

GIÁO DỤC CÔNG DÂN SỐ CHO HỌC SINH TRUNG HỌC PHỔ THÔNG TẠI HÀ NỘI: THỰC TRẠNG VÀ CÁC GIẢI PHÁP PHÒNG NGỪA RỦI RO TRÊN KHÔNG GIAN MẠNG

Nguyễn Thuỳ Dung¹

Email: quocduynguyen57@gmail.com. ORCID: 0009-0007-4478-1581

Ngày tòa soạn nhận được bài báo: 06/07/2026

Ngày hoàn thành đánh giá: 05/10/2026

Ngày bài báo được duyệt đăng: 19/10/2026

DOI: 10.59266/houjs.2026.1505

Tóm tắt: Nghiên cứu này phân tích thực trạng giáo dục công dân số và khả năng phòng ngừa rủi ro mạng của học sinh trung học phổ thông trên địa bàn thành phố Hà Nội. Thông qua khảo sát thực địa 1.150 học sinh tại 06 trường trung học phổ thông kết hợp phương pháp thống kê mô tả và suy luận, bài viết đánh giá sự tương quan giữa năng lực nhận thức số, kỹ năng bảo mật dữ liệu và hành vi ứng phó với các hiểm họa trực tuyến như tin giả và bạo lực mạng. Kết quả chỉ ra một nghịch lý: dù tiếp cận công nghệ thường xuyên, học sinh vẫn thiếu hụt các kỹ năng bảo mật cốt lõi và có xu hướng giữ im lặng (72%) thay vì tìm kiếm sự hỗ trợ học đường khi gặp khủng hoảng số. Từ các phát hiện thực chứng, nghiên cứu đề xuất ba nhóm giải pháp gồm: đổi mới chương trình giáo dục công dân số theo hướng trải nghiệm thực tế; nâng cao năng lực sư phạm số và tư vấn tâm lý học đường cho giáo viên; xây dựng cơ chế phối hợp liên ngành chặt chẽ giữa nhà trường, gia đình và lực lượng chức năng. Những giải pháp này nhằm kiến tạo một môi trường số an toàn, lành mạnh, góp phần phát triển toàn diện cả về tri thức, bản lĩnh, đạo đức cho thế hệ trẻ trong kỷ nguyên chuyển đổi số.

Từ khóa: An toàn internet, công dân số, giải pháp phòng ngừa, học sinh trung học phổ thông, rủi ro không gian mạng

I. Đặt vấn đề

Tiến trình chuyển đổi số quốc gia tại Việt Nam theo Quyết định số 749/QĐ-TTg của Thủ tướng Chính phủ đã đặt giáo dục vào tâm thế tiên phong, đòi hỏi sự thích ứng toàn diện của các cấp học đối với hệ sinh thái số hóa. Tại thủ đô Hà Nội, sự phổ cập hạ tầng băng thông rộng, mạng viễn thông thế hệ mới và thiết bị di

động thông minh đã chuyển dịch không gian học tập, giao tiếp của học sinh trung học phổ thông (THPT) từ không gian lớp học truyền thống sang không gian mạng một cách sâu rộng (Nguyễn, 2021). Tuy nhiên, sự gia tăng bùng nổ về số lượng người dùng trẻ tuổi và thời lượng tiếp xúc công nghệ không đồng nhất với sự phát triển tương xứng của năng lực công dân

