BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA NGƯỜI HỌC TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ GIÁO DỤC

Trần Tuấn Cảnh, Nguyễn Linh Phong
Trường Đại học Tôn Đức Thắng
Trường Đại học Sư phạm Thành phố Hồ Chí Minh
Email: trantuancanh@tdtu.edu.vn

Tóm tắt: *Sự phát triển của chuyển đổi số đang làm thay đổi phương thức quản lý và tổ chức hoạt động giáo dục, kéo theo việc thu thập và sử dụng ngày càng nhiều dữ liệu cá nhân của người học. Bên cạnh những lợi ích trong quản lý và hỗ trợ học tập, quá trình này cũng đặt ra không ít rủi ro liên quan đến quyền riêng tư và bảo mật thông tin. Bài viết tập trung làm rõ đặc điểm của dữ liệu cá nhân trong môi trường giáo dục số, phân tích thực trạng bảo vệ dữ liệu của người học tại Việt Nam và nhận diện những thách thức phát sinh trong quá trình thu thập, lưu trữ và khai thác dữ liệu. Trên cơ sở đó, bài viết đề xuất một số giải pháp nhằm nâng cao hiệu quả bảo vệ dữ liệu cá nhân của người học, góp phần xây dựng môi trường giáo dục số an toàn và bền vững.*

Từ khóa: *Bảo vệ dữ liệu, Chuyển đổi số giáo dục, Dữ liệu cá nhân, Người học, Quyền riêng tư.*

PROTECTING STUDENTS' PERSONAL DATA IN THE CONTEXT OF DIGITAL TRANSFORMATION IN EDUCATION

Abstract: *The development of digital transformation is changing the way educational management and organization are conducted, leading to the increasing collection and use of students' personal data. Besides the benefits in management and learning support, this process also poses significant risks related to privacy and information security. This article focuses on clarifying the characteristics of personal data in the digital education environment, analyzing the current state of student data protection in Vietnam, and identifying the challenges arising in the process of data collection, storage, and exploitation. Based on this, the article proposes several solutions to improve the effectiveness of protecting learners' personal data, contributing to building a safe and sustainable digital education environment.*

Keywords: *Data protection, Digital transformation in education, Personal data, Learners, Privacy.*

Nhận bài: 11/04/2026 *Phản biện: 12/05/2026* *Duyệt đăng: 15/05/2026*

I. ĐẶT VẤN ĐỀ

Chuyển đổi số đang trở thành một trong những động lực quan trọng của quá trình đổi mới giáo dục. Tại Việt Nam, chủ trương này được thúc đẩy thông qua Quyết định số 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ về tăng cường ứng dụng công nghệ thông tin và chuyển đổi số trong giáo dục và đào tạo giai đoạn 2022-2025, định hướng đến năm 2030. Trong cùng bối cảnh, Chương trình Chuyển đổi số quốc gia cũng đặt giáo dục vào nhóm lĩnh vực ưu tiên chuyển đổi số, qua đó khuyến khích việc số hóa hồ sơ, tích hợp dữ liệu, cung cấp dịch vụ công trực tuyến và tăng cường năng lực phân tích, dự báo trong quản lý nhà nước (Thủ tướng Chính phủ, 2020).

Quá trình này đồng thời làm gia tăng đáng kể việc thu thập, lưu trữ và xử lý dữ liệu của người học. Dữ liệu không chỉ bao gồm các thông tin nhận dạng cơ bản mà còn phản ánh kết quả học tập, quá trình tương tác trên môi trường số và nhiều đặc điểm cá nhân khác. Trong điều kiện dữ liệu được chia sẻ và khai thác thông qua nhiều hệ thống công nghệ, nguy cơ xâm phạm quyền riêng tư hoặc sử dụng dữ liệu ngoài mục đích giáo dục cũng ngày càng rõ nét.

