, toàn vẹn và sẵn sàng truy cập khi cần - yếu tố cốt lõi trong bảo mật dữ liệu. Tính bí mật tức là thông tin chỉ được phép truy cập bởi những đối tượng có thẩm quyền; tính toàn vẹn nghĩa là dữ liệu phải chính xác, đầy đủ và không bị thay đổi trái phép và tính sẵn sàng tức là hệ thống dữ liệu phải luôn có thể truy cập được khi cần. Mô hình CIA này được coi là nền tảng cho mọi giải pháp bảo mật thông tin, trong đó có lĩnh vực giáo dục số (Stallings, 2019).



Hình 1. Mô hình bảo mật thông tin CIA (Hashemi-Pour & Chai, 2023)

- Nguyên tắc kết hợp kỹ thuật và quản trị: Các giải pháp kỹ thuật như mã hóa dữ liệu, xác thực đa yếu tố, kiểm soát truy cập hay sao lưu an toàn cần được triển khai đồng bộ với các biện pháp quản trị như quy trình phân quyền, kiểm toán nội bộ và giám sát thường xuyên.

- Bảo mật dữ liệu cần tuân thủ nguyên tắc minh bạch và pháp lý. Các cơ sở giáo dục phải minh bạch trong việc thông báo cho người học và nhà giáo về mục đích, phạm vi cũng như trách nhiệm khi thu thập và xử lý dữ liệu. Đồng thời các tổ chức này

phải tuân thủ hệ thống pháp luật quốc gia và tham chiếu các chuẩn mực quốc tế về bảo vệ dữ liệu. Theo Liu và Khalil (2023), minh bạch và tuân thủ pháp lý chính là yếu tố nền tảng để cân bằng giữa khai thác dữ liệu phục vụ cải tiến giảng dạy và bảo vệ quyền riêng tư của người học.

- Nguyên tắc lấy người học làm trung tâm là một nguyên tắc quan trọng trong bảo mật dữ liệu trong giáo dục số. Bảo mật dữ liệu trong giáo dục số không chỉ nhằm duy trì an toàn cho hệ thống mà còn bảo vệ quyền lợi, quyền riêng tư và niềm tin của người học. Khi người học cảm thấy thông tin cá nhân và dữ liệu học tập được bảo vệ an toàn, họ sẽ tin tưởng và chủ động tham gia tích cực hơn vào các hoạt động dạy - học trực tuyến. Đây là một trong những yếu tố quyết định để giáo dục số phát triển bền vững và được xã hội chấp nhận rộng rãi.

4.4. Hàm ý cho công tác quản lý và hoạch định chính sách

Từ những phân tích trên, có thể rút ra một số hàm ý quan trọng cho công tác quản lý và hoạch định chính sách trong giáo dục số.

Ở cấp cơ sở giáo dục, các trường đại học, cao đẳng và tổ chức đào tạo cần xây dựng và ban hành quy chế bảo mật dữ liệu nội bộ. Các quy chế này không chỉ quy định rõ trách nhiệm của từng cá nhân trong việc bảo vệ dữ liệu, mà còn thiết lập quy trình xử lý khi xảy ra sự cố. Đồng thời, việc tập huấn nâng cao nhận thức và kỹ năng an toàn thông tin cho giảng viên và sinh viên cần được tiến hành thường xuyên, kết hợp với đầu tư hạ tầng an ninh mạng hiện đại nhằm giảm thiểu rủi ro.

Ở cấp quản lý nhà nước, cần ban hành chính sách đồng bộ và thống nhất về an toàn dữ liệu trong giáo dục, trong đó quy định rõ tiêu chuẩn bảo mật đối với

hệ thống LMS, kho học liệu số, cũng như các nền tảng thi trực tuyến. Các tiêu chuẩn này phải dựa trên thông lệ quốc tế, đồng thời phù hợp với bối cảnh trong nước. Như khuyến nghị của OECD (2021), việc thiết lập chuẩn quốc gia cho hạ tầng số trong giáo dục là điều kiện tiên quyết để đảm bảo công bằng, bền vững và an toàn trong quá trình chuyển đổi số.

Ở cấp quốc tế và hợp tác, Việt Nam cần chủ động tham khảo và học hỏi kinh nghiệm từ các quốc gia đi trước, đồng thời từng bước hài hòa hóa quy định pháp luật trong nước với chuẩn mực quốc tế. Một ví dụ điển hình là Quy định bảo vệ dữ liệu chung (GDPR) của Liên minh châu Âu, vốn đang trở thành chuẩn mực toàn cầu về bảo mật dữ liệu. Việc tham chiếu và vận dụng linh hoạt các nguyên tắc của GDPR sẽ giúp nâng cao tính tương thích của hệ thống giáo dục Việt Nam trong bối cảnh hội nhập quốc tế.