¹ Học viện Chính trị, Bộ Quốc phòng, Hà Nội, Việt Nam

số và tư duy phản biện. Học sinh THPT tại các đô thị lớn như Hà Nội hiện nay đang phải đối mặt với các dạng thức rủi ro trên không gian mạng ngày càng tinh vi và phức tạp: từ sự xâm phạm quyền riêng tư, bạo lực ngôn từ trên mạng xã hội đến các chiến dịch thông tin sai lệch, tin giả có chủ đích nhằm thao túng tâm lý (Livingstone và cộng sự, 2012). Mặc dù hệ thống giáo dục phổ thông đã tích hợp nội dung công nghệ thông tin và tin học, song các bài học về đạo đức số, luật pháp số và kỹ năng an toàn mạng vẫn mang tính chắp vá, chưa đủ sức tạo thành màng lọc nhận thức vững chắc cho người học. Việc nghiên cứu thấu đáo thực trạng giáo dục công dân số tại địa bàn trọng điểm như Hà Nội không chỉ mang ý nghĩa lý luận thiết thực mà còn là yêu cầu cấp bách để bảo vệ thể hệ trẻ trước các biến động tiêu cực của không gian mạng, đồng thời cung cấp căn cứ thực chứng cho việc hoạch định chính sách giáo dục địa phương. Bài viết tập trung đánh giá năng lực công dân số thực tế của học sinh, kiểm định các chiều kích tác động thông qua phương pháp thống kê suy luận, nhận diện các khoảng trống trong công tác giáo dục nhà trường và đề xuất hệ thống giải pháp phòng ngừa rủi ro mang tính khả thi cao.

II. Cơ sở lý thuyết

2.1. Khung năng lực công dân số

Công dân số là một khái niệm đa chiều, không chỉ giới hạn ở khả năng vận hành các thiết bị công nghệ thông tin hay phần mềm ứng dụng mà còn bao hàm các chuẩn mực đạo đức, hành vi pháp lý và trách nhiệm xã hội khi tham gia vào hệ sinh thái trực tuyến. Theo Mossberger và cộng sự (2008), công dân số là những cá nhân có khả năng sử dụng internet một

cách thường xuyên, an toàn và hiệu quả để tham gia tích cực vào các hoạt động kinh tế, xã hội và văn hóa. Định nghĩa này nhấn mạnh tầm quan trọng của tính chủ động, năng lực hòa nhập và trách nhiệm công dân trong môi trường số hóa toàn cầu.

Trong khung lý thuyết chuẩn mực của Ribble (2015), năng lực công dân số được cấu thành từ 09 yếu tố then chốt, phân tách thành ba trụ cột cốt lõi phục vụ các mục tiêu khác nhau của đời sống số. Trụ cột Tôn trọng bao gồm tiếp cận số, phép tắc số và luật pháp số, định hướng các chuẩn mực giao tiếp văn minh trên mạng. Trụ cột Giáo dục tập trung vào giao tiếp số, đọc viết số và thương mại số, trang bị kỹ năng khai thác giá trị tri thức và kinh tế từ công nghệ. Trụ cột Bảo vệ đóng vai trò là hệ thống phòng thủ nội tại, bao gồm quyền và trách nhiệm số, an toàn số (bảo mật dữ liệu) và sức khỏe số. Đối với học sinh THPT, nhóm năng lực Bảo vệ có ý nghĩa sống còn, giúp các em tự xác lập ranh giới an toàn, nhận diện các hành vi xâm phạm quyền riêng tư, phòng tránh lừa đảo và duy trì sự cân bằng tâm lý giữa đời sống thực và đời sống ảo.

Quan điểm này hoàn toàn đồng nhất với các tiếp cận đương đại của UNESCO (2018a, 2018b) về việc trang bị năng lực số cho thể hệ trẻ trong kỷ nguyên số hóa. Theo đó, năng lực số không dừng lại ở các thao tác kỹ thuật thuần túy mà phải đạt tới khả năng đánh giá phê phán thông tin, hiểu rõ các tác động pháp lý của hành vi trực tuyến. Trong giai đoạn lứa tuổi vị thành niên, khi học sinh đang định hình bản sắc cá nhân và mở rộng các mối quan hệ xã hội trên nền tảng số, khả năng tự điều chỉnh hành vi, kiểm soát cảm xúc và phân tích ý đồ đằng sau các thông điệp số

trở thành chỉ báo quan trọng nhất phản ánh sự trưởng thành về năng lực công dân số.

2.2. *Rủi ro trên không gian mạng đối với học sinh phổ thông*

Sự tương tác thường nhật của học sinh trên môi trường mạng luôn tiềm ẩn những rủi ro đa dạng, được hệ thống hóa một cách toàn diện qua mô hình 4C của Livingstone (2012). Cấu trúc này cho phép nhận diện bốn nhóm hiểm họa chính mà người học trẻ tuổi thường xuyên đối mặt:

Rủi ro về nội dung (Content risks): Liên quan đến việc học sinh tiếp xúc với các thông điệp bạo lực, nội dung đồi trụy, thông tin sai lệch hoặc các ấn phẩm truyền thông độc hại gây lệch lạc nhận thức và giá trị đạo đức.