Nhận thức được yêu cầu bảo vệ dữ liệu cá nhân (sau đây viết tắt là "DLCN") trong xã hội số, Việt Nam đã từng bước hoàn thiện khung pháp lý thông qua Luật Bảo vệ dữ liệu cá nhân năm 2025 (sau đây viết tắt là "Luật BVDLCN"). Bên cạnh đó, các quy định trong Luật Trẻ em năm 2016, Luật An toàn thông tin mạng năm 2015, Luật An ninh mạng năm 2018, Bộ luật Dân sự năm 2015 và Luật Giáo dục năm 2019 cũng tạo cơ sở pháp lý cho việc bảo vệ quyền riêng tư và thông tin của người học. Tuy nhiên, các quy định hiện hành chủ yếu mang tính khung và chưa phản ánh đầy đủ những đặc thù của hoạt động xử lý dữ liệu trong môi trường giáo dục số.

Xuất phát từ thực tiễn đó, bài viết tập trung làm rõ đặc điểm của DLCN của người học trong môi trường chuyển đổi số giáo dục, phân tích thực trạng bảo vệ dữ liệu trong các cơ sở giáo dục ở Việt Nam, đồng thời nhận diện những thách thức đặt ra đối với hoạt động thu thập, quản lý và khai thác dữ liệu. Trên cơ sở đó, bài viết đưa ra một số kiến nghị nhằm tăng cường bảo vệ DLCN của người học, góp phần xây dựng môi trường giáo dục số an toàn, tin cậy và phát triển bền vững.

II. NỘI DUNG NGHIÊN CỨU

2.1. Đặc thù của dữ liệu cá nhân của người học trong môi trường giáo dục số

Theo Luật BVDLCN và Nghị định 356/2025/NĐ-CP, dữ liệu cá nhân (DLCN) bao gồm dữ liệu cơ bản và dữ liệu nhạy cảm. Trong môi trường giáo dục số, DLCN của người học được thu thập và xử lý xuyên suốt quá trình từ tuyển sinh, quản lý đào tạo đến dạy học trực tuyến, không chỉ gồm thông tin định danh mà còn mở rộng sang dữ liệu học tập, hành vi và dữ liệu nhạy cảm.

Có thể khái quát DLCN của người học thành bốn nhóm chính. Thứ nhất là dữ liệu định danh như họ tên, ngày sinh, giới tính, mã số sinh viên, thông tin liên hệ và người giám hộ, phục vụ quản lý hành chính và học vụ. Thứ hai là dữ liệu học tập, bao gồm kết quả học tập, điểm số, chuyên cần, khen thưởng, kỷ luật và tiến trình học tập, phản ánh toàn bộ quá trình học thay vì chỉ kết quả cuối cùng.

Thứ ba là dữ liệu hành vi, phát sinh từ việc người học tương tác với các nền tảng số như LMS, lớp học trực tuyến hay hệ thống thi cử, bao gồm thời gian truy cập, lịch sử học tập, mức độ tham gia hoạt động và dấu vết số trong quá trình học. Đây là loại dữ liệu mới, có giá trị lớn trong phân tích và quản trị giáo dục số.

Thứ tư là dữ liệu cá nhân nhạy cảm, bao gồm thông tin sức khỏe, dữ liệu sinh trắc học (khuôn mặt, vân tay, giọng nói), hình ảnh và các thông tin liên quan đến hoàn cảnh cá nhân. Đây là nhóm dữ liệu có mức độ rủi ro cao khi bị xâm phạm.

So với nhiều lĩnh vực khác, dữ liệu của người học có tính đặc thù cao do phần lớn chủ thể là trẻ em hoặc người chưa thành niên, vốn là nhóm dễ bị tổn thương và hạn chế về nhận thức rủi ro dữ liệu. Đồng thời, dữ liệu giáo dục còn phản ánh quá trình phát triển dài hạn của cá nhân, có thể được sử dụng để xây dựng hồ sơ số toàn diện về năng lực, hành vi và xu hướng học tập.

Từ đó cho thấy, DLCN của người học là hệ thống dữ liệu đa dạng, bao gồm dữ liệu định danh, học tập, hành vi và nhạy cảm, đòi hỏi cơ chế bảo vệ riêng, phù hợp với đặc thù của môi trường giáo dục số và yêu cầu chuyển đổi số hiện nay.

