

NGUY CƠ MẤT AN TOÀN TRONG SỬ DỤNG MẠNG XÃ HỘI CỦA SINH VIÊN HÀ NỘI

Đặng Vân Trang^{1*}

¹*Khoa Kinh tế – Xã hội và Môi trường, Học viện Chính trị khu vực I*

**Email: dangvantrang317@gmail.com*

Ngày nhận bài: 09/09/2025

Ngày nhận bài sửa sau phản biện: 17/09/2025

Ngày chấp nhận đăng: 24/09/2025

TÓM TẮT

Bài viết phân tích nguy cơ mất an toàn trong sử dụng mạng xã hội của sinh viên Hà Nội – nhóm người dùng trẻ, năng động nhưng dễ tổn thương trên không gian số. Nghiên cứu dựa trên khảo sát 1.149 sinh viên tại ba trường đại học ở Hà Nội, kết hợp tổng quan các công trình liên quan nhằm nhận diện nguy cơ phổ biến và đánh giá mức độ rủi ro. Kết quả cho thấy, hơn 80% từng trải qua ít nhất một mối nguy khi sử dụng mạng xã hội, trung bình mỗi người đối diện khoảng 3, 4 tình huống nguy cơ, tập trung vào ba nhóm: bảo mật và quyền riêng tư, tiếp cận thông tin và quan hệ xã hội trực tuyến. Trong đó, xâm phạm dữ liệu cá nhân được đánh giá nghiêm trọng nhất, tiếp đến là tin giả, nội dung độc hại và các hành vi quấy rối, lừa đảo. Các nguy cơ này có mối liên hệ đan xen, làm gia tăng tác động tiêu cực tổng thể. Qua đó, bài viết cung cấp bằng chứng thực tiễn và gợi ý giải pháp góp phần xây dựng xã hội số an toàn, nhân văn và bền vững.

Từ khóa: *mạng xã hội, nguy cơ mất an toàn, sinh viên.*

RISKS TO ONLINE SAFETY IN SOCIAL MEDIA USE AMONG UNIVERSITY STUDENTS IN HANOI

ABSTRACT

This article examines the risks to online safety arising from social media use among university students in Hanoi – a group that is young, active, yet particularly vulnerable in the digital environment. The study is based on a survey of 1.149 students from three universities in Hanoi, combined with a review of relevant literature to identify common risks and assess their severity. The findings reveal that more than 80% of respondents had encountered at least one online safety threat, with each student facing an average of 3, 4 risky situations, concentrated in three main domains: data security and privacy, information access, and online social relations. Among these, violations of personal data and privacy were considered the most severe, followed by exposure to misinformation, harmful content, and incidents of harassment and fraudulent activities. These risks are interrelated, amplifying their overall negative impact. Accordingly, the paper provides empirical evidence and proposes solutions for promoting a safe, humane, and sustainable digital society.

Keywords: *social media, online safety risks, university students.*

1. ĐẶT VẤN ĐỀ

“Những thách thức đang ngày càng gia tăng trong quá trình hệ sinh thái kỹ thuật số phát triển mạnh mẽ hiện nay. Tội phạm mạng, tấn công mạng, quấy rối và bạo lực trên mạng đã và đang gây ra những mối đe dọa thường xuyên đối với các cá nhân, tổ chức và thậm chí cả tới nền hòa bình và sự phát triển ổn định của các quốc gia” (Liên Hợp Quốc Việt Nam, 2024) – là lời phát biểu của bà Gaelle Demolis, Chuyên gia Chương trình và Chính sách Quản trị, Hòa bình và An ninh, Văn phòng UN Women khu vực Châu Á – Thái Bình Dương tại Hội thảo về an ninh mạng năm 2024. Việt Nam cũng không nằm ngoài thách thức trên, khi an ninh, an toàn mạng nổi lên như một vấn đề cấp thiết.

Trước thực trạng đó, Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 đã xác định ba trụ cột chính phát triển Việt Nam trở thành quốc gia số: Chính phủ số, kinh tế số và xã hội số; trong đó việc xây dựng một “môi trường số an toàn, nhân văn, rộng khắp” đến năm 2030 được xem là điều kiện tiên quyết để nuôi dưỡng một xã hội số lành mạnh và bền vững (Thủ tướng Chính phủ, 2020). Điều này cho thấy an toàn mạng không chỉ là vấn đề công nghệ mà còn gắn liền với trách nhiệm công dân, đòi hỏi mỗi cá nhân phải có hiểu biết và ứng xử phù hợp trong không gian mạng.

Trong bức tranh chung ấy, các trang mạng xã hội (MXH) nổi lên là không gian hình thành và phát triển xã hội số vượt trội hiện nay, đồng hành cùng đồng đạo các bạn trẻ sinh viên (SV). Theo Hội Sinh viên Việt Nam, đại bộ phận SV đều tham gia MXH và coi đó là hoạt động thường nhật (Lưu Trinh, 2023). Đồng nghĩa, SV vừa là nhóm hưởng lợi, vừa là nhóm dễ tổn thương nhất trước những nguy cơ mất an toàn trên MXH từ vấn đề bảo mật, xâm phạm quyền riêng tư, tiếp cận thông tin cho đến việc tương tác giữa các mối quan hệ trực tuyến.