Rủi ro về tiếp xúc (Contact risks): Nảy sinh khi học sinh kết nối, giao tiếp với những đối tượng xấu trên mạng có ý đồ thao túng, dụ dỗ, lừa đảo hoặc xâm hại tình dục trực tuyến.

Rủi ro về hành vi (Conduct risks): Đề cập đến việc học sinh chủ động hoặc vô tình tham gia vào các hành vi gây hại cho người khác như bạo lực mạng (cyberbullying), công kích cá nhân, phát tán hình ảnh nhạy cảm hoặc vi phạm bản quyền số.

Rủi ro về hợp đồng (Contract risks): Liên quan đến việc người học vô tình vi phạm các điều khoản sử dụng dịch vụ, bị khai thác trái phép dữ liệu cá nhân cho các mục đích thương mại phi pháp hoặc bị xâm phạm quyền riêng tư qua các ứng dụng di động độc hại.

Boyd (2014) chỉ ra rằng đặc trưng của không gian mạng xã hội hiện đại là sự xóa nhòa ranh giới giữa không gian công

cộng và không gian riêng tư, khiến học sinh vị thành niên trở thành đối tượng dễ bị tổn thương khi các dấu vết số cá nhân bị lạm dụng ngoài tầm kiểm soát. Tại Việt Nam, các nghiên cứu thực chứng của Trần Thành Nam (2020) về sức khỏe tâm thần trẻ em trên môi trường trực tuyến đã cung cấp những minh chứng sâu sắc về hệ quả nặng nề của các rủi ro này. Kết quả nghiên cứu khẳng định bạo lực mạng và sự cô lập trực tuyến có mối tương quan thuận mạnh mẽ với các hội chứng tâm lý tiêu cực như trầm cảm lâm sàng, rối loạn lo âu, suy giảm lòng tự trọng và hành vi tự hủy hoại ở lứa tuổi học đường. Điều này đòi hỏi giáo dục công dân số phải vượt qua ranh giới của việc truyền thụ kỹ thuật công nghệ, hướng tới mục tiêu cốt lõi là bảo vệ an toàn sức khỏe tâm sinh lý và định hình hệ giá trị nhân văn cho người học.

III. Phương pháp nghiên cứu

3.1. *Phạm vi và mô hình nghiên cứu*

Nghiên cứu áp dụng phương pháp tiếp cận hỗn hợp (kết hợp định lượng làm chủ đạo kết hợp định tính bổ trợ) nhằm khai thác triệt để bức tranh thực trạng và giải mã các chiều kích tác động phức tạp trong hành vi trực tuyến của học sinh phổ thông. Quá trình khảo sát thực địa được triển khai nghiêm túc từ ngày 15/09/2025 đến ngày 15/02/2026 trên địa bàn 06 trường trung học phổ thông đại diện cho các vùng kinh tế - xã hội khác nhau tại thủ đô Hà Nội. Việc lựa chọn mẫu được thực hiện theo phương pháp phân tầng có chọn lọc, bảo đảm sự cân đối tỷ lệ giữa các mô hình trường công lập nội thành (đại diện bởi các quận trung tâm như Phường Hoàn Kiếm, Phường Cầu Giấy với mật

độ tiếp cận hạ tầng số cao), trường công lập ngoại thành (đại diện bởi các Phường Trâu Quỳ, xã Đa Phúc với các đặc thù về khoảng cách tiếp cận truyền thông) và hệ thống trường ngoài công lập chất lượng cao. Tổng số phiếu khảo sát phát ra là 1.200 phiếu thông qua cả hai hình thức trực tiếp và biểu mẫu điện tử bảo mật; qua quá trình sàng lọc, loại bỏ các phiếu trả lời không đầy đủ hoặc chọn đồng nhất một đáp án, nhóm tác giả thu về 1.150 phiếu hợp lệ (đạt tỷ lệ sử dụng rất cao là 95,8%). Về cơ cấu mẫu thực tế, học sinh nam chiếm 48,2% và học sinh nữ chiếm 51,8%; xét theo cấp độ học tập, khối lớp 10 chiếm 34,5%, khối lớp 11 chiếm 38,2% và khối lớp 12 chiếm 27,3%. Sự phân bố mẫu đa dạng và quy mô lớn này tạo ra cơ sở dữ liệu thực chứng tin cậy, phản ánh khách quan đặc điểm tâm lý lứa tuổi và môi trường số của học sinh phổ thông đô thị lớn.