2.2. Thực trạng bảo vệ dữ liệu cá nhân của người học trong hoạt động giáo dục số ở Việt Nam

Về khâu thu thập dữ liệu, các cơ sở giáo dục hiện nay thu thập dữ liệu người học qua nhiều kênh. Kênh truyền thống là hồ sơ nhập học, hồ sơ học vụ, hồ sơ tài chính, hồ sơ khen thưởng - kỷ luật và hồ sơ liên quan đến phụ huynh hoặc người giám hộ. Kênh số bao gồm cổng thông tin sinh viên, hệ thống quản lý đào tạo, LMS, ứng dụng di động, lớp học trực tuyến, hệ thống khảo thí, thư điện tử, cổng thanh toán, hệ thống thư viện, ký túc xá, camera an ninh, hệ thống điểm danh và các nền tảng khảo sát. Trong giáo dục phổ thông, Thông tư số 09/2021/TT-BGDĐT "quy định về quản lý và tổ chức dạy học trực tuyến", qua đó chính thức hóa nhiều hoạt động giáo dục trên môi trường số. Trong giáo dục đại học, các cơ sở đào tạo chủ động triển khai nền tảng LMS, hệ thống học liệu số, phần mềm khảo thí và các công cụ quản lý sinh viên theo yêu cầu quản trị riêng.

Tuy nhiên, vấn đề đặt ra là nhiều hoạt động thu thập dữ liệu chưa được giải thích đầy đủ về mục đích, phạm vi, thời hạn lưu trữ và chủ thể được tiếp cận. Người học thường chỉ biết rằng phải cung cấp thông tin hoặc phải dùng một phần mềm nhất định, nhưng không biết dữ liệu sẽ được xử lý trong bao lâu, có được chuyển cho bên thứ ba hay không, có dùng cho phân tích học tập, quảng bá, nghiên cứu hay huấn luyện thuật toán hay không. Một số biểu mẫu thu thập thông tin trong nhà trường có xu hướng yêu cầu nhiều trường dữ liệu hơn mức cần thiết. Một số hoạt động điểm danh, nhận diện hoặc giám sát thi trực tuyến có thể thu thập dữ liệu sinh trắc học, hình ảnh, âm thanh hoặc không gian riêng tư của người học mà chưa có quy trình đánh giá tác động rõ ràng. Theo nguyên tắc tối thiểu hóa dữ liệu của GDPR, dữ liệu phải phù hợp, liên quan và giới hạn ở mức cần thiết so với mục đích xử lý (European Union, 2016).

Một biểu hiện đáng chú ý trong khâu thu thập là sử dụng công nghệ nhận diện khuôn mặt hoặc sinh trắc học để điểm danh, kiểm soát ra vào, tổ chức thi hoặc xác thực danh tính. Về mặt quản lý, công nghệ này có thể giảm gian lận và tiết kiệm thời gian. Nhưng về mặt bảo vệ dữ liệu, dữ liệu sinh trắc học là dữ liệu nhạy cảm vì gắn chặt với cơ thể và khó thay đổi nếu bị lộ. Mật khẩu có thể đổi, thẻ sinh viên có thể cấp lại, nhưng khuôn mặt, vân tay hoặc giọng nói thì không thể thay thế theo cách tương tự. Nghiên cứu pháp lý về dữ liệu nhạy cảm ở Việt Nam đã chỉ ra rằng dữ liệu sinh trắc học cần cơ chế bảo vệ tăng cường và không nên bị xử lý theo cùng mức độ với thông tin hành chính thông thường (Nguyễn Văn Cương, 2020). Vì vậy, nếu cơ sở giáo dục sử dụng công nghệ này, cần có căn cứ pháp lý rõ, đánh giá rủi ro, lựa chọn công nghệ bảo mật, quy định thời hạn lưu trữ, giới

hạn người truy cập và cơ chế thay thế cho người học có lý do chính đáng không thể hoặc không muốn sử dụng.