Nghiên cứu tập trung tìm hiểu SV trên địa bàn Hà Nội bởi đây là một trong những trung tâm kinh tế – xã hội lớn, thu hút đông đảo bạn trẻ từ nhiều vùng miền đến học tập và phát triển. Họ cũng sớm tham gia các hoạt động

nghề nghiệp, khởi nghiệp, góp phần gia tăng thị hiếu đối với các dịch vụ MXH. Những đặc điểm này giúp phản ánh rõ nét hơn các cơ hội và thách thức trong sử dụng MXH của nhóm SV trên.

Trên cơ sở các vấn đề đặt ra, bài viết hướng đến tìm hiểu và phân tích rõ đặc điểm sử dụng MXH của SV Hà Nội, các nguy cơ mất an toàn trong quá trình sử dụng và đánh giá mức độ rủi ro của các nguy cơ ấy, từ đó đề xuất một số định hướng giải pháp nâng cao nhận thức, trách nhiệm của SV cũng như tăng cường các biện pháp đảm bảo an toàn trên mạng.

2. PHƯƠNG PHÁP NGHIÊN CỨU

Tác giả sử dụng kết hợp các phương pháp nghiên cứu xã hội học định lượng và định tính. Với định lượng, tác giả sử dụng phương pháp Ankét với mẫu khảo sát $N = 1149$ SV thuộc ba trường đại học trên địa bàn Hà Nội, đại diện ba khối đào tạo: xã hội (Học viện Báo chí và Tuyên truyền), kinh tế (Trường Đại học Kinh tế Quốc dân) và kỹ thuật (Học viện Kỹ thuật Quân sự). Mẫu được chọn theo phương pháp chọn mẫu theo chùm, là tập hợp các chuyên ngành tại mỗi trường, từ đó chọn ngẫu nhiên đơn giản một số chùm vào đơn vị quan sát và thu thập dữ liệu qua ứng dụng Google Forms. Dữ liệu định lượng được xử lý bằng phần mềm SPSS 26.0 thông qua các thống kê mô tả và tương quan. Với định tính, tác giả vận dụng phương pháp phân tích tài liệu thông qua sưu tầm, tổng hợp và hệ thống hóa các công trình nghiên cứu, bài viết được đăng tải trên tạp chí, báo cáo khoa học cùng quan điểm của Đảng và Nhà nước liên quan, tạo cơ sở khoa học tường minh cho nghiên cứu thực tiễn về nguy cơ mất an toàn trên MXH. Dữ liệu định tính được phân loại theo nhóm chủ đề để làm rõ, đối chiếu và bổ sung cho kết quả nghiên cứu.

3. KẾT QUẢ VÀ THẢO LUẬN

3.1. Kết quả nghiên cứu

3.1.1. Đặc điểm sử dụng mạng xã hội của sinh viên Hà Nội

Theo kết quả khảo sát năm 2024 của tác giả, 100% SV Hà Nội trả lời có tham gia ít nhất một nền tảng MXH, trung bình mỗi bạn có mặt trên 2,7 nền tảng. Đáng chú ý, phần

lớn SV không chỉ dừng lại ở một kênh duy nhất mà tham gia đồng thời trên từ ba MXH trở lên (82,2%), cho thấy xu hướng đa nền tảng đã trở nên phổ biến. Nhiều ứng dụng góp mặt trong đời sống trực tuyến của họ đã góp phần mở rộng không gian số mà SV có thể tiếp cận.

Không chỉ tham gia nhiều nền tảng, SV còn dành một quỹ thời gian đáng kể trong ngày cho MXH, chủ yếu từ 3 đến 5 giờ. Mục đích sử dụng hầu hết vẫn gắn với nhu cầu cơ bản của lứa tuổi, gồm giữ liên lạc với bạn bè, người thân (79,9%), chat, gửi tin nhắn (77,8%), kết hợp với nhu cầu cập nhật thông tin xã hội (51,1%) và giải trí (50,1%),...

Về mạng lưới xã hội trực tuyến, các con số cũng cho thấy SV Hà Nội góp phần tạo dựng môi trường ảo phong phú, tạo điều kiện có thể tiếp cận đa dạng thông tin, tương tác thường xuyên. 55,9% SV có dưới 500 bạn bè trên các nền tảng, số còn lại sở hữu quy mô bạn bè từ 500 đến hơn 1.000, phản ánh sự kết nối khá rộng rãi. Bên cạnh đó, nhiều SV tham gia từ 10 đến 20 nhóm, fanpage, tạo cơ hội kết nối và tiếp xúc với nhiều dòng thông tin khác nhau, cả chính thống lẫn phi chính thống.

Từ những dữ liệu trên, MXH đã trở thành một phần quan trọng trong đời sống SV, vừa đáp ứng nhu cầu giao tiếp, giải trí, vừa là kênh tìm kiếm thông tin và thể hiện bản thân. Song song với đó, SV cũng dễ dàng trở thành mục tiêu của các nguy cơ mất an toàn, bởi các nguy cơ trực tuyến luôn song hành và là hệ quả tất yếu của sự phát triển công nghệ số ngày nay. Tuy vậy, cần nhấn mạnh rằng mọi rủi ro, nguy cơ mất an toàn không hoàn toàn dẫn đến tổn hại, trong nhiều trường hợp, chúng đóng vai trò như một “tín hiệu cảnh báo”, buộc người dùng phải tỉnh táo và trang bị cho mình những kỹ năng phòng ngừa cần thiết.

