

XÂY DỰNG CHÍNH SÁCH BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA CÁC CƠ SỞ ĐÀO TẠO ĐẠI HỌC Ở VIỆT NAM ĐÁP ỨNG YÊU CẦU CỦA KỶ NGUYÊN SỐ

Nguyễn Phương Dung¹
Email: dungnp@hou.edu.vn

Ngày tòa soạn nhận được bài báo: 19/11/2025

Ngày phản biện đánh giá: 03/12/2025

Ngày bài báo được duyệt đăng: 15/12/2025

DOI: 10.59266/houjs.2025.1032

Tóm tắt: Động lực hình thành kỷ nguyên số là quá trình chuyển đổi số toàn cầu nhằm thay đổi tổng thể và toàn diện phương thức phát triển của xã hội, lối sống và hoạt động trên nền tảng số. Theo Liên hợp quốc, công nghệ số đã tiếp cận khoảng 50% dân số các nước đang phát triển chỉ trong hai thập kỷ và đang chuyển đổi xã hội (United Nations, n.d.). Với sự phát triển nhanh chóng của kỷ nguyên số, con người có thể tiếp cận, khai thác và tổng hợp thông tin dễ dàng, thuận tiện hơn. Do đó, các cơ sở đào tạo đại học đang đối diện với thách thức lớn về việc bảo vệ dữ liệu cá nhân của giảng viên và sinh viên. Bài viết tập trung phân tích khung pháp lý của việc bảo vệ dữ liệu cá nhân trong giáo dục đại học. Từ đó, bài viết đề xuất chính sách bảo vệ dữ liệu cá nhân phù hợp với các cơ sở đào tạo đại học ở Việt Nam hiện nay.

Từ khóa: bảo vệ dữ liệu cá nhân, chính sách bảo mật, giáo dục đại học, kỷ nguyên số, quyền riêng tư trong giáo dục

I. Giới thiệu

Trong kỷ nguyên số, dữ liệu cá nhân đã trở thành tài sản quý giá nhưng rất dễ bị xâm phạm. Ở Việt Nam, các cơ sở đào tạo đại học đang quản lý một số lượng lớn dữ liệu cá nhân của giảng viên và sinh viên như kết quả học tập; tình trạng sức khỏe, thông tin tài chính, an sinh xã hội, cư trú... Theo Bộ Giáo dục và Đào tạo, tính đến năm 2025, hơn 80% cơ sở giáo

dục đại học đã áp dụng hệ thống quản lý trực tuyến. Điều này dẫn đến tăng nguy cơ lộ lọt dữ liệu cá nhân do các trường hầu như chưa được trang bị hệ thống quản lý chuyên nghiệp để tránh tấn công mạng. Do đó, việc xây dựng chính sách về bảo vệ dữ liệu cá nhân của các cơ sở đào tạo đại học là cần thiết để bảo đảm khung pháp lý từ đó thiết lập quy trình bảo vệ hiệu quả đáp ứng yêu cầu của kỷ nguyên số.

¹ Trường Đại học Mở Hà Nội

II. Cơ sở lý luận

2.1. Quy định của một số quốc gia và Việt Nam về trách nhiệm bảo vệ dữ liệu cá nhân của các cơ sở giáo dục đại học

Với sự phát triển mạnh mẽ của công nghệ số và trí tuệ nhân tạo, yêu cầu bảo vệ dữ liệu cá nhân trở nên cấp thiết. Hơn 80 quốc gia trên thế giới đã ban hành đạo luật về bảo vệ dữ liệu cá nhân. Trong đó, vấn đề bảo vệ dữ liệu cá nhân trong các cơ sở giáo dục đang được nhiều quốc gia quan tâm.