Về khâu lưu trữ và quản lý dữ liệu, xu hướng hiện nay là dữ liệu người học được lưu trữ tập trung trong hệ thống quản lý đào tạo, cơ sở dữ liệu nội bộ, máy chủ trường hoặc dịch vụ điện toán đám mây. Việc lưu trữ tập trung có ưu điểm là giúp đồng bộ, tránh phân mảnh, hỗ trợ báo cáo và tích hợp dữ liệu. Nhưng tập trung dữ liệu cũng làm tăng hậu quả nếu xảy ra sự cố. Một tài khoản quản trị bị lộ, một máy chủ cấu hình sai, một đối tác công nghệ thiếu bảo mật hoặc một nhân sự nội bộ truy cập vượt quyền có thể ảnh hưởng đến dữ liệu của hàng nghìn, thậm chí hàng chục nghìn người học. Luật An toàn thông tin mạng năm 2015 yêu cầu "tổ chức, cá nhân xử lý thông tin cá nhân phải áp dụng biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin do mình thu thập, lưu trữ". Luật BVDLCN cũng yêu cầu bên kiểm soát dữ liệu áp dụng biện pháp tổ chức và kỹ thuật, ghi lại nhật ký hệ thống quá trình xử lý dữ liệu, lựa chọn bên xử lý dữ liệu phù hợp và bảo đảm quyền của chủ thể dữ liệu.

Về khâu chia sẻ và khai thác dữ liệu, chuyển đổi số giáo dục khiến dữ liệu người học không còn nằm hoàn toàn trong phạm vi nội bộ nhà trường. Cơ sở giáo dục có thể chia sẻ dữ liệu với cơ quan quản lý nhà nước, đơn vị cung cấp hệ thống quản lý học tập, dịch vụ email, nền tảng họp trực tuyến, các phần mềm khảo thí, dịch vụ thanh toán, thư viện số, đối tác thực tập, tổ chức kiểm định, nhà tài trợ học bổng, công ty công nghệ giáo dục hoặc nhóm nghiên cứu. Chia sẻ dữ liệu có thể hợp pháp và cần thiết, nhưng phải dựa trên mục đích rõ ràng, phạm vi cần thiết, căn cứ xử lý phù hợp và hợp đồng hoặc thỏa thuận bảo vệ dữ liệu. Luật BVDLCN quy định "bên xử lý dữ liệu chỉ tiếp nhận dữ liệu sau khi có hợp đồng hoặc thỏa thuận với bên kiểm soát dữ liệu và phải xử lý theo đúng thỏa thuận đó".

Trí tuệ nhân tạo làm khâu khai thác dữ liệu phức tạp hơn. Các công cụ AI có thể được dùng để chấm bài tự động, phát hiện đạo văn, phân tích nguy cơ bỏ học, gợi ý lộ trình học tập, hỗ trợ tư vấn, cá nhân hóa học liệu hoặc đánh giá năng lực. Nếu được thiết kế cẩn trọng, AI có thể hỗ trợ giáo viên và người học. Nhưng nếu thiếu minh bạch, AI có thể dẫn đến phân loại sai, thiên lệch, suy đoán quá mức hoặc xử lý dữ liệu vượt mục đích. Dữ liệu người học đưa vào công cụ AI bên ngoài có thể bị lưu lại, dùng để cải thiện mô hình hoặc chuyển ra ngoài lãnh thổ mà nhà trường không kiểm soát đầy đủ. Các nghiên cứu pháp lý về AI và quyền riêng tư nhấn mạnh rằng rủi ro không chỉ nằm ở dữ liệu đầu vào mà còn ở khả năng suy luận mới từ dữ liệu, khiến những thông tin không được người học trực tiếp cung cấp vẫn có thể bị dự đoán hoặc gán nhãn (Hartzog, W, & Richards, N. M, 2020).

