

ĐƠN VỊ TỔ CHỨC



**TRUNG TÂM PHÁT TRIỂN
KHOA HỌC VÀ CÔNG NGHỆ TRẺ**

ĐƠN VỊ ĐỒNG HÀNH



**TRƯỜNG ĐẠI HỌC
AN NINH NHÂN DÂN**

ĐƠN VỊ HỖ TRỢ



**SỞ KHOA HỌC VÀ CÔNG NGHỆ
TP. HỒ CHÍ MINH**



**CLB CÁC NHÀ KHOA HỌC TRẺ
TP. HỒ CHÍ MINH**

HỘI THẢO KHOA HỌC

AN NINH SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ



KỶ YẾU
HỘI THẢO KHOA HỌC
AN NINH SINH VIÊN
TRONG THỜI KỲ
CHUYỂN ĐỔI SỐ

MỤC LỤC
HỘI THẢO KHOA HỌC
AN NINH SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

Tiểu ban 1: Những tác động của An ninh mạng đến sinh viên trong thời kỳ chuyển đổi số

1. AN NINH SINH VIÊN 4.0: THỜI CƠ VÀ THÁCH THỨC	6
<i>Lê Minh Diệu - Trường Đại học An ninh nhân dân</i>	
2. CÁC MỐI ĐE DỌA AN NINH MẠNG MÀ HỌC SINH, SINH VIÊN ĐANG PHẢI ĐỐI MẶT TRONG THỜI KỲ CHUYỂN ĐỔI SỐ.....	26
<i>Trần Thị Quỳnh Như - Trường Đại học Sư Phạm, Đại học Đà Nẵng</i>	
3. CHUYỂN ĐỔI SỐ TẠI TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN.....	43
<i>Trần Anh Thành - Trường Đại học An ninh nhân dân</i>	
4. KỸ NĂNG BẢO MẬT THÔNG TIN KHI SỬ DỤNG INTERNET CỦA SINH VIÊN CÁC TRƯỜNG CÔNG AN NHÂN DÂN PHÍA NAM.....	52
<i>ThS. Dương Văn Quế, Trần Minh Hải, Nguyễn Đình Lộc, Nguyễn Minh Tú - Trường Đại học An ninh nhân dân</i>	
5. NHẬN DIỆN CÁC MỐI ĐE DỌA AN NINH ĐỐI VỚI SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ.....	71
<i>ThS. Hoàng Đức Nghi - Trường Đại học An ninh nhân dân</i>	
6. NHẬN DIỆN TÁC ĐỘNG TIÊU CỰC CỦA NGƯỜI CÓ ẢNH HƯỞNG TRÊN KHÔNG GIAN MẠNG (KOLs) ĐỐI VỚI SINH VIÊN VIỆT NAM.....	84
<i>Tổng Quang Minh - Trường Đại học An ninh nhân dân</i>	
7. NHẬN THỨC CỦA SINH VIÊN CÁC TRƯỜNG CAO ĐẲNG, ĐẠI HỌC THÀNH PHỐ HỒ CHÍ MINH VỀ VẤN ĐỀ BẢO VỆ PHỤ NỮ VÀ TRẺ EM TRÊN KHÔNG GIAN MẠNG	91
<i>Lê Thị Huỳnh Như, Huỳnh Lê Phụng Nhi, Lê Ngọc Anh - Học viện Cán bộ TP. Hồ Chí Minh</i>	
8. NHẬN THỨC CỦA SINH VIÊN TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN VỀ VẤN ĐỀ AN NINH THÔNG TIN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ.....	107
<i>Nguyễn Phúc Văn, Nguyễn Thị Diễm My - Trường Đại học An ninh nhân dân</i>	
9. NHẬN THỨC VÀ THÁI ĐỘ CỦA SINH VIÊN CÁC TRƯỜNG ĐẠI HỌC CÔNG AN NHÂN DÂN PHÍA NAM VỀ BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG	121
<i>ThS. Dương Văn Quế - Trường Đại học An ninh nhân dân</i>	
<i>Bùi Thị Thanh Quyên - Trường Đại học An ninh nhân dân</i>	
10. NHẬN THỨC VỀ MỐI ĐE DỌA AN NINH MẠNG VÀ CÁCH BẢO VỆ THANH THIẾU NIÊN	138
<i>Nguyễn Thị Mỹ Hạnh - Đại học Kinh tế TP. Hồ Chí Minh</i>	
11. NHỮNG YẾU TỐ TÁC ĐỘNG ĐẾN QUYẾT ĐỊNH SỬ DỤNG VÍ ĐIỆN TỬ CỦA SINH VIÊN TRÊN ĐỊA BÀN TP. HỒ CHÍ MINH.....	153
<i>Trần Nguyễn Thành Công - Đại học Kinh tế TP. Hồ Chí Minh</i>	
12. NHỮNG YẾU TỐ TÁC ĐỘNG TIÊU CỰC ĐẾN AN NINH SINH VIÊN TRONG QUÁ TRÌNH CHUYỂN ĐỔI SỐ	169
<i>TS. Trần Ngọc Mai - Trường Đại học An ninh nhân dân</i>	
13. TÁC ĐỘNG TIÊU CỰC CỦA CHATGPT ĐẾN AN NINH THÔNG TIN CỦA SINH VIÊN TRƯỜNG ĐẠI HỌC KINH TẾ QUỐC DÂN.....	177
<i>Lê Thị Phương Linh, Lê Nguyễn Phương Chi - Trường Đại học Kinh tế Quốc dân</i>	
<i>Lê Ngọc Thái Hà, Nguyễn Huyền Nhi - Trường Đại học Ngoại ngữ, ĐHQG-HN</i>	
<i>Mai Khánh Linh - Học viện Tài chính</i>	

14. THÁI ĐỘ CỦA SINH VIÊN TẠI THÀNH PHỐ HỒ CHÍ MINH VỀ NHỮNG THÔNG TIN XẤU, ĐỘC TRÊN MẠNG XÃ HỘI VÀ VIỆC ĐỀ XUẤT XÂY DỰNG MÔ HÌNH CÂU LẠC BỘ “PHỦ XANH THÔNG TIN” TRONG CÁC TRƯỜNG ĐẠI HỌC TRÊN ĐỊA BÀN TP. HỒ CHÍ MINH.....	194

Nguyễn Thị Lâm, Trần Phạm Công Tuấn, Nguyễn Quốc Kiệt - Trường Đại học An ninh nhân dân

15. TỘI KHỦNG BỐ TRÊN KHÔNG GIAN MẠNG THỜI KỲ CÁCH MẠNG CÔNG NGHIỆP 4.0 - NGHIÊN CỨU SO SÁNH PHÁP LUẬT VIỆT NAM VÀ MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI.....	216

Nguyễn Văn Tùng, Nguyễn Thị Thùy Trang, Phạm Trung Dũng - Trường Đại học Luật Hà Nội