Ở Hoa Kỳ, Đạo luật Quyền riêng tư và Quyền giáo dục gia đình (Family Educational Rights and Privacy Act - FERPA) được ban hành để bảo vệ quyền riêng tư về hồ sơ giáo dục của học sinh và sinh viên. Đối với sinh viên đủ 18 tuổi trở lên đang theo học tại các cơ sở giáo dục sau trung học có quyền truy cập hoặc đề nghị sửa đổi hồ sơ giáo dục của chính mình nếu có căn cứ cho rằng hồ sơ không chính xác, gây hiểu lầm, vi phạm quyền riêng tư của họ. Các trường đại học không được tiết lộ các thông tin trong hồ sơ giáo dục của sinh viên cho bên thứ ba nếu có không có sự đồng ý bằng văn bản của chính sinh viên đó. FERPA cho phép “cán bộ nhà trường”, bao gồm giảng viên và nhân viên hành chính truy cập hồ sơ giáo dục của sinh viên mà không cần có sự đồng ý của sinh viên nếu họ có “lợi ích giáo dục hợp pháp” để hoàn thành trách nhiệm nghề nghiệp. FERPA cũng cho phép các trường đại học tiết lộ thông tin từ hồ sơ giáo dục của sinh viên cho các nhà cung cấp phần mềm, ứng dụng; chuyên gia tư vấn (như chuyên gia tư vấn dinh dưỡng, tâm lý, luật sư hoặc nhà tư vấn công nghệ thông tin); tình nguyện viên (chẳng hạn như gia sư sinh viên) hoặc bên thứ ba khác mà nhà trường đã thuê nếu đáp ứng các điều kiện

sau: thực hiện dịch vụ hoặc chức năng của nhà trường; chịu sự kiểm soát trực tiếp của nhà trường trong việc sử dụng và truy cập hồ sơ giáo dục của sinh viên; được thực hiện với “lợi ích giáo dục hợp pháp” và phù hợp với các quy định trong thông báo hằng năm của trường.

Ở Châu Âu, Quy định về bảo vệ dữ liệu cá nhân (General Data Protection Regulation - GDPR) chính thức có hiệu lực vào 25/5/2018, đã cung cấp cơ sở pháp lý cho công dân các quốc gia thành viên EU quyền kiểm soát dữ liệu cá nhân. Các tổ chức, cá nhân trong đó có cơ sở giáo dục đại học cần phải tuân thủ một cách nghiêm ngặt các quy định về cách thức thu thập thông tin cá nhân; địa điểm lưu trữ dữ liệu; loại hình dữ liệu được chia sẻ; phải triển khai các biện pháp bảo mật kỹ thuật và tổ chức phù hợp như mã hóa. Trong trường hợp phát hiện có hành vi vi phạm, các cơ sở giáo dục đại học sẽ phải đối mặt với mức phạt rất cao, lên tới 20 triệu Euro hoặc 4% doanh thu toàn cầu hàng năm.

Ở Việt Nam, Luật Bảo vệ dữ liệu cá nhân năm 2025 sẽ có hiệu lực từ 01/01/2026 với nhiều nội dung khá phù hợp với quy định của GDPR. Luật quy định “bên kiểm soát dữ liệu cá nhân là cơ quan, tổ chức, cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân”. Chẳng hạn, khi một cá nhân nhập học tại trường đại học, cá nhân phải cung cấp thông tin và giấy tờ cần thiết. Như vậy, các cơ sở giáo dục đại học được coi là là “bên kiểm soát dữ liệu cá nhân” vì quyết định mục đích sử dụng dữ liệu (mở hồ sơ học tập, tài khoản học trực tuyến, giao dịch thanh toán học phí,...) và phương tiện quản lý (thu thập dữ liệu bằng điện tử và phi điện tử). Bên kiểm soát dữ liệu cá nhân có trách nhiệm theo quy định tại Khoản 1 Điều 37 của Luật. Nếu cơ sở

giáo dục trực tiếp xử lý dữ liệu cá nhân thì sẽ phải thực hiện các trách nhiệm ghi nhận tại Khoản 2 Điều 37. Luật cũng ghi nhận nguyên tắc việc thu thập dữ liệu cá nhân của các cơ sở giáo dục phải phù hợp và giới hạn trong phạm vi, mục đích cần xử lý. Với tư cách là chủ thể dữ liệu, sinh viên, học viên, nhân viên giáo dục có các quyền như quyền được biết, quyền đồng ý, quyền rút lại sự đồng ý, quyền truy cập, quyền xóa dữ liệu, quyền hạn chế xử lý dữ liệu, quyền phản đối xử lý dữ liệu,... Đặc biệt, các cơ sở giáo dục đại học với tư cách bên kiểm soát và xử lý dữ liệu phải xây dựng và duy trì hồ sơ đánh giá tác động liên quan đến bảo vệ dữ liệu cá nhân.