Phân tích học tập cũng đặt ra câu hỏi về giới hạn giữa hỗ trợ và giám sát. Nếu nhà trường phân tích dữ liệu để phát hiện sinh viên có nguy cơ bỏ học và chủ động hỗ trợ, đó là mục tiêu giáo dục tích cực. Nhưng nếu cùng dữ liệu đó được dùng để xếp hạng, hạn chế cơ hội, giám sát quá mức hoặc gán nhãn năng lực cố định, quyền lợi người học có thể bị ảnh hưởng (Francis, 2023). Xu hướng "sinh viên bị giám sát" trong bối cảnh phần mềm giám sát học đường mở rộng từ khuôn viên trường sang thiết bị, hoạt động trực tuyến và đời sống ngoài giờ học; bà cảnh báo rằng giám sát liên tục có thể tác động đến quyền riêng tư, tự do biểu đạt và bình đẳng của người học (Citron, D. K, 2024).

Tuy nhiên, ba hạn chế nổi bật vẫn tồn tại. Một là thiếu quy định chuyên ngành về DLCN của người học. Pháp luật hiện nay có quy định chung về DLCN, trẻ em, giáo dục, an toàn thông tin và dạy học trực tuyến, nhưng chưa có văn bản chuyên biệt xác định danh mục dữ liệu giáo dục, mức độ nhạy cảm của từng loại dữ liệu, căn cứ xử lý, giới hạn chia sẻ, thời hạn lưu trữ, quyền tiếp cận - chỉnh sửa của người học, quy trình xử lý dữ liệu sinh trắc học, và yêu cầu đối với EdTech trong trường học. Hai là thiếu cơ chế kiểm soát dữ liệu xuyên suốt vòng đời. Không ít cơ sở giáo dục mới tập trung vào triển khai phần mềm mà chưa xây dựng bản đồ dữ liệu, đánh giá tác động, quy trình phân quyền, nhật ký truy cập, kiểm toán dữ liệu và phương án ứng phó sự cố. Ba là thiếu quy trình quản trị dữ liệu trong nhà trường. Giáo viên, cán bộ quản lý và người học thường sử dụng nhiều công cụ số trong hoạt động thường ngày, nhưng chưa được đào tạo đầy đủ về bảo vệ dữ liệu, dẫn đến rủi ro từ thói quen làm việc đơn giản như gửi file qua nhóm chat, đăng ảnh người học, chia sẻ màn hình có thông tin cá nhân hoặc dùng công cụ AI công cộng để xử lý bài làm của sinh viên.

2.3. Giải pháp nâng cao hiệu quả bảo vệ dữ liệu cá nhân của người học trong bối cảnh chuyển đổi số giáo dục

2.3.1. Hoàn thiện khung pháp lý về bảo vệ dữ liệu cá nhân trong lĩnh vực giáo dục

Giải pháp đầu tiên là hoàn thiện khung pháp lý chuyên ngành về DLCN của người học. Luật

BVDLCN đã tạo nền tảng chung, nhưng lĩnh vực giáo dục cần hướng dẫn cụ thể hơn vì dữ liệu người học có tính đặc thù về chủ thể, mục đích, bối cảnh xử lý và hệ quả xã hội. Cần xây dựng văn bản hướng dẫn hoặc bộ quy tắc chuyên ngành về bảo vệ dữ liệu người học trong giáo dục số, áp dụng cho cơ sở giáo dục phổ thông, giáo dục nghề nghiệp, giáo dục đại học, cơ sở giáo dục thường xuyên và nhà cung cấp công nghệ giáo dục có xử lý dữ liệu người học tại Việt Nam.