16. TRAO ĐỔI VỀ AN NINH SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ.....	231

Trung tá, ThS. Phạm Văn Tỵ - Trường Đại học An ninh nhân dân

17. ỨNG DỤNG NHẬN DẠNG KHUÔN MẶT TRONG QUẢN LÝ ĐIỂM DANH SINH VIÊN.....	237

Phạm Mai Mẫn Nhi - Trường Đại học Sư phạm Kỹ thuật TP. Hồ Chí Minh

Tiểu ban 2: Pháp luật và những giải pháp đảm bảo An ninh Sinh viên

18. BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ.....	248
<i>Trần Thị Minh An, Hà Quang Bách - Trường Đại học Luật Hà Nội</i>	
19. BẮT NẠT TRỰC TUYẾN TRONG SINH VIÊN – THỰC TRẠNG VÀ GIẢI PHÁP PHÒNG NGỪA.....	265
<i>Trần Linh Huân - Câu lạc bộ các Nhà khoa học trẻ TP. Hồ Chí Minh</i>	
<i>Lê Thị Châu Giang - Trường Đại học Luật TP. Hồ Chí Minh</i>	
20. CÁC GIẢI PHÁP GIẢM THIỂU TỆ NẠN XÃ HỘI TRONG SINH VIÊN.....	276
<i>Phạm Thị Khánh Ly - Trường Đại học Luật Hà Nội</i>	
21. CÔNG TÁC BẢO VỆ AN NINH TƯ TƯỞNG SINH VIÊN TRÊN KHÔNG GIAN MẠNG THỜI KỲ CHUYỂN ĐỔI SỐ TẠI TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN.....	294
<i>Trung tá, TS Nguyễn Trần Tuấn- Trường Đại học An ninh nhân dân</i>	
22. GIẢI PHÁP AN NINH MẠNG VÀ BẢO MẬT THÔNG TIN TẠI TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ.....	301
<i>Lê Cao Hoàng Thiên, Nguyễn Phạm Minh Hiếu, Bùi Quốc Huy, Đặng Bá Hưng - Trường Đại học An ninh nhân dân</i>	
23. GIẢI PHÁP GÓP PHẦN BẢO ĐẢM AN NINH CON NGƯỜI TRƯỚC VẤN ĐỀ LỘ LỘT DỮ LIỆU CÁ NHÂN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ	316
<i>Nguyễn Nhật Phi, Nguyễn Hoàng Trí, Nguyễn Thanh Tuấn - Trường Đại học An ninh nhân dân</i>	
24. HOÀN THIỆN PHÁP LUẬT VỀ BẢO VỆ THÔNG TIN CÁ NHÂN CỦA SINH VIÊN TRONG CÁC CƠ SỞ GIÁO DỤC TẠI VIỆT NAM HIỆN NAY	328
<i>Nguyễn Thái Bình, Đào Tấn Anh, Nguyễn Mai Thảo - Trường Đại học Luật TP. Hồ Chí Minh</i>	
25. MÔ HÌNH CỘNG TÁC PHÁT HIỆN TẤN CÔNG MẠNG VÀ SẴN TÌM MŨI ĐE DỌA DỰA TRÊN PHƯƠNG PHÁP HỌC LIÊN KẾT.....	340
<i>Trần Đức Lương, Huỳnh Thái Thi, Nguyễn Hữu Quyền, Vương Minh Tiến, Ngô Đức Hoàng Sơn - Trường Đại học Công nghệ Thông tin, ĐHQG-HCM</i>	
26. NÂNG CAO NĂNG LỰC CỦA SINH VIÊN TRONG VIỆC ỨNG PHÓ VỚI CÁC RỦI RO TỪ CÔNG NGHỆ DEEPPAKE.....	345
<i>Trần Lê Trọng Văn - Trường Đại học Kinh tế - Luật, ĐHQG-HCM</i>	
27. PHÁP LUẬT VỀ AN NINH SINH VIÊN TỪ GÓC ĐỘ GIỚI HẠN QUYỀN TỰ DO NGÔN LUẬN TRÊN KHÔNG GIAN MẠNG - KINH NGHIỆM QUỐC TẾ VÀ VẬN DỤNG CHO VIỆT NAM.....	360
<i>Bùi Lê Hiếu, Nguyễn Thu Hiền - Học viện Tòa án</i>	
28. PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA SINH VIÊN TẠI VIỆT NAM - ĐỐI CHIẾU VỚI PHÁP LUẬT CỦA LIÊN MINH CHÂU ÂU EU (GDPR)	375
<i>Nguyễn Tiến Đạt, Hà Thảo Trâm - Trường Đại học Sài Gòn</i>	
29. QUẢN LÝ ĐÀO TẠO TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ TẠI CÁC TRƯỜNG ĐẠI HỌC.....	388
<i>Nguyễn Thị Mỹ Hạnh - Đại học Kinh tế TP. Hồ Chí Minh</i>	
30. THỰC TRẠNG VÀ GIẢI PHÁP PHÁT TRIỂN KỸ NĂNG THẨM ĐỊNH THÔNG TIN TRÊN MẠNG XÃ HỘI CHO SINH VIÊN	409
<i>ThS. Trần Minh Tú - Trường Đại học Kinh Tế - Tài Chính TP. Hồ Chí Minh</i>	
<i>ThS. Trương Thanh Văn - Ngân hàng TMCP Ngoại Thương Việt Nam</i>	
31. NÂNG CAO NĂNG LỰC NHẬN DIỆN, CẢNH GIÁC TRƯỚC THÔNG TIN XẤU, ĐỘC TRÊN KHÔNG GIAN MẠNG CHO SINH VIÊN TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN	418
<i>Thiếu tá, ThS. Phạm Thị Thu - Trường Đại học An ninh nhân dân</i>	

**TIỂU BAN 1:
NHỮNG TÁC ĐỘNG CỦA
AN NINH MẠNG ĐẾN
SINH VIÊN TRONG THỜI KỲ
CHUYỂN ĐỔI SỐ**

AN NINH SINH VIÊN 4.0: THỜI CƠ VÀ THÁCH THỨC

SECURITY OF STUDENTS 4.0: CHALLENGES AND OPPORTUNITIES

Lê Minh Diệu

Trường Đại học An ninh nhân dân

Email: leminhdieuu@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Cách mạng công nghiệp 4.0, an ninh sinh viên, cơ hội, thách thức.	Sự phát triển như vũ bão của cuộc Cách mạng công nghiệp 4.0 và xu thế toàn cầu hóa đang diễn ra rộng khắp trên toàn thế giới. Cách mạng công nghiệp 4.0 mở ra vô vàn thời cơ và thách thức, đòi hỏi bản thân mỗi cá nhân trong xã hội chủ động, sáng tạo, không ngừng nâng cao năng lực bản thân, nắm bắt cơ hội để kiến tạo môi trường phát triển toàn diện. Bản chất đơn nhất của mỗi cuộc cách mạng là sự đòi hỏi tương ứng về trình độ của lực lượng lao động nhằm vận hành và sản sinh ra những tri thức mới, những hạ tầng cho phiên bản Cách mạng công nghiệp tiếp theo. Bên cạnh đó, những rủi ro về an ninh thông tin trên không gian mạng, sự xâm nhập của mã độc làm lộ lọt thông tin mật, thông tin cá nhân, xâm phạm nghiêm trọng đến quyền riêng tư người dùng và các tổ chức. Nhận thức được vị trí vai trò của sinh viên trong thời đại 4.0 - những người tương tác, tiếp cận thông tin qua nền tảng số, chịu ảnh hưởng trực tiếp của những tác động trên không gian mạng, do đó vấn đề về an ninh thông tin nhất là đối với sinh viên trong cuộc Cách mạng công nghiệp 4.0 trở nên quan trọng hơn bao giờ hết. Trong bài viết này tác giả sẽ trình bày về bối cảnh, thời cơ, thách thức, đồng thời đề xuất một số giải pháp bảo đảm an ninh thông tin sinh viên trong cuộc Cách mạng công nghiệp 4.0.
<i>Keywords:</i> Industrial Revolution 4.0, student's security, opportunities and challenges.	ABSTRACT The Industrial Revolution 4.0 opens up many opportunities and challenges, requiring individuals in society to be proactive, creative, constantly enhance their abilities, seize the opportunity to create a comprehensive development environment. The unique nature of each revolution is the corresponding qualification of the labour

force to operate and produce new knowledge, new infrastructure for the next version of the Industrial Revolution. Besides, information security risks in the cyberspace, the infiltration of malware exposes confidential information, personal information, serious infringement on the privacy of users and organizations. Being aware of the role of students in the 4.0 era - people who interact, access information through digital platforms, are directly influenced by the impact of cyberspace, so the issue of information security, especially for students during the 4.0 Industrial Revolution, is becoming more important than ever. In this article, the author will present the context, timing, challenges, and suggest some solutions to ensure student information security in the Industrial Revolution 4.0.