3.2. Công cụ đo lường và kiểm định độ tin cậy

Để bảo đảm tính chuẩn hóa quốc tế trong thu thập dữ liệu, bảng hỏi cấu trúc được xây dựng dựa trên sự kế thừa các thang đo chuẩn mực về năng lực số và rủi ro trực tuyến, sử dụng thang đo Likert 5 mức độ (biến thiên từ 1 - Hoàn toàn không đồng ý đến 5 - Hoàn toàn đồng ý). Công cụ đo lường tập trung lượng hóa 04 biến quan sát chủ đạo bao gồm: (1) Nhận thức pháp lý và an toàn mạng (đo lường mức độ thấu hiểu Luật An ninh mạng và các chuẩn mực ứng xử số); (2) Kỹ năng bảo mật dữ liệu cá nhân (đánh giá thao tác thiết lập mã khóa, xác thực hai lớp và bảo vệ quyền riêng tư);

(3) Tần suất tiếp xúc rủi ro mạng (khảo sát mức độ va chạm với tin giả, bạo lực mạng và lừa đảo trực tuyến); và (4) Mức độ chủ động ứng phó khi gặp sự cố (đo lường phản ứng hành vi và kênh tìm kiếm sự trợ giúp). Nhằm loại bỏ sai số hệ thống và bảo đảm tính nhất quán nội tại của công cụ, nghiên cứu đã tiến hành kiểm định độ tin cậy thông qua hệ số Cronbach's Alpha trên toàn bộ tập dữ liệu sơ cấp. Kết quả kiểm định cho thấy tất cả các câu phần đều đạt giá trị vượt trội so với ngưỡng tiêu chuẩn khắt khe của nghiên cứu định lượng (0,70): cụ thể, biến Nhận thức an toàn mạng đạt 0,842; Kỹ năng bảo mật đạt 0,865; Tần suất rủi ro đạt 0,818 và Khả năng ứng phó đạt 0,839. Các chỉ số này minh chứng hùng hồn rằng các thang đo sở hữu độ tin cậy vững chắc, sẵn sàng cung cấp cơ sở dữ liệu chuẩn xác cho các bước phân tích thống kê suy luận tiếp theo.

3.3. Phương pháp phân tích dữ liệu

Toàn bộ dữ liệu định lượng sau khi làm sạch, mã hóa và chuẩn hóa đã được nhập và xử lý chuyên sâu thông qua phần mềm thống kê chuyên dụng SPSS 26.0. Bên cạnh việc sử dụng các chỉ số thống kê mô tả cơ bản (như tần suất xuất hiện, tỷ lệ phần trăm phân bố, giá trị trung bình và độ lệch chuẩn) để phác họa bức tranh toàn cảnh về thực trạng năng lực số của học sinh, nghiên cứu triển khai hệ thống các phép kiểm định thống kê suy luận nâng cao nhằm kiểm chứng các giả thuyết khoa học. Cụ thể, nghiên cứu tiến hành: (1) Kiểm định T-test độc lập (Independent Samples T-test) nhằm so sánh chuẩn xác mức độ khác biệt có ý nghĩa thống kê về

năng lực công dân số và kỹ năng bảo mật giữa học sinh nam và học sinh nữ; (2) Phân tích phương sai một yếu tố (One-way ANOVA) để đánh giá sự biến thiên năng lực số giữa các khối lớp học (từ lớp 10 đến lớp 12) và giữa các loại hình trường học khác nhau; và (3) Phân tích hồi quy tuyến tính bội nhằm lượng hóa chi tiết mức độ tác động, chiều hướng ảnh hưởng của các nhân tố giáo dục từ phía nhà trường và gia đình lên năng lực phòng ngừa rủi ro không gian mạng của học sinh. Việc áp dụng đồng bộ quy trình phân tích định lượng đa tầng này giúp bài báo vượt qua giới hạn của các nghiên cứu mô tả thông thường, mang lại các bằng chứng thực chứng có độ tin cậy học thuật