2.2. Sự cần thiết phải xây dựng chính sách bảo vệ dữ liệu cá nhân của các cơ sở giáo dục đại học ở Việt Nam

Việc xây dựng chính sách bảo vệ dữ liệu cá nhân của các cơ sở giáo dục đại học là rất cần thiết, đặc biệt trong giai đoạn phát triển nhanh chóng của kỷ nguyên số.

Thứ nhất, việc xây dựng chính sách giúp các trường đại học tạo lập khuôn khổ pháp lý trong việc xử lý dữ liệu cá nhân phù hợp với quy định của Nhà nước và yêu cầu của cơ quan quản lý. Trong năm gần đây, trước yêu cầu của kỷ nguyên số, các quy định về bảo vệ dữ liệu cá nhân liên tục được ban hành và sửa đổi, bổ sung. Ngày 17/4/2023, Chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Để tăng cường công tác bảo vệ dữ liệu cá nhân và an toàn thông tin mạng trong ngành giáo dục, Bộ Giáo dục và Đào tạo đã ban hành công văn 4567/BGDĐT-CNTT. Trong đó, yêu cầu các cơ sở giáo dục đại học phải “khẩn trương rà soát các quy định, quy chế nội bộ về quản lý, vận hành, khai thác, sử dụng các hệ thống thông tin, cơ sở dữ liệu thuộc phạm

vi quản lý của đơn vị và của các đơn vị trực thuộc để lồng ghép các quy định hiện hành của pháp luật về bảo vệ dữ liệu cá nhân, trong đó, cần quy định rõ về trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan; về xử lý trách nhiệm của tổ chức, cá nhân khi để xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân thuộc phạm vi phụ trách”. Luật Bảo vệ dữ liệu cá nhân đã được Quốc hội thông qua ngày 26/6/2025 và sẽ có hiệu lực thi hành từ 01/01/2026. Do đó, để kịp thời triển khai thực hiện các quy định mới, các trường đại học cần ban hành và sửa đổi, bổ sung các quy định có liên quan về bảo vệ dữ liệu cá nhân.

Thứ hai, việc xây dựng chính sách bảo vệ dữ liệu cá nhân của các trường đại học ở Việt Nam nhằm chủ động đương đầu với những thách thức trong kỷ nguyên số. Với sự phát triển nhanh chóng của công nghệ, các mối đe dọa về an toàn dữ liệu cá nhân mà các cơ sở giáo dục phải đối mặt gia tăng nhanh chóng. Các trường đại học có thể gặp phải các cuộc tấn công mạng hoặc các phần mềm chứa mã độc làm lộ, lọt thông tin cá nhân hoặc việc sử dụng trái phép dữ liệu cá nhân từ các bên cung ứng dịch vụ. Ở Mỹ, hàng loạt dữ liệu với đầy đủ thông tin đăng nhập cấp quản trị viên bị đánh cắp gần đây từ nhiều trường cao đẳng và đại học đã được công khai quảng cáo và rao bán trên các diễn đàn tội phạm mạng. Cục điều tra liên bang Mỹ (FBI) đã đưa cảnh báo rằng tội phạm mạng đang rao bán nhiều loại thông tin đăng nhập của các tổ chức giáo dục. Thậm chí, một số thông tin đăng nhập được bán trên các diễn đàn có thể truy cập công khai. Các cuộc tấn công có thể gây ra những tổn thất lớn đối với các trường đại học. Điển hình như vụ đột nhập vào máy tính của Trường Đại học California, San Francisco (UCSF)

chứa dữ liệu các thông tin cá nhân của hơn 600.000 người. Nhà trường đã trả 1,14 triệu USD để khôi phục dữ liệu bị đánh cắp liên quan tới các nghiên cứu học thuật quan trọng (Minh Hương, 2020). Như vậy, nguy cơ bị lộ, lọt dữ liệu cá nhân của các cơ sở giáo dục là rất cao.