3.1.2. Các nguy cơ mất an toàn trong sử dụng mạng xã hội của sinh viên Hà Nội

Kết quả khảo sát cho thấy đa số SV Hà Nội đều từng trải qua ít nhất một tình huống là nguy cơ mất an toàn khi tham gia MXH. Trung bình, mỗi SV đối mặt với khoảng 3,37 nguy cơ, thậm chí có trường hợp phải đối mặt tới 12 nguy cơ (1,3%). Đáng chú ý, sự khác

biệt giới khá rõ rệt khi SV nữ thường gặp nhiều nguy cơ mất an toàn hơn, với 5 trên 12 tình huống được ghi nhận có ý nghĩa về mặt thống kê, bao gồm bị hack tài khoản, nhận thông tin sai lệch, bạo lực, nhạy cảm hay bị người lạ quấy rối. Trong khi nam SV chủ yếu đối diện với hai rủi ro đặc thù là mất tài khoản do lừa đảo, bị lôi kéo liên quan chất cấm. Ngoài ra, chỉ 16,4% cho biết chưa từng là “nạn nhân” của bất kì trường hợp nguy hại nào. Như vậy, nguy cơ mất an toàn trên không gian mạng đối với SV là thường trực.

Các nguy cơ mất an toàn trong quá trình sử dụng MXH được chia thành ba nhóm: (1) bảo mật và quyền riêng tư, (2) tiếp cận thông tin và (3) trong các mối quan hệ trực tuyến. Xét tổng thể, nguy cơ về tiếp cận thông tin được SV xác định dễ gặp phải nhất, trong khi đó, việc mất an toàn khi tương tác trong các mối quan hệ trên MXH ít xảy ra với SV Hà Nội hơn cả. Ngoài ra, một khó khăn lớn đối với họ là nhận diện các tình huống liên quan đến bảo mật và quyền riêng tư với hơn 8% tổng SV chưa chắc chắn về sự xuất hiện các vấn đề mất an toàn trên, tỉ lệ này tập trung nhiều ở nữ sinh, cho thấy ngoài việc đối mặt với nhiều nguy cơ hơn, nhóm SV nữ còn có xu hướng dẫn đo khi xác định tình huống, phản ánh sự hiện diện của các nguy cơ tiềm ẩn đang diễn ra âm thầm, nạn nhân khó nhận biết được tình trạng gặp phải nếu thiếu kỹ năng và công cụ kiểm tra.

Trước hết, nguy cơ mất an toàn về bảo mật và quyền riêng tư trên MXH được xem là một trong những mối đe dọa khá phổ biến với nhiều người dùng hiện nay. Kết quả khảo sát SV Hà Nội tại Bảng 1 minh chứng rõ: có tới 38,6% từng bị “hack” tài khoản hoặc nhận tin nhắn chứa vi-rút, 29,8% bị mất tài khoản do lừa đảo, 20,5% bị lấy cắp hình ảnh, thông tin cá nhân khi chưa cho phép và 12,4% đã bị sử dụng vào mục đích xấu. Thực tế này càng đáng lo ngại khi báo cáo của Hiệp hội An ninh mạng năm 2024 ghi nhận 66,24% người dùng tại Việt Nam từng bị lộ lọt dữ liệu cá nhân, trong đó 73,99% do cung cấp thông tin khi mua hàng trực tuyến, 62,13% khi chia sẻ trên MXH (Mai Phương & Quang Thuần, 2025). Những con số trên phản ánh mức độ hiện hữu

và rủi ro của nguy cơ về quyền riêng tư trong quá trình SV sử dụng MXH, đặc biệt nếu họ là những người dùng duy trì thói quen bảo mật kém hoặc thiết lập quyền riêng tư chưa

phù hợp, bởi theo đó còn có sự phát triển ngày càng tinh vi của công nghệ như trí tuệ nhân tạo, khiến cho việc xâm nhập và khai thác dữ liệu cá nhân trở nên dễ dàng hơn.

Bảng 1. Tỷ lệ SV có nguy cơ mất an toàn về bảo mật và quyền riêng tư trên MXH

Tình huống	1. Chưa từng (%)	2. Đã/Đang gặp phải (%)	3. Không rõ (%)
1. Bị mất tài khoản MXH do lừa đảo	64,0	29,8	6,3
2. Bị “hack” tài khoản, nhận tin nhắn có chứa vi-rút,...	55,5	38,6	5,8
3. Bị lấy cắp hình ảnh, thông tin cá nhân (không được cho phép)	67,1	20,5	12,4
4. Bị sử dụng hình ảnh, thông tin cá nhân vào mục đích xấu (mạo danh, lừa đảo, ghép mặt vào hình ảnh/video nhạy cảm, lan truyền tin không chính xác,...)	78,4	12,4	9,2
Tổng	66,3	25,3	8,4

(Nguồn: Kết quả khảo sát của tác giả, 2024)

Tiếp theo, kết quả phân tích Bảng 2 cho thấy nhóm nguy cơ mất an toàn khi SV tiếp cận thông tin trên MXH có mức phổ biến rất cao với khoảng 60% từng tiếp nhận các thông tin sai lệch, quan điểm sai trái thù địch và tiếp xúc với hình ảnh, video,... có nội dung khiêu dâm, bạo lực. Chỉ riêng giai đoạn dịch Covid-19, tin giả, xấu độc đã có cơ hội bùng phát mạnh mẽ trở thành vấn nạn toàn cầu. Tại nước ta, năm 2020 đã phát hiện khoảng 100 hội nhóm và 14.000 chuyên trang Facebook, cùng hơn 80 kênh YouTube chống phá phát tán thường xuyên trên 54.000 video sai sự thật, xử phạt hơn 1.000

đối tượng vi phạm, ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội nói chung (Nguyễn Ngọc Cương & Nguyễn Ngọc Quỳnh, 2021). Như vậy, việc phải đối mặt với tin giả, tin xấu độc và nội dung không lành mạnh trên MXH luôn là vấn đề nhức nhối, phản ánh môi trường thông tin trên mạng ảnh hưởng tiêu cực đến nhu cầu và hoạt động trực tuyến của người dùng. Bên cạnh đó, một bộ phận thừa nhận không rõ các tình huống có nguy cơ rủi ro trên, thiếu kỹ năng phân biệt tin thật – tin giả hoặc vô tình tiếp cận nội dung độc hại mà không nhận thức được mức độ nghiêm trọng.