Bảng 1. Thực trạng kỹ năng bảo mật dữ liệu và ứng xử số của học sinh THPT

Chỉ báo năng lực công dân số	Mức độ thấp (%)	Mức độ trung bình (%)	Mức độ cao (%)
Sử dụng mật khẩu mạnh và xác thực hai lớp (2FA)	62,5	24,1	13,4
Kỹ năng nhận diện tin giả và thông tin xuyên tạc	48,7	36,2	15,1
Hiểu biết về quyền riêng tư và bảo vệ dữ liệu cá nhân	55,8	32,5	11,7
Ứng xử văn minh và kiểm soát ngôn từ trên mạng xã hội	31,4	45,9	22,7

Nguồn: Kết quả khảo sát thực địa của nhóm tác giả (2025-2026)

Số liệu tại Bảng 1 phản ánh một nghịch lý rõ rệt: học sinh rất thành thạo các thao tác giải trí và kết nối công nghệ nhưng lại tỏ ra cực kỳ thụ động, thiếu hụt trầm trọng các kỹ năng phòng thủ số cơ bản. Có tới 62,5% học sinh vẫn duy trì thói quen sử dụng mật khẩu đơn giản, dễ đoán hoặc dùng chung một mật khẩu cho nhiều tài khoản mạng xã hội khác nhau, tạo ra kẽ hở lớn cho các nguy cơ tấn công chiếm đoạt tài khoản.

4.2. Kết quả kiểm định thống kê suy luận và phân tích các nhân tố tác động

Để làm rõ sự khác biệt về năng lực số theo giới tính, kiểm định T-test độc

cao phục vụ cho phần thảo luận và kiến nghị giải pháp.

IV. Kết quả nghiên cứu và thảo luận

4.1. Thực trạng năng lực công dân số và kỹ năng bảo mật của học sinh THPT tại Hà Nội

Kết quả khảo sát mô tả cho thấy 100% học sinh tham gia khảo sát đều tiếp cận internet hằng ngày thông qua thiết bị di động thông minh cá nhân với thời gian sử dụng trung bình đạt 5,2 giờ/ngày. Tuy nhiên, mức độ hiểu biết về hành lang pháp lý, cụ thể là Luật An ninh mạng năm 2018 của Việt Nam, còn ở mức rất thấp: chỉ có 15,2% học sinh tự tin nắm vững các quy định và hành vi bị nghiêm cấm trên không gian mạng.

lập đã được thực hiện. Kết quả kiểm định cho thấy không có sự khác biệt có ý nghĩa thống kê về thời gian sử dụng internet giữa nam sinh và nữ sinh ($p > 0,05$). Tuy nhiên, đối với chỉ số *Kỹ năng bảo mật dữ liệu cá nhân*, điểm trung bình của nam sinh ($M=2,84, SD=0,72$) cao hơn có ý nghĩa thống kê so với nữ sinh ($M=2,51, SD=0,68$ với $t(1148)=4,32, p<0,001$). Ngược lại, đối với chỉ số *Ứng xử văn minh và kiểm soát ngôn từ*, nữ sinh đạt điểm trung bình ($M=3,42, SD=0,65$) cao hơn đáng kể so với nam sinh ($M=3,12, SD=0,71$ với $t(1148)=-3,85, p<0,001$), phản ánh đặc điểm khác biệt về hành vi số giữa hai giới.

Kết quả phân tích hồi quy tuyến tính bội nhằm xác định các yếu tố tác động đến *Khả năng chủ động ứng phó rủi ro của học sinh* cho thấy mô hình hồi quy đạt độ thích hợp cao ($R^2=0,428, F=56,42, p<0,001$). Các hệ số phóng đại phương sai VIF đều dao động từ 1,21 đến 1,84 (thấp hơn ngưỡng 3,0), xác nhận không có hiện tượng đa cộng tuyến. Kết quả chỉ ra rằng *Mức độ truyền đạt kiến thức an toàn mạng từ nhà trường* ($\beta=0,342, p<0,001$) và *Sự đồng hành, đối thoại của phụ huynh về trải nghiệm số* ($\beta=0,295, p<0,001$) là hai nhân tố có tác động mạnh mẽ nhất đến năng lực tự vệ của học sinh, vượt trội hơn so với yếu tố thời gian sử dụng thiết bị.