Thứ ba, việc xây dựng chính sách bảo vệ dữ liệu cá nhân giúp các trường đại học có thể phân bổ nguồn lực hợp lý cho hoạt động bảo mật thông tin, đồng thời đảm bảo căn cứ pháp lý để triển khai hiệu quả các biện pháp tổ chức, kỹ thuật khi có hành vi xâm phạm dữ liệu cá nhân. Trong quá trình đào tạo, các cơ sở giáo dục thu thập rất nhiều dữ liệu cá nhân của người học và người lao động như thông tin cá nhân (họ tên, ngày sinh, giới tính, quốc tịch, số căn cước công dân, địa chỉ cư trú, số điện thoại, địa chỉ email, chữ ký,...); thông tin học tập (kết quả học tập, trình độ chuyên môn, văn bằng, chứng chỉ có liên quan, nhận xét, đánh giá của giảng viên,...); dữ liệu tài chính (số tài khoản, giao dịch học phí, thu nhập, bảo hiểm xã hội, mã số thuế,...); dữ liệu sinh trắc học (dấu vân tay, khuôn mặt để điểm danh); thông tin đời sống cá nhân (hoàn cảnh gia đình, tình trạng hôn nhân,...). Hầu hết trường đại học đều tích hợp công nghệ vào tất cả các khâu như triển khai các công cụ để quản lý sinh viên, quản lý lớp học; lên kế hoạch giảng dạy và phân bổ giảng viên; quy trình quản lý nhân sự, tài chính và hành chính nội bộ; quản lý và công bố sản phẩm nghiên cứu khoa học;... Do đó, khi có các quy định rõ ràng về bảo vệ dữ liệu cá nhân, các cơ sở giáo dục đại học sẽ có sự quan tâm đúng mức và phân bổ hiệu quả nguồn lực để triển khai các biện pháp kỹ thuật. Đây là các biện pháp phòng ngừa, ngăn chặn, xử lý từ sớm, từ xa đối với các hành vi xâm hại, bảo đảm

sự toàn vẹn, chính xác và bảo mật của dữ liệu cá nhân.

Thứ tư, việc xây dựng chính sách bảo vệ dữ liệu cá nhân góp phần nâng cao nhận thức của sinh viên, giảng viên, cán bộ quản lý và nhân viên ngành giáo dục về các mối đe dọa xâm phạm dữ liệu cá nhân; các biện pháp bảo đảm an toàn và minh bạch trong quản lý dữ liệu giáo dục. Hiện nay, một số trường đại học vẫn còn tình trạng công bố dữ liệu cá nhân của sinh viên, người lao động đang công tác tại đơn vị dưới dạng file word, excel,... trên trang thông tin điện tử hoặc các trang mạng xã hội như zalo, facebook,... hoặc niêm yết công khai (Đình Tuệ, 2024). Điều này khiến các đối tượng xấu dễ dàng tiếp cận những thông tin này nhằm mục đích rao bán để trục lợi hoặc lừa đảo. Việc ban hành chính sách bảo vệ dữ liệu cá nhân sẽ giúp nâng cao nhận thức, trách nhiệm của các chủ thể liên quan trong việc bảo đảm thông tin khỏi sự truy cập, sử dụng, tiết lộ trái phép.

Trong bối cảnh phát triển mạnh mẽ của kỷ nguyên số, việc xử lý và bảo vệ dữ liệu cá nhân đặt ra nhiều thách thức cho các cơ sở giáo dục. Do đó, việc xây dựng chính sách bảo vệ dữ liệu cá nhân trong các cơ sở giáo dục đại học là vấn đề cấp bách để bảo đảm môi trường học tập an toàn và hiệu quả.

III. Phương pháp nghiên cứu

3.1. Phương pháp phân tích - tổng hợp tài liệu

Được sử dụng để hệ thống hóa cơ sở lý luận, phân tích các quy định pháp luật về trách nhiệm bảo vệ dữ liệu cá nhân của các cơ sở đào tạo đại học. Đồng thời, bài viết cũng sử dụng phương pháp này để đánh giá thực trạng xây dựng chính sách

bảo vệ dữ liệu cá nhân tại các trường đại học ở Việt Nam hiện nay.