1. Giới thiệu

Cuộc Cách mạng công nghiệp lần thứ 4 hay Công nghiệp 4.0, là xu hướng hiện tại của tự động hóa và trao đổi dữ liệu toàn cầu với mã nguồn mở, nó cho phép các cá nhân tham gia tạo lập, chia sẻ, sao chép, chỉnh sửa các thông tin tự do theo nguyên tắc mà nền tảng đó cho phép. Nó bao gồm hệ thống các mạng vật lý, mạng Internet kết nối vạn vật và điện toán đám mây. "Cách mạng công nghiệp lần thứ tư" là một thuật ngữ được dùng để chỉ sự phát triển công nghệ quan trọng. Theo đó, khái niệm Công nghiệp 4.0 hay nhà máy thông minh lần đầu tiên được đưa ra ở Hội chợ công nghiệp Hannover tại Cộng hòa Liên bang Đức vào năm 2011, công nghiệp 4.0 hướng tới nhiệm vụ thông minh hóa quá trình sản xuất và quản lý trong ngành công nghiệp chế tạo. Sự ra đời của Công nghiệp 4.0 tại Đức đã thúc đẩy các nước tiên tiến khác như Mỹ, Nhật, Trung Quốc, Ấn Độ phát triển các chương trình tương tự nhằm duy trì lợi thế cạnh tranh của mình. Cuộc Cách mạng số này đã mở cửa cho nhiều cơ hội, đồng thời cũng đặt ra vô vàn thách thức đối với mỗi quốc gia, tổ chức và cá nhân, nó đã và đang tác động ngày càng mạnh mẽ đến tất cả các lĩnh vực đời sống kinh tế, xã hội đất nước. Toàn thế giới bước vào kỷ nguyên số, mọi mặt đời sống xã hội của con người gắn liền với ứng dụng công nghệ và dữ liệu số hoá, các tương tác trực tuyến trên không gian mạng đi sâu vào cuộc sống thường nhật của con người, dần trở thành một phần lưu trữ, môi trường tiếp nhận thông tin, dữ liệu cực kỳ quan trọng. Thế hệ trẻ, những người được sinh ra và trưởng thành trong môi trường có sự bao bọc bởi công nghệ số, là những sinh viên mang trên vai mình những trọng trách tương lai xây dựng và phát triển đất nước. Những trải nghiệm, thói quen và hành vi liên quan đến công nghệ và không gian số, đặc biệt là

mạng xã hội đang ngày một thắt chặt mối quan hệ giữa bản thân người dùng và “hệ sinh thái” đa dạng đó.

An ninh thông tin trên không gian mạng được xem xét, đánh giá qua lăng kính của một vấn đề kỹ thuật, nguyên tắc vận hành với yêu cầu cần được xử lý trong không gian công nghệ nhằm bảo đảm an toàn dữ liệu và đề xuất phương hướng quản trị rủi ro một cách hiệu quả. Mối quan hệ giao tiếp giữa các nền tảng thông minh, sự “cộng sinh” giữa trí tuệ sáng tạo con người và sản phẩm trí tuệ nhân tạo trên phạm vi rộng lớn có tính phổ quát, từ đó ảnh hưởng đến mọi mặt đặc biệt là vấn đề về an ninh thông tin trên không gian mạng mà đối tượng chịu tác động trực tiếp, ảnh hưởng nhiều và sâu sắc nhất chính là đại bộ phận học sinh, sinh viên đang ngồi trên ghế nhà trường - một lứa tuổi đủ đẹp để tiếp thu mọi tinh hoa nhân loại, nhưng cũng đủ non nớt để các đối tượng xấu lợi dụng đầu độc thông tin. Vậy vấn đề đặt ra là làm thế nào để sinh viên có thể tự nhận thức, tự nắm bắt cơ hội nhằm trui rèn, mài dũa năng lực chủ động, sáng tạo trong học tập, góp nhặt kiến thức thông qua các nguồn dữ liệu phong phú, đa dạng trên không gian mạng phục vụ nhu cầu xây dựng nền tảng kiến thức cơ sở vững chắc, từ đó tiến vững vào tương lai hoà nhập với thời đại của công nghệ số hoá. Bên cạnh đó, bản thân mỗi sinh viên cũng cần nhìn nhận lại mối quan hệ, sự liên kết và độ tin cậy giữa các nguồn thông tin, biết so sánh, đối chiếu chọn lọc và phản biện các dữ liệu chưa chính xác, bảo vệ quan điểm ý kiến đúng đắn trước những luận điệu sai trái thù địch mà các đối tượng vẫn luôn lợi dụng không gian mạng nhằm đầu độc thông tin người dùng. Đồng thời, học cách bảo mật các dữ liệu thông tin cá nhân quan trọng, tránh sự xâm nhập phát tán dữ liệu cá nhân, làm mất an toàn cho bản thân trên không gian mạng!

Liên hệ đến bản thân sinh viên trường Đại học An ninh nhân dân, căn cứ vào đặc thù đào tạo và mục tiêu nhà trường đề ra nhằm đảm bảo các yêu cầu về mục tiêu giáo dục của Luật giáo dục về đào tạo nguồn nhân lực cho sự nghiệp xây dựng và bảo vệ Tổ quốc. Theo đó, mỗi sinh viên cần đáp ứng các yêu cầu về phẩm chất, giá trị nhân cách, giá trị sức lao động, năng lực nghề nghiệp, mục tiêu đào tạo của từng chuyên ngành cụ thể. Muốn đạt được những mục tiêu đó, bản thân sinh viên phải không ngừng cải thiện nâng cao năng lực mỗi ngày, đồng thời tăng cường các hoạt động cá nhân trong tự học, đặc biệt là tìm kiếm cơ hội để tiếp thu, học hỏi những kiến thức được cập nhật hàng giây, hàng phút trên không gian mạng. Không dừng lại ở đó, mỗi sinh viên An ninh cần ý thức rõ về mức độ bảo mật và an toàn thông tin của các dữ liệu trong và ngoài ngành, để từ đó tìm kiếm những giải pháp nhằm nâng cao hiệu quả bảo mật, phòng ngừa rủi ro về an toàn thông tin.

2. Cơ sở lý thuyết

An ninh thông tin trên không gian mạng là một bộ phận không thể tách rời của an ninh mạng nó bao gồm các lĩnh vực về an toàn thông tin, bảo mật cơ sở dữ liệu, quản

trị không gian mạng, an ninh mạng và bảo mật hệ thống, mã hoá giải mã, lỗ hổng và khai thác lỗ hổng website, mã độc, vi-rút,... Dựa trên cơ sở lý thuyết về An ninh mạng và An toàn thông tin, tác giả đào sâu phân tích, tổng hợp dữ liệu nhằm đưa ra luận điểm khách quan về những thời cơ và thách thức mà sinh viên phải đối mặt về an ninh thông tin trong cuộc cách mạng số, đồng thời đề xuất một số giải pháp nhằm nâng cao hiệu quả tiếp nhận và xử lý thông tin đối với bản thân mỗi sinh viên, đặc biệt là sinh viên mang những đặc thù đặc biệt - sinh viên trường Đại học An ninh nhân dân.

Ngoài ra, tác giả còn căn cứ vào những văn bản, Luật hiện hành có liên quan đến chủ đề an ninh thông tin thời kỳ 4.0 như: Luật tiếp cận thông tin năm 2016, Luật An ninh mạng năm 2018, cùng các bài nghiên cứu, tạp chí từ các trang của Bộ Thông tin và Truyền truyền, Bộ Công an và các ban ngành, tổ chức cơ sở đã nghiên cứu, báo cáo về các chủ đề gần với chủ đề này.