4.3. Nhận diện các rủi ro mạng phổ biến và khoảng trống hỗ trợ học đường

Kết quả phân tích định lượng kết hợp dữ liệu phỏng vấn sâu đã xác nhận một cách đanh thép rằng rủi ro về nội dung và rủi ro về hành vi hiện đang là những hiểm họa phổ biến và nhức nhối nhất đối với học sinh trung học phổ thông tại thủ đô Hà Nội. Trong đó, mức độ tiếp xúc thường xuyên với các luồng thông tin sai lệch, tin giả chiếm tỷ lệ cao nhất với 45%, tiếp theo sát phía sau là tình trạng bạo lực trực tuyến dưới các hình thức lăng mạ, miệt thị ngoại hình, bôi nhọ danh dự và nhân phẩm trên các nền tảng mạng xã hội chiếm 38%. Đáng chú ý, hiện tượng cô lập và tẩy chay xã hội ngầm diễn ra trong các hội nhóm kín, nhóm chat riêng tư của học sinh đang dần trở thành một biến thể vô cùng nguy hiểm của bạo lực học đường truyền thống. Biến thể này gây ra những áp lực tâm lý vô cùng nặng nề, trực tiếp làm suy giảm nghiêm trọng lòng tự trọng và phong độ học tập, đặc biệt tập trung ở học sinh khối lớp 10 và lớp 11,

giai đoạn các em đang có sự chuyển biến mạnh mẽ về tâm sinh lý và định hình bản sắc cái tôi cá nhân.

Bên cạnh các nguy cơ ngoại sinh từ không gian mạng, một phát hiện thực tiễn vô cùng quan trọng và đáng báo động từ dữ liệu phỏng vấn sâu chính là sự tồn tại của một khoảng trống giao tiếp trầm trọng giữa học sinh và hệ thống hỗ trợ sư phạm của nhà trường. Khi không may phải đối mặt với các sự cố bị đe dọa, tổn thương bằng hình ảnh, quấy rối hoặc lừa đảo trực tuyến, có tới 72% học sinh tham gia khảo sát lựa chọn phương án tự mình giải quyết trong âm thầm hoặc giữ im lặng tuyệt đối trước người lớn. Trong khi đó, chỉ có vọn vẹn 8% học sinh chủ động tìm kiếm sự hỗ trợ, can thiệp chính thức từ giáo viên chủ nhiệm, bộ phận tư vấn tâm lý hay ban giám hiệu nhà trường. Dưới lăng kính nghiên cứu tâm lý học đường, Patchin và Hinduja (2012) đã lý giải hiện tượng này xuất phát từ tâm lý lo sợ bị nhà trường kỷ luật, lo sợ bị thu hồi thiết bị kết nối công nghệ, hoặc do sự e ngại, thiếu niềm tin từ phía học sinh khi cho rằng các thầy cô giáo thế hệ trước không đủ sự thấu cảm, am hiểu và kỹ năng công nghệ để giải quyết các vấn đề phức tạp phát sinh trong không gian ảo. Sự đứt gãy nghiêm trọng trong kênh kết nối này khiến cho các vụ việc bạo lực mạng và khủng hoảng tâm lý của học sinh thường chỉ bị phát hiện khi sự việc đã đi quá xa, để lại những tổn thương tinh thần sâu sắc. Thực trạng này đặt ra yêu cầu cấp thiết và sống còn đối với các cơ sở giáo dục phổ thông trong việc đổi mới căn bản quy trình tham vấn tâm lý học đường số, xây dựng các kênh tiếp nhận thông tin bảo mật và củng cố niềm tin vững chắc giữa thầy và trò.