3.2. Phương pháp quy nạp và suy luận logic

Được sử dụng trong quá trình tổng hợp kết quả nghiên cứu và đưa ra các khuyến nghị đối với các cơ sở giáo dục đại học để xây dựng chính sách bảo dữ liệu cá nhân phù hợp với quy định pháp luật và thực tiễn triển khai tại Việt Nam.

3.3. Phương pháp phân tích trường hợp điển hình

Được sử dụng để phân tích chính sách bảo vệ dữ liệu cá nhân của Trường Đại học Vinuni (đơn vị tiên phong ban hành và công khai chính sách bảo vệ dữ liệu cá nhân) từ đó phân tích khả năng áp dụng cho các cơ sở giáo dục đại học khác tại Việt Nam.

IV. Kết quả và thảo luận

4.1. Thực trạng xây dựng chính sách bảo vệ dữ liệu cá nhân của các cơ sở giáo dục đại học ở Việt Nam

Ở Việt Nam, hiện nay chưa có số liệu thống kê chính thức các cơ sở giáo dục nói chung và cơ sở giáo dục đại học nói riêng đã có chính sách về bảo vệ dữ liệu cá nhân. Theo nghiên cứu của tác giả thì có rất ít cơ sở giáo dục đại học ban hành và công khai các quy định về bảo vệ dữ liệu cá nhân.

Điển hình nhất có Trường Đại học Vinuni đã xây dựng chính sách bảo vệ dữ liệu cá nhân và đăng công khai trên website của nhà trường (Công ty TNHH giáo dục và đào tạo Vinacademy & Trường Đại học Vinuni, 2020). Nghiên cứu chính sách bảo vệ dữ liệu cá nhân của Trường Đại học Vinuni có thể thấy một số điểm nổi bật như sau:

Thứ nhất, Chính sách Bảo vệ dữ liệu cá nhân này mô tả cách VinUni thu thập, sử dụng và xử lý dữ liệu cá nhân phát sinh trong quá trình hoạt động, kinh doanh của VinUni, khi người dùng cung cấp thông tin liên quan thông qua trang web, ứng dụng, sản phẩm, dịch vụ và các chương trình do VinUni quản lý theo quy định trong Chính sách. Tức là với tất cả chương trình, dự án của Trường Đại học Vinuni có liên quan đến dữ liệu cá nhân sẽ được xử lý theo quy định của Chính sách này.

Thứ hai, về cơ chế đồng ý được quy định cụ thể như sau: “Bằng việc chấp nhận Chính sách này, chủ thể dữ liệu cá nhân đã đồng ý để dữ liệu được xử lý bởi VinUni và đồng ý rằng VinUni, tổ chức, cá nhân tham gia quá trình xử lý dữ liệu không cần thực hiện thông báo lại trước khi xử lý”. Như vậy, việc chủ thể dữ liệu biết và chấp nhận chính sách sẽ đồng thời “đồng ý” cho Vinuni xử lý dữ liệu.

Thứ ba, các quy định được ghi nhận trong Chính sách Bảo vệ dữ liệu cá nhân của Trường Đại học Vinuni khá tương đồng với Nghị định 13/2023/NĐ-CP. Đồng thời, chính sách này cũng quy định khá cụ thể về mục đích xử lý dữ liệu cá nhân, cách thức xử lý dữ liệu cá nhân, cá nhân, tổ chức tham gia quá trình xử lý dữ liệu,... phù hợp với chức năng, nhiệm vụ và mô hình vận hành của nhà trường.

Đây là một trong những ví dụ điển hình về việc xây dựng chính sách bảo vệ dữ liệu cá nhân của các trường Đại học ở Việt Nam. Tuy nhiên, hiện nay các cơ sở giáo dục đại học, đặc biệt là các trường đại học đào tạo ngành luật trọng điểm quốc gia như Trường Đại học Luật Hà Nội, Trường Đại học Luật thành phố Hồ Chí Minh, Trường Đại học Luật - Đại học quốc gia Hà Nội,... cũng chưa ban

hành và công khai quy định về bảo vệ dữ liệu cá nhân. Điều này cho thấy mức độ không đồng đều trong việc ban hành quy định về bảo vệ dữ liệu cá nhân của các trường đại học.