Bảng 2. Tỷ lệ SV có nguy cơ mất an toàn khi tiếp cận thông tin trên MXH

Tình huống	1. Chưa từng (%)	2. Đã/Đang gặp phải (%)	3. Không rõ (%)
1. Bắt gặp/nhận các thông tin sai lệch, quan điểm sai trái, thù địch,...	34,1	60,7	5,1
2. Bắt gặp/nhận hình ảnh, video,... có nội dung khiêu dâm, bạo lực	37,7	56,7	5,6
Tổng	35,9	58,7	5,4

(Nguồn: Kết quả khảo sát của tác giả, 2024)

Cuối cùng, Bảng 3 tập trung vào các nguy cơ mất an toàn xuất phát từ các mối quan hệ xã hội trên MXH, tuy mức độ phổ biến thấp hơn hai nhóm trên nhưng vẫn đáng lo ngại.

Trung bình 19,4% SV đã trải nghiệm các tình huống tương tác nguy hiểm, nổi bật nhất là lừa đảo chiếm đoạt tiền và bị quấy rầy từ người lạ, đều ảnh hưởng đến gần 30% SV.

Ngoài ra, 24,8% từng nhận bình luận, tin nhắn ác ý; một số bị dụ dỗ tình cảm, tình dục, tham gia mua bán chất cấm hoặc bị cô lập khỏi nhóm. Dù tần suất thấp hơn, các rủi ro này lại trực tiếp đe dọa tài sản, danh dự và sức khỏe của SV. Thực tế toàn quốc cũng chỉ ra hậu quả nặng nề có thể định lượng được: năm 2024, cứ 220 người dùng thì có 1 người trở thành nạn nhân của lừa đảo trực tuyến với

tổng thiệt hại ước tính khoảng 18.900 tỉ đồng (Trần Bình, 2024); riêng năm 2023, con số thiệt hại đã đạt 8.000 – 10.000 tỉ đồng, tăng gấp rưỡi so với 2022 (Bùi Tuấn & Mai Hoa, 2024). Bên cạnh mức độ phổ biến, hiệu quả ứng phó với rủi ro từ các mối quan hệ trực tuyến vẫn còn hạn chế, khiến SV trở thành nhóm dễ bị lợi dụng trong nhiều tình huống đầy rủi ro.

Bảng 3. Tỷ lệ SV có nguy cơ mất an toàn trong các mối quan hệ trên MXH

Tình huống	1. Chưa từng (%)	2. Đã/Đang gặp phải (%)	3. Không rõ (%)
1. Bị dụ dỗ/lừa đảo/chiếm đoạt tiền qua MXH	66,3	29,4	4,3
2. Bị dụ dỗ, lừa đảo hẹn hò/tình dục qua MXH	82,2	14,3	3,5
3. Nhận các bình luận/tin nhắn ác ý, đe dọa, gây tổn thương hay miệt thị ngoại hình,...	69,3	24,8	5,9
4. Bị dụ dỗ, lừa đảo mua bán chất cấm, chất kích thích	87,7	9,1	3,2
5. Người lạ trên MXH tìm cách gặp mặt (nhắn tin quá đà, spam,...)	65,2	29,8	5,0
6. Bị cô lập/loại trừ trên các hội nhóm MXH	84,9	9,1	5,9
Tổng	76,0	19,4	4,6

(Nguồn: Kết quả khảo sát của tác giả, 2024)

Từ bức tranh về thực trạng diễn biến các nguy cơ mất an toàn trên MXH, các bạn SV đang phải đối mặt với nhiều mối nguy có thể gây rủi ro trong quá trình tham gia các trang mạng, đặc biệt là tình trạng rủi ro ẩn, các nguy cơ diễn ra âm thầm và khó nhận diện. Như vậy, bên cạnh những lợi ích đáng kể, sự phát triển vũ bão của MXH cũng kéo theo sự phổ biến của các nguy cơ, đặt ra yêu cầu cần đánh giá mức độ rủi ro tác động của từng nguy cơ để thấy được đâu là nhóm nguy cơ quan ngại nhất.

3.1.3. Đánh giá mức độ rủi ro các nguy cơ mất an toàn trên mạng xã hội của sinh viên Hà Nội

Đánh giá mức độ rủi ro là bước tiếp nối quan trọng nhằm lượng hóa mức độ nghiêm trọng của các nguy cơ mà SV Hà Nội phải đối diện trên MXH. Dưới đây là kết quả khảo sát đánh giá của SV về các mối nguy trên MXH, được trình bày theo thang điểm trung bình (ĐTB) tăng dần từ 1 đến 5, trong đó mức 1 là mức rủi ro thấp nhất và mức 5 là mức rủi ro cao nhất, đồng nghĩa điểm số

càng cao phản ánh mức độ rủi ro, tổn hại càng lớn, bên cạnh là mức độ phân tán của dữ liệu đánh giá mức độ rủi ro được biểu thị qua độ lệch chuẩn (SD).