V. Kết luận và kiến nghị

5.1. Kết luận

Nghiên cứu đã hoàn thành mục tiêu đề ra khi làm rõ bức tranh toàn cảnh về thực trạng năng lực công dân số cũng như hệ thống các rủi ro trên không gian mạng mà học sinh trung học phổ thông tại thủ đô Hà Nội đang phải trực tiếp đối mặt. Thông qua việc kết hợp chặt chẽ giữa phương pháp định lượng với quy mô mẫu lớn (1.150 học sinh) và phân tích định tính bổ trợ, bài viết đã cung cấp những bằng chứng thực chứng và thống kê suy luận vững chắc về chiều hướng tác động của các nhân tố giáo dục gia đình và nhà trường. Kết quả khảo sát thực tế đã chỉ ra một nghịch lý đáng báo động rằng: mặc dù học sinh thế hệ số sở hữu lợi thế vượt trội về thời lượng và khả năng tiếp cận hạ tầng công nghệ, các em vẫn thiếu hụt trầm trọng các kỹ năng nền tảng cốt lõi như bảo mật dữ liệu cá nhân, nhận diện thông tin sai lệch (tin giả) và phương pháp đối phó hiệu quả với các hành vi bạo lực trực tuyến. Bên cạnh đó, việc phát hiện ra sự đứt gãy nghiêm trọng trong kênh giao tiếp hỗ trợ học đường, khi phần lớn học sinh chọn cách im lặng hoặc tự giải quyết khi gặp khủng hoảng, là một hồi chuông cảnh tỉnh đối với công tác quản lý giáo dục phổ thông hiện nay. Những phát hiện này khẳng định rằng việc duy trì mô hình giáo dục hình thức, truyền thống không còn phù hợp. Do đó, đòi hỏi toàn bộ hệ thống giáo dục phải có một sự chuyển dịch mang tính chiến lược, toàn diện và thực chất trong công tác giáo dục công dân số, nhằm xây dựng một môi trường mạng an toàn, lành mạnh, giúp thế hệ trẻ phát triển toàn diện cả về tri thức, kỹ năng tự vệ lẫn bản lĩnh đạo đức trong kỷ nguyên số hóa.

5.2. Kiến nghị giải pháp

Một là, đổi mới chương trình giáo dục công dân số theo hướng trải nghiệm thực tế: Phương pháp truyền thụ lý thuyết truyền thống đã bộc lộ nhiều hạn chế, không còn theo kịp tốc độ biến đổi của không gian mạng. Do đó, nhà trường cần chuyển dịch triết lý giáo dục sang mô hình học tập trải nghiệm. Các nội dung về an toàn mạng, kỹ năng nhận diện công nghệ nguy trang Deepfake tinh vi, cùng phương pháp kiểm chứng thông tin đa chiều phải được lồng ghép sống động vào các giờ học chính khóa và hoạt động ngoại khóa. Việc tổ chức các phiên tòa giả định mô phỏng những vụ án có thật xoay quanh hành vi vi phạm Luật An ninh mạng năm 2018 sẽ giúp học sinh chuyển hóa các điều luật khô khan thành nhận thức pháp lý trực quan. Cách tiếp cận này không chỉ giúp học sinh trang bị áo giáp phòng vệ trước cám dỗ trực tuyến mà còn rèn luyện tư duy phản biện sắc bén trước các chiến dịch thông tin độc hại.

Hai là, nâng cao năng lực sư phạm số và tư vấn học đường cho đội ngũ giáo viên: Trong hệ sinh thái số hóa học đường, giáo viên đóng vai trò là điểm tựa tin cậy, song thực tế đội ngũ này đang thiếu hụt trầm trọng các kỹ năng nhận diện rủi ro ảo. Nhà trường cần chủ động tổ chức các khóa bồi dưỡng chuyên sâu nhằm trang bị cho giáo viên chủ nhiệm và cán bộ Đoàn Thanh niên năng lực thấu cảm tâm lý học đường số. Thầy cô cần được huấn luyện cách phát hiện sớm các biểu hiện khủng hoảng tâm lý, sự thay đổi hành vi đột ngột của học sinh do bị cô lập hay bạo lực mạng. Song song với đó, việc thiết lập các kênh tiếp nhận phản hồi bảo mật, ẩn danh và đáng tin cậy sẽ phá vỡ bức tường im lặng, giúp học sinh chủ động tìm kiếm sự trợ giúp từ nhà trường ngay khi gặp sự cố.