4.5. Thảo luận

Kết quả nghiên cứu khẳng định rằng bảo mật dữ liệu giữ vai trò trung tâm trong tiến trình phát triển giáo dục số. Bảo mật không chỉ là khía cạnh kỹ thuật mà còn mang tính quản trị và đạo đức. Các sự cố rò rỉ dữ liệu trong thực tế cho thấy nếu thiếu biện pháp bảo mật chặt chẽ, niềm tin của người học, phụ huynh và xã hội vào hệ thống giáo dục số có thể bị tổn thương nghiêm trọng.

Trong bối cảnh Việt Nam, việc xây dựng khung pháp lý bảo vệ dữ liệu cá nhân trong giáo dục còn nhiều hạn chế và các cơ sở giáo dục thường thiếu nguồn lực hoặc chuyên môn để thực hiện đầy đủ các giải pháp kỹ thuật và quản trị bảo mật. Để làm rõ mức độ hoàn thiện của khung pháp lý trong nước so với chuẩn mực quốc tế, bảng dưới đây trình bày so sánh các nguyên tắc bảo mật dữ liệu giữa Việt Nam và các quy định quốc tế (GDPR/OECD).

Bảng 1. So sánh nguyên tắc bảo mật giữa Việt Nam và quốc tế (GDPR (EU)/OECD)

Tiêu chí	Việt Nam - Nghị định 13/2023/NĐ-CP	GDPR (EU)/OECD
Cơ sở pháp lý	Quy định bảo vệ dữ liệu cá nhân, hiệu lực từ 01/7/2023	GDPR (EU) là luật bắt buộc; OECD ban hành nguyên tắc khuyến nghị.
Quyền của chủ thể dữ liệu	Có 11 quyền: được biết, truy cập, chỉnh sửa, xóa, phản đối, rút lại đồng ý, khiếu nại, bồi thường...	Quyền toàn diện: được quên, phản đối, hạn chế xử lý, di chuyển dữ liệu, khiếu nại...
Mức độ chế tài	Có xử phạt hành chính và trách nhiệm dân sự; chưa có mức phạt cao như GDPR.	Phạt tới 20 triệu EUR hoặc 4% doanh thu toàn cầu.
Tiêu chuẩn bảo mật	Yêu cầu biện pháp kỹ thuật phù hợp, chưa quy định chuẩn ISO hay LMS cụ thể.	Thường áp dụng ISO/IEC 27001 như chuẩn tham chiếu bảo mật.
Nguyên tắc xử lý & giám sát	Yêu cầu minh bạch, thông báo cho người dùng; chưa có cơ quan giám sát độc lập riêng.	Bắt buộc thông báo vi phạm trong 72h; có cơ quan giám sát độc lập ở mỗi nước EU.
Chuyển dữ liệu ra nước ngoài	Có quy định điều kiện và trách nhiệm bảo đảm an toàn khi chuyển dữ liệu.	Quy định chặt chẽ: chỉ chuyển khi có cơ chế bảo vệ thích hợp (Adequacy, SCCs...).

Từ kết quả so sánh trên, có thể thấy việc đối chiếu giữa quy định trong nước và chuẩn mực quốc tế là cơ sở quan trọng để định hướng xây dựng các giải pháp lý luận và thực tiễn cho phát triển hạ tầng giáo dục số an toàn và bền vững. Bài nghiên cứu này góp phần bổ sung góc nhìn lý luận về cách thức kết hợp công nghệ, chính sách và nhận thức người dùng để triển khai hạ tầng giáo dục số một cách an toàn, bền vững và đáng tin cậy.

V. Kết luận và kiến nghị

Kết quả nghiên cứu đã khẳng định rằng công nghệ số vừa là nền tảng, vừa là động lực thúc đẩy đổi mới giáo dục, song đồng thời cũng đặt ra những thách thức phức tạp về bảo mật dữ liệu. Đối chiếu với các nghiên cứu trước đây của Hoel (2018), Liu và Khalil (2023) hay Chatterjee và cộng sự (2023), có thể thấy xu hướng chung là nhấn mạnh tính cấp thiết của việc bảo vệ dữ liệu trong bối cảnh học tập trực tuyến và phân tích học tập (learning analytics). Tuy nhiên, bài báo này bổ sung một góc nhìn tích hợp hơn khi chỉ ra rằng bảo mật dữ liệu trong giáo dục số không thể chỉ dựa vào giải pháp kỹ thuật, mà cần được đặt trong mối quan hệ hữu cơ giữa

công nghệ, quản trị, chính sách pháp lý và yếu tố con người.

Từ những kết quả đạt được, nghiên cứu gợi ý một số định hướng chính.