Thông qua những cơ sở Pháp lý trên, bước đầu vạch rõ những vấn đề nghiên cứu cụ thể về thời cơ và thách thức của sinh viên trong thời kỳ chuyển đổi số về an ninh thông tin trên không gian mạng.

3. Phương pháp nghiên cứu

Bài báo cáo sử dụng phương pháp luận của chủ nghĩa duy vật biện chứng, chủ nghĩa duy vật lịch sử của chủ nghĩa Mác Lênin, tư tưởng Hồ Chí Minh và đường lối chính sách của Đảng, Nhà nước Việt Nam về con người, nhà nước pháp quyền về bảo đảm quyền riêng tư trên không gian mạng theo pháp luật Việt Nam hiện hành.

Quá trình nghiên cứu, báo cáo sử dụng các phương pháp nghiên cứu cụ thể như: nghiên cứu tài liệu, phân tích, tổng hợp, phương pháp luật học so sánh, đối chiếu, phân tích thuần túy quy phạm pháp luật,... để phân tích và luận chứng các vấn đề khoa học cần làm sáng rõ trong báo cáo này, các phương pháp được sử dụng cụ thể như sau:

- Phương pháp nghiên cứu tài liệu: Phương pháp này được sử dụng để thu thập và nghiên cứu những kết quả của các tác giả trong sách, báo, tạp chí, báo cáo tổng kết liên quan đến chủ đề bài báo cáo.

- Phương pháp phân tích - tổng hợp: Phương pháp được sử dụng xuyên suốt báo cáo để nghiên cứu, phản biện đưa ra lập luận chính xác, đánh giá đúng những thời cơ và thách thức của an ninh sinh viên về thông tin số trên không gian mạng, đồng thời đề xuất giải pháp phù hợp nâng cao hiệu quả bảo đảm an ninh thông tin sinh viên thời đại 4.0.

- Phương pháp luật học so sánh: Phương pháp này được sử dụng thông qua vận dụng, so sánh tham khảo kinh nghiệm của một số nghiên cứu, báo cáo khác liên quan đến an ninh thông tin trên không gian mạng.

Trong quá trình thực hiện báo cáo, tác giả tiếp thu có chọn lọc kết quả nghiên cứu của các công trình khoa học đã công bố; các đánh giá, tổng kết của các cơ quan chuyên môn và các chuyên gia về những vấn đề có liên quan đến các vấn đề nghiên cứu.

4. Kết quả nghiên cứu và đề xuất giải pháp

Chuyển đổi số trên phương diện tổng quát là quá trình thay đổi toàn diện trong cách thức vận hành, tổ chức của một cơ quan, một đơn vị, một tập thể hay một bộ máy. Các chương trình làm việc, các dữ liệu được số hoá dựa trên cơ sở hạ tầng của kỹ thuật số. Hiện nay, Đảng và Nhà nước ta đã lãnh đạo các ngành đẩy mạnh ứng dụng khoa học công nghệ, xây dựng và triển khai chính sách thúc đẩy phát triển ngành công nghiệp công nghệ thông tin, điện tử - viễn thông. Kinh tế số được hình thành và phát triển dần trở thành một bộ phận quan trọng của nền kinh tế, công nghệ số được áp dụng ngày càng nhiều trong mọi lĩnh vực từ nông nghiệp, công nghiệp đến dịch vụ từ đó tạo nhiều cơ hội về việc làm, tăng tính tiện ích và nâng cao chất lượng cuộc sống cho nhân dân. Việc xây dựng chính phủ điện tử, chính phủ số được triển khai quyết liệt và bước đầu đạt được nhiều kết quả tích cực, trong đó việc cung cấp tài khoản định danh điện tử được đánh giá là một giải pháp đột phá nâng cao hiệu quả và bảo mật các dịch vụ công năm trong Đề án 06 “Phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số (CĐS) quốc gia giai đoạn 2022- 2025, tầm nhìn đến năm 2030” phục vụ chuyển đổi số quốc gia. Mô hình chính phủ điện tử hướng đến tăng tính hiệu quả, cải thiện chất lượng, tăng khả năng tiếp cận dịch vụ công và tính minh bạch, trách nhiệm cao hơn. Người dân sẽ được thông báo và theo sát những hoạt động, chính sách mà chính phủ đã đề ra và đang thực hiện từ đó tăng độ minh bạch của chính phủ. Mặt khác, mô hình này giúp cải thiện được hiệu quả so với hệ thống hành chính làm việc trên bàn giấy, giúp tiết kiệm thời gian, đồng thời rút gọn khoảng cách giao tiếp giữa chính phủ và doanh nghiệp, giảm được phần chi phí dành cho việc phục vụ các hoạt động của công chức và mua sắm công. Cuối cùng, nó cho phép người dân có thể truy cập và thu thập thông tin liên quan đến bất kỳ bộ phận nào của chính phủ và tham gia vào quá trình ra quyết định của chính phủ. Tuy nhiên, một vài vấn đề về bảo mật thông tin cá nhân xuất hiện, việc lưu trữ dữ liệu của công dân có thể bị xem là kiểm soát quyền riêng tư hoặc lạm dụng cho mục đích khác, đồng thời tiềm ẩn nguy cơ mất cắp dữ liệu, rò rỉ thông tin hoặc thông tin bị bán, sử dụng cho các mục đích thương mại. Song hành cùng chính phủ số là những nền tảng rộng lớn của thông tin được số hóa trên mạng xã hội, các website yêu cầu cung cấp thông tin để thực hiện các thuật toán khảo sát tâm lý người dùng, người sử dụng được đề xuất những sản phẩm phù hợp với nhu cầu, mong muốn, tuy nhiên cũng tiềm ẩn rủi ro bởi những kết quả độc hại mà các đối tượng cài cắm lợi dụng lỗ hổng thuật toán để tiếp cận người dùng. Từ việc kiểm soát thông tin người dùng, các nhà chủ quan các công ty công nghệ phần mềm đó có thể sử dụng trực tiếp các dữ liệu cá nhân thậm chí trở thành món hàng được đưa lên sàn giao dịch trở thành món hàng thông tin béo bở cho các mục đích thương mại khác.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Trong kỷ nguyên mà cả thế giới đang chứng kiến một sự thay đổi lớn về hình thái hoạt động theo cuộc Cách mạng Công nghệ 4.0, bản thân mỗi sinh viên có muôn vàn cơ hội để phát triển năng lực bản thân, bắt kịp xu hướng phát triển của thời đại. Bên cạnh đó, họ đồng thời phải đối mặt với những rủi ro tiềm ẩn trên không gian mạng bao gồm sự riêng tư và thông tin cá nhân, xác thực thông tin và chịu tác động trực tiếp từ các rủi ro bảo mật trên không gian mạng. Hệ lụy từ những nguy cơ thường gặp trên không gian mạng đã được chỉ ra rất nhiều lần nhưng vẫn luôn là một vấn đề nóng đáng được lưu tâm, cảnh báo.

4.1. Kết quả nghiên cứu:

Dẫn luận theo đánh giá của Bộ Thông tin và Truyền thông (TT&TT), cơ quan thường trực Ủy ban quốc gia về chuyển đổi số, công tác tổ chức kiểm tra, đánh giá, giám sát bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin, triển khai “Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025 tầm nhìn 2030”. Theo Thứ trưởng Bộ TT&TT Nguyễn Huy Dũng, điểm cảnh báo đỏ là giá trị của chỉ số an toàn thông tin mạng năm 2022 tuy đã có tăng trưởng trên 46% so với năm 2021, nhưng vẫn ở mức thấp, dưới mức trung bình, mới chỉ đạt 0,48. Do đó, đây tiếp tục là vấn đề cần đặc biệt quan tâm trong năm 2023. Tính đến hết tháng 6-2023, tuy tổng số hệ thống thông tin của cơ quan nhà nước đã phê duyệt hồ sơ đề xuất cấp độ an toàn là 1.949/3.094, đạt 63%; nhưng số hệ thống thông tin của cơ quan nhà nước đã đáp ứng yêu cầu bảo đảm an toàn theo cấp độ mới chỉ là 285/3.094, đạt tỷ lệ 9,2%, Bộ TT&TT đưa ra nhận định, đây là nguy cơ mất an toàn, an ninh mạng ở mức rất cao.