Ba là, xây dựng cơ chế phối hợp liên ngành giữa nhà trường, gia đình và cơ quan an ninh: Phòng ngừa rủi ro mạng là một bài toán mang tính hệ thống, vượt ngoài khả năng giải quyết đơn lẻ của một tổ chức. Các cơ sở giáo dục cần thiết lập quy trình phản ứng nhanh, phối hợp chặt chẽ với lực lượng công nghệ cao để xử lý kịp thời các vụ việc bạo lực mạng hoặc lừa đảo có tính chất nghiêm trọng. Ở bình diện gia đình, phụ huynh cần được định hướng chuyển đổi từ phương pháp cấm đoán cực đoan sang hình thức giám sát chủ động, đồng hành và chia sẻ trải nghiệm số cùng con cái. Sự kết nối nhịp nhàng, đồng bộ giữa các chủ thể này sẽ tạo ra một mạng lưới bảo vệ đa tầng, giúp học sinh vững vàng phát triển toàn diện trong môi trường số an toàn.

Lời cảm ơn: Nghiên cứu này được thực hiện với sự hỗ trợ chuyên môn và dữ liệu thực tế từ Ban Giám hiệu cùng tập thể giáo viên, học sinh các trường THPT trên địa bàn thành phố Hà Nội. Tác giả xin trân trọng cảm ơn sự đồng hành và đóng góp quý báu này.

Tài liệu tham khảo

- Boyd, D. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.
- Livingstone, S. (2012). Critical reflections on network learning. LSE Research Online.
- Livingstone, S., Mascheroni, G., Ólafsson, K., & Haddon, L. (2012). *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile*. London School of Economics and Political Science.
- Luật An ninh mạng. (2018). *Luật số 24/2018/QH14 được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam thông qua ngày 12 tháng 6 năm 2018*.
- Mossberger, K., Tolbert, C. J., & McNeal, R. S. (2008). *Digital citizenship: The internet, society, and participation*. MIT Press.
- Nguyễn, Q. T. (2021). *Chuyển đổi số trong giáo dục đại học: Lý luận và thực tiễn*. NXB Đại học Quốc gia Hà Nội.
- Patchin, J. W., & Hinduja, S. (2012). *Cyberbullying prevention and response: Ways to make a difference*. Routledge.
- Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.
- Trần, T. N. (2020). *Bạo lực mạng và sức khỏe tâm thần của học sinh Việt Nam*. NXB Giáo dục.
- UNESCO. (2018a). *A global framework of reference on digital literacy skills for Indicator 4.4.2*. UNESCO Institute for Statistics.
- UNESCO. (2018b). *Digital literacy equity outcomes: A global framework*. UNESCO Institute for Statistics.

DIGITAL CITIZENSHIP EDUCATION FOR HIGH SCHOOL STUDENTS IN HANOI: CURRENT STATUS AND PREVENTIVE SOLUTIONS AGAINST CYBER RISKS

Nguyen Thuy Dung¹

Abstract: *This study analyzes the current status of digital citizenship education and cyber risk prevention capabilities among high school students in Hanoi. Through a field survey of 1,150 students across six high schools combined with descriptive and inferential statistical methods, the paper evaluates the correlation between digital cognitive competence, data security skills, and behavioral responses to online hazards such as fake news and cyberbullying. The results reveal a paradoxical reality: despite frequent technology engagement, students severely lack core data security skills and tend to remain silent (72%) rather than seeking school support during digital crises. Based on these empirical findings, the study proposes three key groups of solutions: reforming digital citizenship education curricula toward practical experiential learning; enhancing digital pedagogical competence and school psychological counseling skills for teachers; and establishing a robust interdisciplinary coordination mechanism among schools, families, and authorities. These solutions aim to foster a safe and healthy digital environment, contributing to the comprehensive development of knowledge and ethical resilience for the younger generation in the digital transformation era.*

Keywords: *cyber risks, digital citizenship education, high school students, internet safety, preventative solutions*

¹ Political Academy, Ministry of National Defence, Hanoi, Vietnam