Thứ nhất, ở cấp cơ sở giáo dục:

- Thiết lập quy trình bảo mật dữ liệu toàn diện, bao gồm quy định phân quyền truy cập, kiểm toán định kỳ và cơ chế ứng phó sự cố an ninh mạng.

- Triển khai giải pháp kỹ thuật bảo mật hiện đại như mã hóa dữ liệu, xác thực đa yếu tố (MFA), sao lưu an toàn và giám sát truy cập theo thời gian thực.

- Thành lập tổ chuyên trách an toàn thông tin trong nhà trường, chịu trách nhiệm quản lý, đào tạo và phản ứng khi xảy ra sự cố.

- Tổ chức bồi dưỡng, tập huấn định kỳ cho giảng viên, sinh viên và cán bộ kỹ thuật về nhận thức và kỹ năng bảo mật dữ liệu.

- Khuyến khích các trường áp dụng tiêu chuẩn ISO/IEC 27001 trong quản lý dữ liệu học tập và quản trị hệ thống.

Thứ hai, cấp bộ, ngành quản lý:

- Xây dựng và hoàn thiện khung pháp lý về bảo mật dữ liệu trong giáo dục

số, đảm bảo đồng bộ giữa Bộ Giáo dục và Đào tạo với Bộ Thông tin và Truyền thông.

- Ban hành quy chuẩn kỹ thuật quốc gia (QCVN) về bảo mật dữ liệu giáo dục, áp dụng cho hệ thống LMS, kho học liệu số và nền tảng thi trực tuyến.

- Thiết lập cơ chế kiểm định, đánh giá định kỳ đối với các hệ thống quản lý học tập và dịch vụ số trong cơ sở giáo dục.

- Xây dựng chương trình đào tạo và cấp chứng chỉ an toàn thông tin trong giáo dục, hướng đến đội ngũ quản lý, kỹ thuật viên và giảng viên phụ trách hạ tầng số.

- Thúc đẩy chuyển giao công nghệ và hợp tác nghiên cứu giữa các cơ sở giáo dục với doanh nghiệp công nghệ trong lĩnh vực an ninh mạng.

Thứ ba, ở cấp quốc gia:

- Xây dựng Chiến lược bảo mật dữ liệu giáo dục quốc gia như một hợp phần trong Chiến lược chuyển đổi số quốc gia, gắn với Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.

- Thiết lập cơ sở dữ liệu quốc gia về sự cố an ninh mạng trong giáo dục, làm căn cứ cho việc cảnh báo, dự báo và xây dựng chính sách phòng ngừa.

- Tăng cường hợp tác công - tư (PPP) giữa Nhà nước, doanh nghiệp và cơ sở giáo dục nhằm chia sẻ giải pháp, kinh nghiệm và nguồn lực bảo mật.

- Tham chiếu và hài hòa hóa quy định pháp luật Việt Nam với chuẩn mực quốc tế như GDPR (EU) và nguyên tắc của OECD, hướng đến sự tương thích trong quản lý và bảo vệ dữ liệu.

- Khuyến khích các dự án thử nghiệm (sandbox) ứng dụng công nghệ mới như AI, blockchain, điện toán đám mây an toàn trong quản lý dữ liệu học tập và thi cử.

Như vậy, nghiên cứu đã đạt được mục tiêu đề ra khi làm rõ mối quan hệ giữa công nghệ số và bảo mật dữ liệu trong giáo dục số, nhận diện nguy cơ - thách thức, đề xuất nguyên tắc định hướng và đưa ra hàm ý quản lý. Những kiến nghị này không chỉ có ý nghĩa lý luận, góp phần bổ sung khung phân tích cho nghiên cứu về giáo dục số mà còn có giá trị thực tiễn trong việc định hướng chính sách và triển khai chuyển đổi số trong giáo dục theo hướng an toàn, bền vững và lấy người học làm trung tâm.

Tài liệu tham khảo

- [1]. Bộ Thông tin và Truyền thông. (2023, ngày 06 tháng 04). *Quyết định số 566/QĐ-BTTTT về Kế hoạch hành động thực hiện Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030*. Hà Nội: Bộ TT&TT. Truy cập từ Caselaw Việt Nam. <https://caselaw.vn/van-ban-phap-luat/507995-quyet-dinh-so-566-qd-btttt-ngay-06-04-2023>
- [2]. Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity, and Availability in Information Security. *Journal of ICT in Education*, 8(2), 34-42. <https://doi.org/10.37134/jictie.vol8.2.4.2021>
- [3]. Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing Data Security of Cloud-Based LMS. *International Journal of Emerging Technologies in Learning (iJET)*. <https://pmc.ncbi.nlm.nih.gov/articles/PMC10023308>.
- [4]. Chính phủ nước Cộng hòa Xã hội Chủ nghĩa Việt Nam. (2022, ngày 10 tháng 08). *Quyết định số 964/QĐ-TTg phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030*. Hà Nội: Văn phòng Chính phủ.