4.1.1. Thực trạng về an ninh sinh viên trên không gian mạng trong thời kỳ chuyển đổi số

Dẫn luận theo đánh giá của Bộ Thông tin và Truyền thông (TT&TT), cơ quan thường trực Ủy ban quốc gia về chuyển đổi số, công tác tổ chức kiểm tra, đánh giá, giám sát bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin, triển khai “Chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025 tầm nhìn 2030”. Theo Thứ trưởng Bộ TT&TT Nguyễn Huy Dũng, điểm cảnh báo đỏ là giá trị của chỉ số an toàn thông tin mạng năm 2022 tuy đã có tăng trưởng trên 46% so với năm 2021, nhưng vẫn ở mức thấp, dưới mức trung bình, mới chỉ đạt 0,48. Do đó, đây tiếp tục là vấn đề cần đặc biệt quan tâm trong năm 2023. Tính đến hết tháng 6-2023, tuy tổng số hệ thống thông tin của cơ quan nhà nước đã phê duyệt hồ sơ đề xuất cấp độ an toàn là 1.949/3.094, đạt 63%; nhưng số hệ thống thông tin của cơ quan nhà nước đã đáp ứng yêu cầu bảo đảm an toàn theo cấp độ mới chỉ là 285/3.094, đạt tỷ lệ 9,2%, Bộ TT&TT đưa ra nhận định, đây là nguy cơ mất an toàn, an ninh mạng ở mức rất cao.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Trước sự phổ biến của kết nối Internet, các ứng dụng dựa trên website và hệ thống thông tin chứa mã nguồn mở, ranh giới dữ liệu được xóa mờ, mức độ tương tác, giao thức trực tuyến trở nên dễ dàng, người dùng có thể truy cập, tìm kiếm các thông tin công khai, thu thập dữ liệu bán công khai trên cơ sở tự do tìm kiếm và tiếp nhận thông tin. Xu hướng công nghệ mang lại sự cạnh tranh ngày càng tăng, cùng với đó là sự xuất hiện của nhiều lỗ hổng và rủi ro bảo mật, các tác nhân độc hại có thể dễ dàng truy cập và khai thác dữ liệu một cách hợp pháp. An ninh thông tin trên không gian mạng đã trở thành một vấn đề quan trọng, bằng chứng về các vụ phá hoại thành công gây ra tác động tàn phá to lớn đối với các tổ chức cá nhân.

Thực trạng thông tin sai lệch trên không gian mạng

Thứ nhất, thông tin chưa qua kiểm duyệt tự do tung hoành tiếp cận người tiêu dùng thông tin, internet với đặc điểm về sự chia sẻ thông tin nhanh chóng, kiểm duyệt không chặt chẽ với mục đích chia sẻ thông tin khác nhau và nhu cầu tiêu thụ thông tin lớn từ người dùng đã khiến thông tin sai lệch, tin giả lan truyền một cách nhanh chóng. Theo nghiên cứu của Viện Công nghệ Massachusetts, tin giả lan truyền nhanh hơn so với tin tức thật với tốc độ lan truyền gấp 10 lần so với những tin tức hợp pháp. Không những thế phạm vi tiếp cận của các thông tin này còn rộng hơn rất nhiều so với các tin tức hợp pháp, 1% tin giả tiếp cận được từ 1.000 đến 100.000 người trong khi thông tin có độ xác thực cao, đã qua kiểm duyệt chỉ tiếp cận được hơn 1.000 người, trong đó tin tức chính trị sai lệch có tốc độ lan truyền nhanh nhất.

Thứ hai, thông tin xuyên tạc, sai trái được các đối tượng, thế lực thù địch nhào nặn, nê nếm thêm những mâu thuẫn, mơn trớn những tư tưởng cực đoan hướng đến đầu độc người tiêu dùng thông tin. Theo số liệu thống kê của Bộ Thông tin và Truyền thông, Việt Nam hiện nay có 1.952 trang thông tin điện tử tổng hợp và 935 mạng xã hội trong nước đã được cấp phép hoạt động. Đây đều là những diễn đàn trực tuyến để người dân có thể tự do chia sẻ, bày tỏ thông tin, quan điểm cá nhân. Theo đó, những thông tin về Việt Nam không có tự do biểu đạt, tự do báo chí, tự do ngôn luận hay không có Internet mà các thế lực lưu vong phản động bàn tán về cộng đồng mạng chúng ta là hoàn toàn sai trái. Một số tổ chức phản động như “Việt Tân”, “Chính phủ quốc gia Việt Nam lưu vong”, “VOA tiếng việt” đã thiết lập các diễn đàn trực tuyến, trang Facebook, các kênh Youtube, Tiktok liên tục đưa một khối lượng lớn những thông tin sai lệch, những quan điểm sai trái, thù địch lên không gian mạng. Chúng sử dụng triệt để mạng xã hội, ứng dụng tối đa công nghệ thông tin để bẻ cong sự thật, bóp méo thông tin, cắt ghép hình ảnh, video để xuyên tạc, bôi nhọ, dựng chuyện đời tư của một số nhân sự cấp cao của Đảng liên quan đến một vài cán bộ cấp cao bị xử lý kỷ luật trong thời gần đây nhằm phá hoại niềm tin của Nhân dân vào Đảng, Nhà nước nhằm âm mưu thực hiện “diễn biến hòa bình, bạo loạn lật đổ”. Ngày 11/01/2023, sự việc về một clip dài 15 giây xuất

hiện trên không gian mạng được cho là có 01 nữ sinh trường Đại học Ngoại ngữ Tin học thành phố Hồ Chí Minh đang học quân sự tại Trường Quân sự Quân khu 7 bị quân nhân cưỡng bức tập thể và nhảy lầu tự tử. Sau đó, vụ việc được lan truyền với tốc độ khủng khiếp trên các nền tảng mạng xã hội và các phần tử, đối tượng phản động chia sẻ, đăng tải, tuyên truyền sai lệch, gán ghép Quân đội giấu diếm, không cung cấp thông tin xác thực. Từ đó, chúng tạo thành một chiến dịch “truyền thông bẩn”, xuyên tạc hình ảnh, hạ thấp nhân phẩm, uy tín, phẩm chất tốt đẹp của Quân nhân. Đáng báo động hơn những thông tin sai sự thật đó được cộng đồng mạng lan truyền một cách chóng mặt trên các mạng xã hội, các nền tảng video, diễn đàn trực tuyến. Mỗi cư dân mạng phải nâng cao kiến thức cá nhân về các vấn đề trong đời sống văn hóa, xã hội, thường xuyên cập nhật các thông tin chính thống qua các kênh thông tin, các Fanpage, các Cổng thông tin điện tử của các cơ quan Đảng, Nhà nước, các cơ quan báo chí chính thống như: Báo Nhân dân, Thông tin Chính phủ, VTV24, Truyền hình Quốc Hội, các Cổng thông tin điện tử, các Fanpage của chính quyền địa phương. Từ đó, mỗi cá nhân “tự đề kháng”, “tự miễn dịch” trước những thông tin xấu, độc, có đủ khả năng nhận diện và phản bác lại các quan điểm sai trái, thù địch trên không gian mạng.