Thứ nhất là nhóm nguy cơ mất an toàn về bảo mật và quyền riêng tư trên MXH (Bảng 4) được SV đánh giá là đáng lo ngại nhất, với ĐTB là 3,81 trên tổng 5 điểm – cao nhất trong ba nhóm nguy cơ được khảo sát. Đặc biệt, trường hợp bị sử dụng các thông tin cá nhân vào mục đích xấu được cho là rủi ro nghiêm trọng nhất, cho thấy SV lo lắng trước các nguy cơ bị đánh cắp danh tính, mạo danh hay xâm phạm đời tư qua mạng hơn cả. Tương tự, báo cáo của Tổ chức World Wide Web và Hội Nữ Hướng đạo Thế giới (2020) cho hay, mối quan tâm hàng đầu của giới trẻ khiến họ lo lắng nhất là việc người khác chia sẻ hình ảnh, video hoặc tin nhắn riêng tư mà không có sự đồng ý. Thực tế, các trường hợp xâm phạm trên có thể kéo theo hệ quả nặng nề như bị bôi nhọ danh dự, tổn tiền..., đặc biệt khi công nghệ trí tuệ nhân tạo “deepfake” phát triển

vượt trội, một phần là lí do dẫn đến sự dè chừng phần nhiều ở SV nữ.

Thứ hai là nhóm nguy cơ liên quan đến việc tiếp cận thông tin trên MXH có ĐTB đạt 3,69 trên tổng 5 điểm. Khi MXH trở thành nguồn tin tức chủ yếu của giới trẻ, các rủi ro về thông tin không chỉ mang tính phổ biến mà còn để lại hậu quả khó lường. Phân tích số liệu Bảng 5, SV đặc biệt lo ngại về việc bắt gặp hay tiếp nhận các thông tin sai lệch, quan điểm sai trái, thù địch,... với ĐTB lên tới 3,78 điểm. Vấn đề trên đã trở thành “bệnh dịch” ảnh hưởng lớn đến an toàn người dùng, thậm chí là an ninh quốc gia. Theo báo cáo Rủi ro Toàn cầu năm 2024 của Diễn đàn Kinh tế thế giới, thông tin sai lệch được dự đoán là rủi ro có mức độ nghiêm trọng cao nhất trong hai năm tới, bởi “các tác nhân trong và ngoài nước sẽ lợi dụng thông tin sai lệch để gia tăng sự chia rẽ trong chính trị và xã hội”. Bên cạnh tin sai lệch, SV đánh giá rủi ro từ việc tiếp xúc nội dung độc hại như khiêu dâm, bạo lực cũng ở mức cao, tương ứng 3,72 điểm. Việc hiển thị các nội dung trên gây tác động tiêu cực, sai lệch trong nhận thức, đạo đức và sau cùng là hành vi xã

hội của người dùng. Do đó, không khó hiểu khi họ xem đây là một nguy cơ lớn đối với bản thân trong quá trình sử dụng MXH.

Thứ ba là nguy cơ trong các mối quan hệ trực tuyến trên MXH (Bảng 6) được đánh giá tổng thể đạt 3,43 trên 5 điểm, mặc dù có số điểm thấp nhất trong đánh giá về mức độ tổn hại/nghiêm trọng xảy ra với bản thân SV nhưng vẫn thuộc nhóm điểm rủi ro khá cao. Một mặt, việc bị người dùng khác quấy rối tình dục trên mạng được xem là có mức độ rủi ro cao nhất, đạt 3,81 điểm như một lời cảnh tỉnh về vấn nạn quấy rối trực tuyến đang ngày càng nhức nhối. Mặt khác, các hoạt động như người lạ gửi lời mời kết bạn, người lạ nhắn tin được nhận xét ít tác động hơn cả, bởi có thể họ tin rằng bản thân kiểm soát được các mối quan hệ trên mạng hơn là kiểm soát luồng thông tin hay dữ liệu cá nhân. Quan điểm trên có sự tương đồng trong một khảo sát giới trẻ đô thị ở Hà Nội và Nam Định: có khoảng 1/3 cho rằng nhìn chung có thể tin tưởng mọi người trên MXH và cảm thấy không cần quá cẩn thận khi giao tiếp trực tuyến (Trịnh Hòa Bình & Lê Thế Linh, 2015).

Bảng 4. ĐTB đánh giá mức độ rủi ro các nguy cơ về bảo mật và quyền riêng tư trên MXH

Tình huống	ĐTB chung	Nam	Nữ	SD
1. Người dùng khác sử dụng hình ảnh, thông tin của bạn vào mục đích xấu (giả mạo, lừa đảo, ghép mặt vào hình ảnh/ video nhạy cảm,...)	3,90	3,73	4,08	1,28
2. Bị lấy cắp hình ảnh, thông tin cá nhân	3,88	3,69	4,08	1,28
3. Công khai hồ sơ cá nhân (tên thật, ngày sinh, địa chỉ nhà, số điện thoại,...)	3,65	3,44	3,87	1,27
Tổng	3,81	4,01	3,62	

(Nguồn: Kết quả khảo sát của tác giả, 2024)