4.2. Một số khuyến nghị trong xây dựng chính sách bảo vệ dữ liệu cá nhân của các cơ sở giáo dục đại học ở Việt Nam

Để bảo đảm các yêu cầu của Nghị định 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân năm 2025 (sẽ có hiệu lực từ 01/01/2026) các cơ sở giáo dục đại học cần xây dựng chính sách bảo vệ dữ liệu cá nhân, trong đó cần tập trung vào những vấn đề sau:

Thứ nhất, xây dựng khung quản trị dữ liệu tích hợp (Data Governance Framework). Khung quản trị dữ liệu tích hợp đòi hỏi cơ sở giáo dục đại học phải xây dựng quy trình và chính sách để quản lý tài sản dữ liệu mà đơn vị thu thập và xử lý từ nhiều nguồn khác nhau (như hệ thống quản lý sinh viên, đăng ký tín chỉ; hệ thống quản lý học tập; hệ thống quản lý tài chính, hệ thống quản lý nhân sự,...). Mục tiêu là bảo đảm dữ liệu thống nhất, đầy đủ, chính xác giúp trường đại học quản lý hiệu quả, đồng thời, giúp bảo mật dữ liệu an toàn cho chủ thể dữ liệu.

Thứ hai, thiết lập quy trình thu thập trong hoạt động quản lý của cơ sở giáo dục cần sự “đồng ý” của chủ thể dữ liệu. Theo quy định của Nghị định 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân năm 2025, cơ chế đồng ý là nền tảng pháp lý cho hầu hết các hoạt động xử lý dữ liệu trong môi trường số. Theo đó, sự đồng ý phải đáp ứng các tiêu chuẩn nghiêm ngặt: phải là tự nguyện, dựa trên sự hiểu biết rõ ràng của chủ thể dữ liệu về loại dữ liệu được xử lý, mục đích xử lý, các bên thứ ba được chia sẻ, và hậu quả của việc không đồng ý. Sự

đồng ý này phải được thể hiện bằng một hành động rõ ràng và cụ thể. Điều này đòi hỏi các cơ sở đào tạo giáo dục cần quy định chặt chẽ về quy trình thu thập thông tin bảo đảm sự “đồng ý” xử lý dữ liệu cá nhân của chủ thể dữ liệu.

Thứ ba, quy định về chia sẻ và chuyển giao dữ liệu cá nhân cho bên thứ ba. Trong môi trường giáo dục số, việc chia sẻ dữ liệu với bên thứ ba (như nhà cung cấp dịch vụ đám mây, hạ tầng đào tạo trực tuyến; đối tác marketing, đối tác liên kết đào tạo hoặc công ty cung ứng dịch vụ phần mềm quản lý học tập, phần mềm kế toán,...) là gần như không thể tránh khỏi. Việc chia sẻ dữ liệu cá nhân phải tuân thủ nghiêm ngặt các điều kiện pháp lý và cần được quy định rõ ràng trong chính sách của nhà trường. Trong đó, cần lưu ý điều kiện tiên quyết là phải có sự đồng ý rõ ràng của chủ thể dữ liệu cho việc chuyển giao đó, và việc chia sẻ phải phục vụ mục đích đã được thông báo trước. Để thiết lập chuỗi trách nhiệm rõ ràng, các trường đại học với tư cách là bên kiểm soát dữ liệu phải đảm bảo rằng hợp đồng xử lý dữ liệu (Data Processing Agreements - DPA) với bên thứ ba có đầy đủ các điều khoản bắt buộc theo quy định, bao gồm cam kết về bảo mật, giới hạn mục đích sử dụng, và cơ chế ứng phó sự cố.