Thứ ba, thông tin mang tính công kích, xúc phạm danh dự nhân phẩm cá nhân, tuy tương tác trên không gian ảo nhưng tác động mà nó mang lại là những tác động ảnh hưởng trực tiếp đến người tham gia không gian mạng. Theo Điều 25, Hiến pháp nước Cộng hòa xã hội chủ nghĩa Việt Nam năm 2013 ghi nhận mọi công dân đều có quyền tự do ngôn luận. Tuy nhiên, Hiến pháp cũng đảm bảo các quyền, lợi ích khác của các nhân như: quyền bất khả xâm phạm về đời sống riêng tư; bí mật cá nhân và gia đình; quyền bất khả xâm phạm về sức khỏe, danh dự, nhân phẩm. Các hành vi đăng tải, chia sẻ, bình luận có nội dung chưa được kiểm chứng, sai sự thật, xúc phạm danh dự, nhân phẩm, làm mất uy tín cá nhân, cơ quan, tổ chức có thể bị xử phạt hành chính tùy thuộc tính chất và mức độ nghiêm trọng của vụ việc.

Thứ tư, sự ảnh hưởng của người nổi tiếng và phát ngôn của mình, một số người nổi tiếng sử dụng sức ảnh hưởng từ lời nói của mình tác động trực tiếp đến tư duy, suy nghĩ và hành động của người tiêu dùng thông tin trên không gian mạng. Đứng trước bối cảnh đáng “báo động” về văn hóa ứng xử của người nổi tiếng trên mạng xã hội, trong không gian công cộng lại rơi vào diện cấp thiết. Những phát ngôn phóng túng, thiếu kiểm soát, những thông tin thiếu chính xác, những hành vi vi phạm pháp luật diễn ra với mật độ dày đặc đã khiến nhiều nghệ sĩ mất điểm trong lòng công chúng. Lời nói, ngôn ngữ, hành vi vốn là “cái vỏ vật chất của tư duy” nên hiện tượng “lệch chuẩn” trong văn hóa ứng xử của một số văn nghệ sĩ nhanh chóng bị tẩy chay. Tuy nhiên, chính những phát ngôn này ảnh hưởng không nhỏ đến một bộ phận đại chúng tiếp nhận thông tin, họ có xu

hướng tin vào những dữ liệu được những người nổi tiếng đề cập mà không cần tìm hiểu nguồn cơ hay kiểm tra tính xác thực của thông tin.

Trong bối cảnh thông tin và an ninh thông tin trở nên nóng hơn bao giờ hết, cá nhân mỗi người tham gia không gian mạng cần ý thức, nghiêm túc hơn về vấn đề tiếp nhận và xử lý thông tin. Cũng như cơ thể chúng ta, nếu khỏe mạnh, cường tráng, có đủ sức đề kháng thì sẽ dễ dàng miễn dịch được trước những bệnh dịch nguy hiểm. Vì vậy, cách tốt nhất để xây dựng một cộng đồng mạng thông thái, biết tiếp nhận những thông tin chính thống, sàng lọc, loại bỏ những thông tin xấu, độc, những quan điểm sai trái, thù địch thì mỗi cư dân mạng phải nâng cao “sức đề kháng”, “tự miễn dịch” trước những luồng thông tin đó.

Thực trạng “bạo lực thông tin” trên không gian mạng

Bạo lực ảo nạn nhân thật, người sử dụng thông tin với các tương tác của mình trên không gian mạng vô tình dính líu vào các xung đột, đe dọa, bắt nạt thậm chí là ngược đãi về mặt tinh thần đối với nạn nhân thông qua điện thoại, máy tính. Các hành vi tấn công hình sự hoặc phi hình sự trực tuyến có thể ảnh hưởng trầm trọng đến sức khỏe thể chất, tâm lý hoặc tình cảm của nạn nhân. Kinh khủng hơn, khi bạo lực mạng không chỉ diễn ra một mình, mà còn là nhiều người cùng rủ nhau bạo lực mạng hội đồng. Không ít những hậu quả đáng buồn đã xảy ra, nhẹ thì bị ảnh hưởng gây nên tình trạng rối loạn tâm thần, trầm cảm, nặng hơn nữa là những hành động nghĩ quẩn, chọn cách kết liễu bản thân để giải thoát khỏi những ám ảnh về hành vi bạo lực mạng mà họ phải gánh nhận. Theo khảo sát năm 2019 của Viện nghiên cứu quản lý phát triển bền vững (MSD) và Tổ chức cứu trợ trẻ em quốc tế (Save the Children) cho biết chỉ tính riêng năm 2018 số vụ báo cáo liên quan Việt Nam về hình ảnh/video xâm hại tình dục trẻ em trên mạng là 706.435 - đứng thứ 2 trong ASEAN, chỉ sau Indonesia. Tương tự, năm 2019 tổ chức cũng cung cấp số liệu báo cáo về an ninh thông tin trên không gian mạng cho biết 21% thanh, thiếu niên Việt Nam tham gia khảo là nạn nhân của bắt nạt trên mạng và hầu hết (75%) đều không biết về đường dây nóng hoặc các dịch vụ có thể giúp họ nếu bị bắt nạt, hoặc bị bạo lực trên mạng. Một nghiên cứu khác của tổ chức cứu trợ trẻ em quốc tế (Save the Children) chỉ ra rằng, 70,8% trẻ em Việt Nam từ 11 đến 14 tuổi từng chứng kiến hành vi bắt nạt trực tuyến, trong đó có 60,2% là nạn nhân của bắt nạt trực tuyến. Tác hại của bạo lực mạng vô cùng lớn, nó ảnh hưởng trực tiếp đến tâm lý của nạn nhân, khiến họ sợ hãi, lo lắng, bất an, hoặc tệ hơn là phải chịu sự chi phối của các đối tượng xấu như trộm cắp, giết người. Nỗi đau gây ra bởi bắt nạt qua mạng là rất lớn và không thể lường trước được, nếu không được kiểm soát can thiệp kịp thời nó có thể trở thành một vết sẹo xuyên suốt cả cuộc đời của nạn nhân bạo lực mạng.

Xâm hại quyền riêng tư trên không gian mạng

Sự phát tán các mã độc trên các mạng xã hội, nhằm xâm nhập vào thông tin cá nhân của nạn nhân từ việc vô tình cung cấp thông tin cá nhân về tên đăng nhập và mật khẩu, một vài trường hợp được ghi nhận về mất tiền oan từ việc mất an toàn về thông tin ngân hàng. Trích dẫn từ báo cáo tổng kết tình hình An ninh mạng Việt Nam 6 tháng đầu năm 2023 số vụ tấn công an ninh mạng vào các hệ thống tại Việt Nam lên đến hơn 5.100 vụ, gần 400 cơ quan tổ chức có tên miền “.gov.vn” và “.edu.vn” bị xâm nhập, chèn mã quảng cáo cờ bạc, cá độ, hàng loạt hình thức lừa đảo tinh vi liên tục xảy ra, thiệt hại có vụ việc lên đến hàng trăm triệu đồng. Các cuộc gọi lừa đảo qua Zalo, Facebook ngày càng biến chuyển khó lường với sự xuất hiện của công nghệ Deepface khiến cho các nạn nhân dễ bị sa bẫy vì được mắt thấy, tai nghe bằng hình ảnh, âm thanh, chính công nghệ này xoá nhoà ranh giới giữa thật và giả.

Sự xâm nhập và phát tán các hình ảnh nhạy cảm cá nhân, làm ảnh hưởng đến nhân phẩm danh dự của nạn nhân, đặc biệt là những vụ việc liên quan đến xâm hại, bạo lực trẻ em trên không gian mạng. Theo thống kê của UNICEF, 92% trẻ em Việt Nam được tiếp xúc sử dụng các thiết bị kết nối internet, duy trong năm 2022 Tổng đài Quốc gia Bảo vệ trẻ em đã ghi nhận 1.500 cuộc gọi can thiệp hỗ trợ, trong đó có 419 cuộc gọi báo cáo về hoạt động xâm hại trẻ em trên không gian mạng.