Bảng 5. ĐTB đánh giá mức độ rủi ro các nguy cơ về tiếp cận thông tin trên MXH

Tình huống	ĐTB chung	Nam	Nữ	SD
1. Bắt gặp/nhận các thông tin sai lệch, quan điểm sai trái, thù địch,...	3,78	3,65	3,92	1,22
2. Xuất hiện/nhận hình ảnh, video,...nội dung khiêu dâm, bạo lực	3,72	3,53	3,91	1,23
3. Xuất hiện quá nhiều luồng thông tin khác nhau về một sự việc đang diễn ra	3,57	3,45	3,69	1,19
Tổng	3,69	3,54	3,84	

(Nguồn: Kết quả khảo sát của tác giả, 2024)

Bảng 6. ĐTB đánh giá mức độ rủi ro các nguy cơ trong các mối quan hệ trên MXH

Tình huống	ĐTB chung	Nam	Nữ	SD
1. Bị người dùng khác quấy rối tình dục	3,81	3,60	4,03	1,29
2. Người lạ đề nghị gặp mặt	3,70	3,49	3,91	1,23
3. Bị người dùng khác bắt nạt, đe dọa, gây tổn thương hay miệt thị ngoại hình,...	3,68	3,49	3,88	1,26
4. Mua bán, trao đổi hàng hóa trên MXH	3,20	3,09	3,31	1,13
5. Người lạ nhắn tin	3,14	3,03	3,26	1,10
6. Người lạ gửi lời mời kết bạn	3,03	2,94	3,12	1,12
Tổng	3,43	3,27	3,59	

(Nguồn: Kết quả khảo sát của tác giả, 2024)

Đáng chú ý, độ lệch chuẩn (SD) ở các tình huống nguy cơ đều lớn hơn 1 cho thấy mức độ phân tán lớn trong đánh giá rủi ro của SV. Điều này chỉ ra rằng, các nguy cơ mất an toàn trong sử dụng MXH tác động không đồng đều đến toàn thể SV tham gia khảo sát, một bộ phận nhận xét mức độ rủi ro rất nghiêm trọng, trong khi nhóm khác lại nhìn nhận rủi ro thấp hơn, từ đó, gợi mở các giải pháp can thiệp có trọng tâm vào nhóm dễ tổn thương, nhất là SV nữ với ĐTB đánh giá luôn cao hơn SV nam. Nhìn chung, SV bước đầu đã nhận diện được những nguy cơ hiện hữu, đặc biệt ở khía cạnh bảo mật thông tin và quyền riêng tư, nhưng vẫn còn khoảng cách giữa nhận thức và hành vi phòng ngừa. Đây chính là cơ sở quan trọng để tiếp tục làm rõ mối liên hệ giữa các nguy cơ và định hướng giải pháp, nhằm xây dựng một môi trường mạng an toàn và lành mạnh hơn.

3.2. Thảo luận

Nghiên cứu này được tiến hành trong bối cảnh các nguy cơ mất an toàn trên không gian mạng gia tăng mạnh, đặc biệt đối với giới trẻ, đã đặt SV – nhóm gắn bó mật thiết với MXH – vào vị thế dễ tổn thương. Bài viết góp phần cung cấp dữ liệu thực chứng, đồng thời lí giải nhận thức và cách đánh giá của SV về những nguy cơ hiện hữu trên MXH.

Khảo sát 1.149 SV Hà Nội cho thấy hơn 80% từng trải qua ít nhất một nguy cơ mất an toàn trên mạng, trung bình mỗi người đối diện khoảng 3,4 tình huống nguy cơ. Đáng chú ý, SV nữ thường báo cáo nhiều tình huống rủi ro hơn nam, tương đồng với nhiều nghiên cứu trong và ngoài nước. Theo báo cáo của tổ chức Vận động Phụ nữ Châu Âu (2017), phụ

nữ trên toàn cầu có nguy cơ bị quấy rối trực tuyến – một trong những nguy cơ mất an toàn được khảo sát – cao gấp 27 lần nam giới. Còn ở nước ta, khảo sát thanh niên toàn quốc ghi nhận nữ giới thường dễ gặp rủi ro hơn trong tiếp xúc tin giả, vi phạm bảo mật và nội dung quấy rối/bạo lực (Nguyễn Tuấn Anh, 2022). Điều này khẳng định rủi ro trực tuyến không còn là hiện tượng cá biệt mà là trải nghiệm phổ biến. Trên cơ sở kế thừa nghiên cứu trước, tác giả phân loại các nguy cơ thành ba nhóm chính, gồm bảo mật và quyền riêng tư, tiếp cận thông tin và quan hệ xã hội trực tuyến. Ba nhóm tuy được tách biệt nhưng có quan hệ chặt chẽ, bởi một sự cố có thể khởi phát từ một nhóm rồi lan sang nhóm khác, làm trầm trọng thêm tác động tổng thể của các nguy cơ.