Thứ tư, xây dựng quy định trách nhiệm giải trình và đánh giá tác động (Accountability & DPIA). Theo quy định tại Điều 21 Luật Bảo vệ dữ liệu cá nhân năm 2025, bên kiểm soát dữ liệu phải lập, lưu trữ hồ sơ đánh giá tác động xử lý dữ liệu cá nhân và gửi 01 bản chính cho cơ quan chuyên trách bảo vệ dữ liệu cá nhân trong thời gian 60 ngày kể từ ngày đầu tiên xử lý dữ liệu cá nhân, trừ trường hợp quy định tại khoản 6 Điều này. Như vậy,

hồ sơ đánh giá tác động bảo vệ dữ liệu (DPIA) trở thành quy trình hoạt động bắt buộc đối với mọi dịch vụ và dự án mới của cơ sở đào tạo. Việc lồng ghép DPIA vào giai đoạn thiết kế sản phẩm hoặc dịch vụ mới (Privacy by Design) là chiến lược tối ưu để đảm bảo tuân thủ ngay từ đầu, giảm thiểu chi phí sửa đổi pháp lý sau này. Do đó, trong chính sách về bảo vệ dữ liệu cá nhân, các trường đại học cần xác định việc thực hiện Hồ sơ đánh giá tác động bảo vệ dữ liệu (DPIA) là quy trình bắt buộc trước khi triển khai bất kỳ hoạt động, dự án nào liên quan đến dữ liệu cá nhân.

Thứ năm, khi xây dựng chính sách các cơ sở giáo dục đại học cần ưu tiên quy định về các biện pháp kiểm soát an ninh mạng, kiểm soát nội bộ để chống lại hành vi mua bán dữ liệu từ nhân viên và nguồn kinh phí để thực triển khai các biện pháp này.

Như vậy, việc ban hành chính sách bảo vệ dữ liệu giúp các cơ sở giáo dục đào tạo giúp đảm bảo tuân thủ bền vững, chuẩn bị cho Luật Bảo vệ dữ liệu cá nhân 2025 (chính thức có hiệu lực từ 01/01/2026), khi các quy định về xử lý dữ liệu, chế tài và trách nhiệm của nhà trường với tư cách bên kiểm soát dữ liệu chặt chẽ hơn.

V. Kết luận và kiến nghị

Bảo vệ dữ liệu cá nhân trong các cơ sở giáo dục đại học là vấn đề phức tạp, đòi hỏi sự phối hợp của nhiều các bên liên quan. Trong đó, việc xây dựng chính sách bảo vệ dữ liệu cá nhân được coi là giải pháp mang tính chủ động và cần được ưu tiên thực hiện để tạo lập môi trường giáo dục an toàn, minh bạch và phát triển bền vững trong kỷ nguyên số. Tuy nhiên hiện nay nhiều trường đại học chưa chú trọng vấn đề này. Bài viết chỉ ra sự cần thiết phải xây dựng chính sách bảo vệ dữ

liệu cá nhân của các cơ sở giáo dục đại học đồng thời đưa ra một số khuyến nghị để các cơ sở đào tạo xây dựng chính sách phù hợp với quy định của Luật Bảo vệ dữ liệu cá nhân năm 2025 (sẽ có hiệu lực từ 01/01/2026).

Lời cảm ơn: Nghiên cứu này được tài trợ bởi Đề tài khoa học cấp Trường Đại học Mở Hà Nội, mã số MHN 2025-02.57.