Các thiết bị thông minh, trí tuệ nhân tạo bùng nổ trong thời kỳ chuyển đổi số, nhất là sự phát triển của các ứng dụng trên điện thoại thông minh nó trở thành mối đe dọa an ninh mạng, trật tự an toàn xã hội, do người dùng cấp quá nhiều quyền truy cập, cũng như cung cấp thông tin cá nhân trên mạng xã hội, ứng dụng nhắn tin gọi điện trực tuyến dẫn đến tình trạng bị chiếm đoạt, lợi dụng vi phạm pháp luật. Đặc biệt, các mối đe dọa đến từ các thiết bị IoT vẫn là vấn đề lớn, hiện chưa có giải pháp tổng thể nào nhằm bảo đảm an toàn, an ninh mạng, bảo vệ bí mật nhà nước cho các thiết bị IoT, do đó nhiều vụ lộ, lọt thông tin cá nhân nhạy cảm, riêng tư bị phát tán trên mạng. Các cơ quan ban, ngành đã được cảnh báo về nguy cơ bị chiếm đoạt thông tin, tài liệu, song sự chủ quan, thiếu kiến thức, ý thức bảo mật của người tiêu dùng thông tin vô hình chung tạo điều kiện thuận lợi cho các đối tượng xấu tấn công, chiếm đoạt, thu thập hình ảnh, dữ liệu cá nhân sử dụng vào mục đích bất chính.

Dẫn luận số liệu thực tế

Trích dẫn số liệu từ Trung tâm Giám sát an toàn không gian mạng quốc gia NCSC về cảnh báo an toàn thông tin tuần 32 năm 2023. Theo đó, các tổ chức quốc tế đã công bố và cập nhật ít nhất 871 lỗ hổng, trong đó có 304 lỗ hổng mức cao, 215 lỗ hổng mức trung bình, 03 lỗ hổng mức thấp và 349 lỗ hổng chưa đánh giá, trong đó có ít nhất 130 lỗ hổng cho phép chèn và thực thi mã lệnh - đồng nghĩa với việc chương trình làm việc bị ảnh hưởng, gián đoạn thậm chí có thể bị kiểm soát ngược từ các đối tượng. Ở Việt

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Nam, các chương trình tấn công lừa đảo người dùng trên không gian mạng ghi nhận 365 nạn nhân phản ánh do sử dụng Internet, qua kiểm tra phân tích có nhiều trường hợp lừa đảo giả mạo website của ngân hàng, các trang thương mại điện tử. Đáp ứng những yêu cầu về vấn đề nhận diện và phòng tránh tội phạm lừa đảo công nghệ cao Bộ Thông tin và Truyền thông đưa ra Cẩm nang: Nhận diện và phòng chống lừa đảo trực tuyến, các hình thức lừa đảo trên không gian mạng được đối tượng thực hiện bằng nhiều hình thức khác nhau và ngày càng tinh vi nhắm vào nhiều đối tượng ở những độ tuổi khác nhau, nhằm dẫn dụ, lấy lòng đánh cắp thông tin người dùng, chiếm đoạt tài sản. Trong đó, có 03 nhóm lừa đảo chính giả mạo thương hiệu, chiếm đoạt tài sản và các hình thức kết hợp khác.

Hình 1: Danh sách IP/tên miền độc hại có nhiều kết nối từ Việt Nam

differentia.ru: 7422 IP		xjpakmdcfuqe.ru: 18 IP
STT	Website lừa đảo	Ghi chú
1	Ymx33.com	Website giả mạo Amazon
2	shopelpie.com bb9998.com h5.50db8hsdoq.shop	Website giả mạo sàn TMĐT Shopee
3	eulo99.com fhel11.com eulo11.com	Website giả mạo sàn TMĐT Tiki
4	nouespaipenedes.com	Website giả mạo MXH Facebook
5	dichvucongbaohiemxahoi.com dangkyhosotruoctuyen2023.com handico.vaytienmat-nhanh24h.com m.vnsc-finhay.com ...	Website giả mạo, lừa đảo

Hình 2: Danh sách website lừa đảo người dùng Việt Nam

Hình 3: Danh sách thông tin điểm yếu, lỗ hổng

6	Apache	CVE-2023-39508 CVE-2023-37581 CVE-2022-47185 ...	Nhóm 05 lỗ hổng trong Apache cho phép đối tượng tấn công thực thi mã từ xa, thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép	Đã có thông tin xác nhận và bản vá
7	Cisco	CVE-2020-26064 CVE-2020-26065 CVE-2020-26082	Nhóm 03 lỗ hổng trong Cisco phép đối tượng tấn công thực thi mã tùy ý, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

Số liệu thống kê về các vụ việc liên quan trong vòng một tuần đủ nói lên tình trạng nghiêm trọng của an ninh trên không gian mạng về vấn đề thông tin và bảo mật.

Pháp luật về an ninh thông tin trên không gian mạng

TT	Sản phẩm/ dịch vụ	Mã lỗi quốc tế	Mô tả ngắn	Ghi chú
1	Microsoft	CVE-2023-21709 CVE-2023-35385 CVE-2023-36903 ...	Nhóm 74 lỗ hổng trong Microsoft cho phép đối tượng tấn công thực hiện leo thang đặc quyền, thực thi mã từ xa, thực hiện lỗi Spoofing, tấn công từ chối dịch vụ.	Đã có thông tin xác nhận và bản vá
2	Linux	CVE-2023-4128 CVE-2023-4147 CVE-2023-4194	Nhóm 04 lỗ hổng trong Linux (kernel) cho phép đối tượng tấn công thực hiện leo thang đặc quyền, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
3	Google	CVE-2023-33913 CVE-2023-20783 CVE-2023-20784 ...	Nhóm 38 lỗ hổng trong Google cho phép đối tượng tấn công thực hiện leo thang đặc quyền, tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá
4	Wordpress	CVE-2023-3452 CVE-2023-2843 CVE-2023-4140 ...	Nhóm 77 lỗ hổng trong Wordpress cho phép đối tượng tấn công thực hiện tấn công chèn SQL, tấn công CSRF, thực hiện tấn công XSS, truy cập và thực hiện các hành động trái phép.	Đã có thông tin xác nhận và bản vá
5	Zoom	CVE-2023-36534 CVE-2023-39216 CVE-2023-36541 ...	Nhóm 15 lỗ hổng trong Zoom cho phép đối tượng tấn công thực hiện leo thang đặc quyền, tấn công từ chối dịch vụ, truy cập và thực hiện các hành động trái phép.	Chưa có thông tin xác nhận và bản vá

Trước những mối đe dọa đáng quan ngại về tình hình mất an toàn, an ninh thông tin, lộ, lọt dữ liệu cá nhân, bí mật nhà nước. Các thế lực thù địch không ngừng gia tăng các hoạt động chống phá Đảng, Nhà nước, tiến hành đầu độc vào thể hệ trẻ những tư tưởng lệch lạc, những thông tin sai trái, bịa đặt, xuyên tạc lịch sử. Chính phủ quyết tâm

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

triển khai các đề án hướng đến nhiệm vụ bảo đảm an toàn thông tin, thể chế hoá kịp thời chủ trương, đường lối của Đảng và Nhà nước thông qua các Luật, Văn bản quy phạm pháp luật về bảo mật, an toàn và an ninh mạng.

- Luật tiếp cận thông tin số 104/2016/QH13 có hiệu lực thi hành từ ngày 01/7/2018. Đây là luật rất quan trọng, tạo khuôn khổ pháp lý cho việc thực hiện quyền tiếp cận thông tin của công dân và nâng cao tính công khai, minh bạch trong hoạt động của các cơ quan nhà nước.