Nội dung đầu tiên của khung chuyên ngành là phân loại dữ liệu người học. Văn bản hướng dẫn nên xác định rõ dữ liệu định danh, dữ liệu học tập, dữ liệu hành chính, dữ liệu hành vi, dữ liệu sinh trắc học, dữ liệu sức khỏe, dữ liệu tâm lý, dữ liệu vị trí, dữ liệu kỷ luật, dữ liệu nghiên cứu và dữ liệu tạo ra bởi phân tích học tập hoặc AI. Mỗi nhóm dữ liệu cần có mức độ bảo vệ tương ứng. Dữ liệu sinh trắc học, sức khỏe, tâm lý, hoàn cảnh gia đình, kỷ luật và dữ liệu liên quan đến trẻ em phải được coi là nhóm rủi ro cao, chỉ xử lý khi thật cần thiết, có căn cứ rõ ràng, có đánh giá tác động và có biện pháp bảo vệ tăng cường.

2.3.2. Xây dựng cơ chế quản trị dữ liệu tại các cơ sở giáo dục

Pháp luật chỉ đặt khung, còn hiệu quả bảo vệ dữ liệu phụ thuộc nhiều vào tổ chức thực hiện trong nhà trường. Mỗi cơ sở giáo dục cần xây dựng chính sách bảo vệ dữ liệu người học như một bộ phận của quy chế quản trị giáo dục, không xem đây là phụ lục kỹ thuật của bộ phận công nghệ thông tin. Chính sách này phải được ban hành chính thức, phổ biến tới cán bộ, giảng viên, giáo viên, người học và đối tác liên quan.

Tiếp theo là phân quyền và kiểm soát truy cập. Dữ liệu người học phải được truy cập theo vai trò. Giáo viên chỉ cần dữ liệu của lớp mình phụ trách; cố vấn học tập chỉ cần dữ liệu phục vụ hỗ trợ; phòng tài chính chỉ cần dữ liệu liên quan đến học phí; phòng khảo thí chỉ cần dữ liệu thi; bộ phận truyền thông không được truy cập bảng điểm hoặc hồ sơ cá nhân nếu không có mục đích hợp pháp. Tài khoản quản trị phải có xác thực mạnh, không dùng chung, có nhật ký truy cập và định kỳ rà soát. Khi nhân sự chuyển vị trí hoặc nghỉ việc, quyền truy cập phải được thu hồi kịp thời. Đây là biện pháp tổ chức cơ bản nhưng có ý nghĩa lớn trong phòng ngừa rò rỉ dữ liệu nội bộ.

Bước thứ năm là quy trình xử lý sự cố dữ liệu. Mỗi cơ sở giáo dục cần có kịch bản khi xảy ra lộ lọt dữ liệu, truy cập trái phép, gửi nhầm thông tin, mất thiết bị, tài khoản bị chiếm đoạt hoặc nhà cung cấp gặp sự cố. Quy trình phải xác định người tiếp nhận thông tin, cách khoanh vùng, cách đánh giá mức độ ảnh hưởng, thời hạn thông báo nội bộ, nghĩa vụ thông báo cơ quan có thẩm quyền và chủ thể dữ liệu, biện pháp khắc phục, hỗ trợ người học và lưu hồ sơ sự cố.

2.3.3. Nâng cao nhận thức và năng lực bảo vệ dữ liệu của các chủ thể trong môi trường giáo dục

Giải pháp tiếp theo là nâng cao nhận thức và năng lực của các chủ thể trong môi trường giáo dục. Bảo vệ dữ liệu không thể thành công nếu chỉ có văn bản pháp luật và phần mềm bảo mật. Phần lớn sự cố dữ liệu bắt nguồn từ hành vi hằng ngày: mật khẩu yếu, gửi nhầm tệp, chia sẻ tài khoản, tải dữ liệu về thiết bị cá nhân, đăng ảnh không xin phép, sử dụng công cụ AI tùy tiện, lưu bảng điểm trong thư mục mở hoặc nhấp vào đường dẫn độc hại. Vì vậy, bảo vệ dữ liệu phải trở thành năng lực số cơ bản của nhà trường.