Tài liệu tham khảo

- [1]. Bộ Khoa học và công nghệ. (2022). Thông tin của nhiều trường đại học tại Mỹ được rao bán công khai. <https://mst.gov.vn/thong-tin-cua-nhieu-truong-hoc-tai-my-duoc-rao-ban-cong-khai-197154471.htm>.
- [2]. Công ty TNHH giáo dục và đào tạo Vinacademy, & Trường Đại học Vinuni. (2020). *Chính sách bảo vệ dữ liệu cá nhân*. https://vinuni.edu.vn/wp-content/uploads/2020/07/VinUni_Chinh-sach-bao-ve-Du-lieu-ca-nhan.pdf.
- [3]. Đình Tuệ. (2024). Văn hoá ứng xử trong trường học: Cần bảo mật dữ liệu cá nhân. *Giáo dục thời đại*. <https://giaoducthoidai.vn/van-hoa-ung-xu-trong-truong-hoc-can-bao-mat-du-lieu-ca-nhan-post684485.html>.
- [4]. Lê, T. P. (2024). Một số vấn đề bảo mật và an toàn thông tin trong nhà trường. *Tạp chí thiết bị Giáo dục*, 1(7), tr. 86. <https://sti.vista.gov.vn/publication/view/mot-so-van-de-bao-mat-va-an-toan-thong-tin-trong-nha-truong-ec5607f5b2d5f5936fc9ef659deee82f-416930.html>.
- [5]. Minh Hương. (2020, July 4). Đại học Mỹ trả 1,14 triệu USD để chuộc lại dữ liệu bị hacker đánh cắp. *Dân trí*. <https://dantri.com.vn/giao-duc/dai-hoc-my-tra-114-trieu-usd-de-chuoc-lai-du-lieu-bi-hacker-danh-cap-20200704232601558.htm>.

- [6]. Ngô, V. B. D. (2025). Nghị định 13 và Luật Bảo vệ quyền lợi người tiêu dùng năm 2023 - Phân tích sự giao thoa pháp lý và chiến lược quản trị rủi ro tuân thủ. Trong *Kỷ yếu Tọa đàm “Pháp luật về bảo vệ quyền lợi người tiêu dùng trong bối cảnh chuyển đổi số hiện nay”* (tr. 285). Khoa Luật, Trường Đại học Mở Hà Nội.
- [7]. Nghị viện Châu Âu. (2016). Quy định chung về bảo vệ dữ liệu cá nhân của Liên minh châu Âu (GDPR). <https://gdpr-info.eu/>.
- [8]. Quốc hội. (2025). Luật Bảo vệ dữ liệu cá nhân 2025 số 91/2025/QH15. <https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-du-lieu-ca-nhan-2025-so-91-2025-QH15-625628.aspx>.
- [9]. Văn phòng chính sách bảo mật sinh viên, Bộ Giáo dục Hoa Kỳ. (2025). *Hướng dẫn dành cho sinh viên đủ điều kiện Đạo luật Quyền riêng tư và Quyền giáo dục gia đình (FERPA)* <https://www.hardincoschools.com/wp-content/uploads/2025/04/FERPA-Student-Guide-Vietnamese.pdf>.
- [10]. United Nations. (n.d.). *The impact of digital technologies*. <https://www.un.org/en/un75/impact-digital-technologies>.
- [11]. Vietnamnet. (2025). Mỹ cảnh báo tin tặc đang nhắm vào các trường học. <https://Vietnamnet.vn/my-canhh-bao-tin-tac-dang-nham-vao-cac-truong-hoc-i361494.html>
- [12]. Vietnamnet. (2025). Trộm dữ liệu từ trường học, Sở KH&ĐT và EVN đem bán, thu lợi hàng trăm triệu đồng. <https://Vietnamnet.vn/trom-du-lieu-ca-nhan-tu-truong-hoc-so-kh-dt-va-evn-dem-ban-kiem-loi-2446727.html>.

DEVELOPING PERSONAL DATA PROTECTION POLICIES FOR HIGHER EDUCATION INSTITUTIONS IN VIETNAM IN RESPONSE TO THE REQUIREMENTS OF THE DIGITAL ERA

Nguyen Phuong Dung¹

Abstract: *The driving force behind the formation of the digital era is the global digital transformation process, aimed at comprehensively and thoroughly changing the societal development model, lifestyles, and activities on a digital platform. According to the United Nations, digital technology has reached approximately 50% of the population in developing countries in just two decades and is transforming society (United Nations, n.d.). With the rapid development of the digital era, people can access, exploit, and synthesize information more easily and conveniently. As a result, higher education institutions are facing significant challenges in protecting the personal data of lecturers and students. This article analyzes the legal framework for personal data protection in higher education. Based on that analysis, the article proposes personal data protection policies suitable for higher education institutions in Vietnam at present.*

Keywords: *personal data protection, privacy policy, higher education, digital era, privacy rights in education*

¹ Hanoi Open University