- [5]. Chính phủ. (2023). *Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân*. Hà Nội: Chính phủ nước Cộng hòa Xã hội Chủ nghĩa Việt Nam.
- [6]. Chính phủ nước Cộng hòa Xã hội Chủ nghĩa Việt Nam. (2023, ngày 17 tháng 4). *Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân*. Hà Nội: Chính phủ. <https://vanban.chinhphu.vn/?pageid=27160&docid=209481>.
- [7]. EDUCAUSE. (2021). *Report Tackles Cybersecurity and Privacy in Higher Ed*. <https://thejournal.com/edu/campus-technology/articles/2021/03/09/educase-report-tackles-cybersecurity-and-privacy-in-higher-ed.aspx>.
- [8]. European Union. (2016, April 27). *General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council)*. Official Journal of the European Union, L119, 1-88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [9]. Hashemi-Pour, C., & Chai, W. (2023). *What is the CIA triad (confidentiality, integrity, and availability)?* <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?>
- [10]. Hoel, T. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim-towards a proposal. *International Journal of Educational Technology in Higher Education*, 15(1), 20. <https://doi.org/10.1186/s41039-018-0086-8>.
- [11]. Hồng Anh. (2024). An ninh, bảo mật dữ liệu của học sinh và giáo viên: Kinh nghiệm quốc tế và khuyến nghị. *Tạp chí Giáo dục*.
- [12]. Lê, T. P. (2024). Một số vấn đề bảo mật và an toàn thông tin trong nhà trường. *Journal of Educational Equipment: Applied Research*, 1(316).
- [13]. Liu, Q., & Khalil, M. (2023). Understanding privacy and data protection issues in learning analytics using a systematic review. *British Journal of Educational Technology*, 54(6), 1715-1747. <https://doi.org/10.1111/bjet.13325>.
- [14]. Lynn, T., Rosati, P., Conway, E., Curran, K., & Fox, G. (2022). Digital education. In T. Lynn, J. Mooney, P. Rosati, & M. Cummins (Eds.), *Disruptive technologies for business and society* (pp. 155-174). Springer. https://doi.org/10.1007/978-3-030-91247-5_7.
- [15]. Nambisan, S. (2017). Digital entrepreneurship: Toward a digital technology perspective of entrepreneurship. *Entrepreneurship Theory and Practice*, 41(6), 1029-1055. <https://doi.org/10.1111/etap.12254>.
- [16]. OECD. (2021). *Shaping Digital Education: Enabling Factors for Quality, Equity and Efficiency* (Chapter: Accessible, Innovative and High-Quality Infrastructure for Digital Education). Paris: OECD Publishing. <https://doi.org/10.1787/bac4dc9f-en>.
- [17]. Phạm, T. H. T. (2024). Vai trò của dữ liệu số và những vấn đề đặt ra đối với dữ liệu số trong giáo dục, đào tạo. *Tạp chí Quản lý Nhà nước*, 342(7).
- [18]. Stallings, W. (2019). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Addison-Wesley Professional.
- [19]. Trịnh, T. P., & Nguyễn, T. H. (2024). Áp dụng công nghệ Blockchain trong quy trình bảo mật bài thi thực hành tại phòng máy tính. *Tạp chí Khoa học Trường Đại học Hồng Đức*, 71(11), 92-100. <https://doi.org/10.70117/hdujs.2.2024.745>.
- [20]. University of Edinburgh. (2023). *What is digital education? The University of Edinburgh*. <https://edwebprofiles.ed.ac.uk/institute-academic-development/learning-teaching/staff/digital-ed/what-is-digital-education>.

DIGITAL TECHNOLOGY AND DATA SECURITY IN DIGITAL EDUCATION

Bui Thi Lu², Tran Thi Huong Ly², Dang Thuy Huong²

Abstract: *The rapid development of digital technology has opened up many opportunities for innovation in education, but it also poses major challenges for data security and information safety. The article analyzes the theoretical foundations, pointing out the risks of personal data leakage, cyberattacks, and privacy violations in the implementation of digital education. Based on a synthesis of existing research, the paper emphasizes that data security is not only a technical requirement but is also closely tied to organizational, policy, and educational ethics factors. The article examines the relationship between digital technology and data security, identifies risks and challenges to data protection, and proposes key principles and directions for data security, as well as governance and policy implications for ensuring data security in digital education.*

Keywords: *digital technology, data security, digital education infrastructure, information safety, digital transformation*

² Hanoi Open University