Về mức độ phổ biến và tổn hại của từng nhóm nguy cơ, nguy cơ về bảo mật và quyền riêng tư được đánh giá rủi ro cao nhất, phản ánh mối lo hàng đầu về xâm phạm dữ liệu cá nhân và danh tính. Ngược lại, mối nguy khi tiếp cận thông tin tuy phổ biến rất cao nhưng SV đánh giá mức độ tổn hại thấp hơn, dù ý thức được nguy hại của tin giả, nội dung độc hại nhưng thường loại rủi ro này ít nhắm thẳng vào cá nhân nên họ đánh giá mức độ tổn hại cá nhân thấp hơn so với rủi ro xâm phạm trực tiếp mình. Nhóm rủi ro trong các mối quan hệ trực tuyến ít phổ biến và đánh giá thấp nhất nhưng mức độ tổn hại không thể coi nhẹ, phản ánh một số mối nguy hiểm gặp nhưng gây thiệt hại lớn cần đề phòng. Điểm nổi bật là kết quả ghi nhận khác biệt rõ ràng trong đánh giá mức độ rủi ro giữa SV nam và nữ, sự chênh lệch này bắt nguồn từ vai trò giới, kì vọng xã hội. Minh chứng cho điều này

là con số 2/3 trong hơn 3000 thanh thiếu niên tham gia dự án xuyên quốc gia về quấy rối tình dục trực tuyến của Ủy ban Châu Âu (2017) đã nhận định rằng, họ sẽ nghĩ xấu về một cô gái nếu bị đăng hình ảnh nhạy cảm lên mạng, cao hơn nhiều nếu nạn nhân là nam giới, điều này một phần nêu lên hiện thực áp lực xã hội của nữ giới.

Các nguy cơ về bảo mật và quyền riêng tư nổi lên như nhóm rủi ro trọng yếu cần được ưu tiên giải quyết trước hết, bởi nó vừa được đánh giá là nguy hiểm nhất, vừa có tính chất nền tảng. Một khi thông tin cá nhân bị lộ, nhiều hệ lụy dây chuyền sang khía cạnh khác có thể xảy ra. Song song, không thể xem nhẹ nhóm nguy cơ trong quá trình tiếp cận thông tin trên MXH vì mức độ phổ biến quá cao của tin giả, xấu độc và nội dung độc hại đang đe dọa đến chất lượng môi trường thông tin số. Nhóm rủi ro gây mất an toàn cho SV xảy ra trong các mối quan hệ trực tuyến tuy SV có phần chủ quan hơn, nhưng những trường hợp nghiêm trọng như bắt nạt, quấy rối, lừa đảo cần được nhận diện đầy đủ để không bị coi nhẹ. Như vậy, các nhóm nguy cơ có mối quan hệ tương hỗ do nội dung độc hại dễ kéo theo xâm phạm dữ liệu, còn các mối quan hệ trực tuyến có thể trở thành kênh trung gian cho lừa đảo và xâm hại, đòi hỏi chiến lược ứng phó tổng thể trong bối cảnh bùng nổ công nghệ số.

Từ những kết quả này, cần triển khai giải pháp đồng bộ ở ba cấp độ cá nhân, tổ chức và chính sách, đồng thời chú ý đến nhóm nguy cơ cao – SV nữ. Ở cấp độ cá nhân, SV cần chủ động nâng cao kỹ năng số để bảo vệ bản thân, có ý thức, trách nhiệm chủ động báo cáo các sự cố hay hành vi vi phạm tới nhà cung cấp dịch vụ hoặc cơ quan chức năng để giảm thiểu rủi ro lan rộng. Ở cấp tổ chức, nhà trường và đoàn thể đóng vai trò quan trọng trong việc giáo dục và hỗ trợ SV, cần đưa nội dung an toàn số vào đào tạo, tổ chức tập huấn, đồng thời thiết lập kênh hỗ trợ khi có sự cố nhằm trang bị kỹ năng cụ thể, xây dựng kênh tư vấn và hỗ trợ, phát động các chiến dịch tuyên truyền về văn hóa ứng xử thông minh, lành mạnh và có trách nhiệm công dân số trên MXH. Ở cấp chính sách, Nhà nước cần hoàn

thiện pháp luật bảo vệ dữ liệu, siết chặt trách nhiệm của các nền tảng MXH và triển khai chương trình giáo dục kỹ năng số thống nhất. Các sáng kiến như thực hành an toàn số dành cho nữ giới, khóa học về tự bảo vệ trên mạng và diễn đàn chia sẻ kinh nghiệm giữa các trường đại học sẽ góp phần nâng cao tính chủ động của SV trước các nguy cơ mới. Bởi sau cùng, sử dụng MXH an toàn là điều kiện cần thiết để SV trở thành những thành viên sáng giá trong xây dựng và phát triển một xã hội số “khỏe mạnh”.

Tựu chung lại, nghiên cứu này nhấn mạnh tính cần thiết của việc sử dụng MXH một cách an toàn đối với SV – những công dân số tiềm năng. Chỉ khi nhận diện rõ ràng các nguy cơ, chủ động trang bị kỹ năng phòng ngừa và có sự hỗ trợ từ nhà trường, chính sách, họ mới có thể phát huy vai trò tích cực trên không gian mạng mà vẫn bảo vệ được bản thân trước những thách thức của kỷ nguyên số. Điều này không chỉ có ý nghĩa đối với cá nhân SV mà còn đóng góp xây dựng một cộng đồng mạng lành mạnh, bền vững, đúng như mục tiêu hướng tới của Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 của Việt Nam. Với sự kết hợp hài hòa của cả cá nhân, tổ chức và Nhà nước, MXH sẽ thực sự trở thành “bạn đồng hành” hữu ích và an toàn cho thế hệ trẻ nói riêng và cộng đồng nói chung trong chặng đường phía trước.