Đối với giáo viên, giảng viên và cán bộ quản lý, cần tập huấn các kỹ năng cụ thể: phân biệt dữ liệu thường và dữ liệu nhạy cảm; sử dụng email, LMS và kho lưu trữ an toàn; đặt mật khẩu và xác thực hai yếu tố; xử lý bảng điểm, bài làm, danh sách lớp; xin phép khi sử dụng hình ảnh người học; hạn chế chia sẻ dữ liệu qua mạng xã hội; nhận diện lừa đảo; sử dụng AI có trách nhiệm; và phản ứng khi phát hiện sự cố. Nội dung tập huấn không nên quá lý thuyết mà cần gắn với tình huống thường gặp trong nhà trường.

Đối với người học, cần giáo dục quyền và trách nhiệm dữ liệu. Người học cần biết mình có quyền được thông tin, quyền yêu cầu truy cập, chỉnh sửa, hạn chế hoặc phản ánh về việc xử lý dữ liệu theo quy định pháp luật; đồng thời có nghĩa vụ tôn trọng dữ liệu của người khác, không phát tán hình ảnh, bài làm, thông tin cá nhân của bạn học hoặc giáo viên. Giáo dục bảo vệ dữ liệu nên được lồng ghép vào kỹ năng số, giáo dục công dân, nhập môn đại học hoặc tuần sinh hoạt công dân.

Đối với phụ huynh, đặc biệt trong giáo dục phổ thông, cần nâng cao hiểu biết về dữ liệu trẻ em. Phụ huynh thường được yêu cầu ký nhiều biểu mẫu, cài nhiều ứng dụng, tham gia nhóm liên lạc và cung cấp thông tin cho nhà trường. Nhà trường cần cung cấp thông tin rõ ràng, tránh yêu cầu phụ huynh cung cấp dữ liệu thừa, không công khai thông tin riêng của học sinh trong nhóm lớp và có kênh để phụ huynh hỏi về quyền riêng tư của con.

III. KẾT LUẬN

Dữ liệu cá nhân của người học là nhóm dữ liệu có tính đặc thù trong môi trường giáo dục số, bao gồm không chỉ dữ liệu định danh mà còn cả dữ liệu học tập, dữ liệu hành vi và nhiều loại dữ liệu nhạy cảm khác. Do gắn liền với quá trình học tập, phát triển và cơ hội nghề nghiệp của mỗi cá nhân, nhóm dữ liệu này cần được bảo vệ ở mức độ cao hơn so với dữ liệu thông thường. Mặc dù Việt Nam đã từng bước hoàn thiện khung pháp lý về bảo vệ DLCN, đặc biệt với việc ban hành Luật BVDLCN, nhưng các quy định dành riêng cho lĩnh vực giáo dục vẫn còn những khoảng trống nhất định trước yêu cầu của chuyển đổi số. Thực tiễn cho thấy việc thu thập, lưu trữ và khai thác dữ liệu người học ngày càng mở rộng, đặt ra nhiều thách thức đối với quyền riêng tư và an toàn thông tin. Vì vậy, bảo vệ DLCN của người học cần được xem là một nội dung quan trọng của quản trị giáo dục hiện đại. Việc hoàn thiện pháp luật, tăng cường cơ chế quản trị dữ liệu trong nhà trường và nâng cao nhận thức của các chủ thể liên quan sẽ góp phần xây dựng môi trường giáo dục số an toàn, tin cậy và phát triển bền vững.

TÀI LIỆU THAM KHẢO

Quốc hội. (2015). Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015.

Bộ Giáo dục và Đào tạo. (2021). Thông tư số 09/2021/TT-BGDĐT ngày 30/3/2021 quy định về quản lý và tổ chức dạy học trực tuyến trong cơ sở giáo dục phổ thông và cơ sở giáo dục thường xuyên.

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council, General Data Protection Regulation.

Francis, M., Avoseh, M., Card, K., Newland, L., & Streff, K. (2023). Student privacy and learning analytics: Investigating the application of privacy within a student success information system in higher education. Journal of Learning Analytics, 10(3), 102-114.

Hartzog, W., & Richards, N. M. (2020). Privacy's constitutional moment and the limits of data protection. Boston College Law Review, 61, 1687–1761.

Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim towards a proposal. Research and Practice in Technology Enhanced Learning, 13(20), 1–14.