4. KẾT LUẬN

Nghiên cứu khẳng định SV Hà Nội vừa là nhóm sử dụng MXH tích cực vừa là đối tượng thường xuyên đối diện nhiều nguy cơ mất an toàn. Ba nhóm nguy cơ chính gồm bảo mật và quyền riêng tư, tiếp cận thông tin và quan hệ xã hội trực tuyến không tồn tại tách biệt mà đan xen, tạo nên những tác động đa chiều, trong đó, xâm phạm đời tư và dữ liệu cá nhân nổi lên như mối lo ngại hàng đầu. Kết quả trên mang lại ý nghĩa thực tiễn khi có thể trở thành tài liệu tham khảo về chủ đề an toàn số, sử dụng MXH của sinh viên Hà Nội, đồng thời cung cấp bằng chứng gợi mở giải pháp nâng cao nhận thức, trách nhiệm cá nhân và tăng cường các biện pháp bảo đảm an toàn trên mạng. Tuy còn giới hạn

về phạm vi khảo sát và phương pháp, nghiên cứu đã chỉ ra hướng đi quan trọng tiếp theo như mở rộng đối tượng, triển khai nghiên cứu cắt dọc để theo dõi xu hướng biến đổi của các nguy cơ theo thời gian và đánh giá hiệu quả can thiệp. Qua đó, có thể xây dựng các giải pháp toàn diện hơn nhằm bảo vệ SV và góp phần kiến tạo một xã hội số an toàn, nhân văn và bền vững.

LỜI CẢM ƠN

Bài viết là một phần kết quả nghiên cứu luận văn của tác giả với chủ đề “Sử dụng mạng xã hội an toàn của sinh viên trên địa bàn Hà Nội hiện nay”, xuất bản năm 2024 tại Học viện Báo chí và Tuyên truyền, Hà Nội.

TÀI LIỆU THAM KHẢO

- Bùi Tuấn & Mai Hoa. (2024). *Người dân bị lừa qua mạng năm 2023 khoảng 10.000 tỉ đồng*. Truy cập ngày 06/9/2025, tại <https://mst.gov.vn/nguoi-dan-bi-lua-qua-mang-nam-2023-khoang-10000-ty-dong-197240627091654788.htm>
- European Commission. (2017). *Project de SHAME – Young people’s experiences of online sexual harassment*. Truy cập ngày 17/9/2025, tại https://www.childnet.com/wp-content/uploads/2021/11/Project_deSHAME_Dec_2017_Report.pdf
- European Women’s Lobby. (2017). *Her Net Her Rights – Resource Pack on ending online violence against women and girls in Europe*. Truy cập ngày 17/9/2025, tại https://womenlobby.org/wp-content/uploads/2018/01/hernetherights_resource_pack_2017_web_version.pdf
- Liên Hợp Quốc Việt Nam. (2024). *Phụ nữ, Hòa bình và An ninh mạng. Hội thảo “Nâng cao nhận thức, năng lực cho phụ nữ và trẻ em gái trong việc ứng phó với các thách thức trên không gian mạng”*, Ninh Bình, 2024.
- Lưu Trinh. (2023). *Hơn 85% sinh viên được khảo sát lên mạng xã hội hàng ngày với mục đích gì?*. Truy cập ngày 16/9/2025, tại <https://tienphong.vn/hon-85-sinh-vien-duoc-khao-sat-len-mang-xa-hoi-hang-ngay-voi-muc-dich-gi-post1574423.tpo>
- Mai Phương & Quang Thuần. (2025). *Thiệt hại lớn vì lộ dữ liệu, thông tin cá nhân*. Truy cập ngày 16/9/2025, tại <https://thanhnien.vn/thiet-hai-lon-vi-lo-du-lieu-thong-tin-ca-nhan-185250402225909595.htm>
- Nguyễn Ngọc Cương & Nguyễn Ngọc Quỳnh. (2021). *Phòng, chống tin giả trên không gian mạng và cách nhận diện*. Truy cập ngày 16/9/2025, tại <https://mst.gov.vn/phong-chong-tin-gia-tren-khong-gian-mang-va-cach-nhan-dien-197147407.htm>
- Nguyễn Tuấn Anh. (2022). Tiếp cận “tin giả” và những nguy cơ rủi ro khi sử dụng mạng xã hội ở thanh niên. *Kỷ yếu Hội thảo Khoa học “Năng lực chuyển đổi số cho thanh niên”*, Trường Đại học Ngân hàng TP.HCM, 2022 (221–229).
- Thủ tướng Chính phủ. (2020). *Quyết định 749/QĐ-TTg ngày 03/06/2020 của Thủ tướng Chính phủ về Phê duyệt “Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”*.
- Trần Bình. (2024). *Lừa đảo trực tuyến ở Việt Nam gây thiệt hại khoảng 18.900 tỉ đồng*. Truy cập ngày 16/9/2025, tại <https://www.sggp.org.vn/lua-dao-truc-tuyen-o-viet-nam-gay-thiet-hai-khoang-18900-ty-dong-post773272.html>
- Trịnh Hòa Bình & Lê Thế Linh. (2015). *Mạng xã hội trực tuyến của giới trẻ ở đô thị hiện nay*. *Tạp chí Xã hội học*, 1(129), 52–59.
- World Economic Forum. (2024). *The Global Risks Report 2024*. Truy cập ngày 05/9/2025, từ <https://www.weforum.org/publications/global-risks-report-2024/>
- World Wide Web Foundation and World Association of Girl Guides and Girl Scouts. (2020). *Survey – Young people’s experience of online harassment*. Truy cập ngày 05/9/2025, từ https://webfoundation.org/docs/2020/03/WF_WAGGGS-Survey-1-pager-1.pdf