- Luật Bảo vệ bí mật nhà nước được Quốc hội khóa XIV thông qua tại Kỳ họp thứ 6 ngày 15/11/2018. Luật gồm 5 chương và 28 điều, có hiệu lực thi hành kể từ ngày 01/7/2020. Trong đó, một số quy định liên quan đến lập, thẩm định, ban hành danh mục bí mật nhà nước, thời hạn bảo vệ bí mật nhà nước, gia hạn thời hạn bảo vệ bí mật nhà nước có hiệu lực thi hành kể từ ngày 01/01/2019. Luật quy định về thời hạn bảo vệ bí mật nhà nước, gia hạn thời hạn bảo vệ bí mật nhà nước. Đây là quy định mới vì Pháp lệnh số 30/2000/PL-UBTVQH10 và các văn bản trước Pháp lệnh đều không quy định thời hạn bảo vệ bí mật nhà nước. Luật quy định thời hạn bảo vệ đối với bí mật nhà nước độ Tuyệt mật là 30 năm, độ Tối mật là 20 năm, độ Mật là 10 năm. Luật quy định, bí mật nhà nước được giải mật khi hết thời hạn bảo vệ bí mật nhà nước và thời gian gia hạn thời hạn bảo vệ hoặc giải mật để đáp ứng yêu cầu thực tiễn bảo vệ lợi ích quốc gia, dân tộc, phát triển kinh tế - xã hội, hội nhập, hợp tác quốc tế hoặc bí mật nhà nước không còn thuộc danh mục bí mật nhà nước. Thông tin về quốc phòng, an ninh, cơ yếu là một trong 15 lĩnh vực thuộc phạm vi Bí mật nhà nước. Căn cứ vào tính chất quan trọng của nội dung thông tin, mức độ nguy hại nếu bị lộ, bị mất thì thông tin bí mật thuộc lĩnh vực Cơ yếu được phân loại thành 03 độ mật là: Tuyệt mật, Tối mật và Mật (Điều 8).

- Luật An ninh mạng được Quốc hội thông qua ngày 12/6/2018, có hiệu lực thi hành kể từ ngày 01/01/2019. Luật gồm 07 chương, 43 điều quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức và cá nhân.

Sinh viên an ninh với vấn đề về an toàn thông tin trên không gian mạng

Nhận thức được vai trò và nhiệm vụ thông qua các môn học đại cương từ năm nhất về vấn đề bảo mật và an ninh thông tin nội bộ, nâng cao trình độ nhận thức về chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, quan điểm chủ trương, chính sách của Đảng và Nhà nước để ứng phó trước tác động tiêu cực của thông tin độc, tin xấu trên không gian mạng. Nâng cao trình độ, kiến thức chuyên môn để có đủ khả năng nhận thức, phản biện các thông tin sai trái, xuyên tạc, từ đó nâng cao khả năng “miễn dịch” với tin giả trên không gian mạng.

Hiểu được vai trò và tầm quan trọng của việc bảo vệ an toàn thông tin, kịp thời cung cấp những thông tin về xâm phạm an ninh thông tin cho các cơ quan chức năng có thẩm quyền. Là người tiêu dùng thông tin trong thời đại số hoá, khi tiếp nhận thông tin phải biết thẩm định đánh giá thông tin, luôn nghi ngờ về tính xác thực và tìm kiếm những minh chứng kiểm chứng, đối chiếu thông tin, từ đó đánh giá độ tin cậy của thông tin. Hạn chế cung cấp thông tin cá nhân trên các trang mạng xã hội, các website trực tuyến, tuyệt đối bảo mật các hồ sơ liên quan đến việc học tập theo quy định của ngành. Luôn được giáo dục tư tưởng sâu sắc và quan điểm, bản lĩnh chính trị vững vàng để có khả năng phản bác lại các luận điệu sai trái, xuyên tạc của thế lực thù địch. Ý thức sâu rộng về vai trò của an toàn và an ninh thông tin, là cánh tay nối dài giữa pháp luật với gia đình, bạn bè và xã hội.

4.1.2. An toàn thông tin trong sử dụng mạng xã hội

Khái niệm mạng xã hội là một khái niệm để chỉ một website mở, nối kết các thành viên cùng sở thích, mối quan tâm trên không gian Internet với nhiều mục đích khác nhau, có thể tương tác trực tuyến không giới hạn về không gian, thời gian và ranh giới quốc gia. Những trang mạng xã hội là môi trường màu mỡ cung cấp, chia sẻ, sáng tạo đa nội dung, là nơi giao lưu kết nối bạn bè trên toàn thế giới, góp phần phát triển các lĩnh vực về kinh doanh online, quảng cáo trực tuyến thúc đẩy sự phát triển của xã hội ngày càng sâu sắc hơn. Một lượng thông tin khổng lồ được tạo lập bởi người dùng cùng sự tương tác trực tuyến xuất hiện và tăng dần lên mỗi ngày. Internet tại Việt Nam 2023 đang phát triển mạnh với 77 triệu người dùng chiếm 79,1% dân số, mạng xã hội cũng trở thành nền tảng quan trọng với hơn 70 triệu người tham gia tương đương 71% tổng dân số. Dẫn luận số liệu thống kê từ báo cáo Digital Vietnam năm 2023, Việt Nam nằm trong top 10 quốc gia có lượng người dùng Facebook nhiều nhất thế giới với 66,2 triệu tín đồ trong tổng số 2,99 tỉ người dùng trên toàn thế giới, tương tự Việt Nam cũng góp mặt trong top 10 về số lượng người dùng đối với các trang mạng xã hội TikTok và Youtube. Tổng số kết nối di động đang hoạt động là 161,6 triệu, tương đương với 164,0% tổng dân số. Dữ liệu này cho thấy Việt Nam có tổng số người dùng Internet và mạng xã hội rất đáng kể, cùng với số lượng kết nối di động vượt quá tổng dân số, đồng nghĩa với việc tăng khả năng rủi ro về an ninh mạng.

Căn cứ vào các khái niệm về an toàn thông tin mạng, các đặc điểm phù hợp riêng cho mạng xã hội trong thực tế, an toàn thông tin trên mạng xã hội bao gồm:

- Bảo vệ an toàn cá nhân trước những thông tin không lành mạnh trên mạng xã hội, đặc biệt là các thông tin giả mạo, tin độc, tin xấu. Các thông tin không đúng sự thật bị các đối tượng xấu lợi dụng gây ảnh hưởng nhằm mục đích bôi nhọ, xúc phạm danh dự, uy tín, lôi kéo kích động đám đông, mức độ lan truyền các thông tin đó rất nhanh và

khó kiểm soát, gây ảnh hưởng cực kỳ lớn đối với người tiêu dùng thông tin nếu không có các biện pháp tự bảo vệ mình trước sự tấn công của các nguồn tin đó.

- Bảo vệ an toàn không bị lây nhiễm mã độc qua mạng xã hội. Không gian mở trên mạng xã hội giúp người dùng dễ dàng tham gia các trò chơi, truy cập tùy ý vào các đường liên kết. Tuy nhiên chúng ta lại không để ý các điều khoản, các quyền mà trò chơi, hoặc ứng dụng yêu cầu cấp quyền truy cập, dẫn đến tiêu tốn băng thông dữ liệu mạng di động hoặc liên tục nhận được các thông báo rác, bị gắn thẻ, nhắc tên vào những bài viết không liên quan. Nguy hại hơn là nguy cơ bị đánh cắp thông tin tài khoản cá nhân, một vài trường hợp ghi nhận các kẻ gian xâm nhập đánh cắp thông tin ngân hàng qua những dữ liệu mà ta vô tình cung cấp.

- Bảo vệ an toàn thông tin cá nhân trước nguy cơ tấn công của những “kẻ cắp” trên không gian mạng. Thông qua việc đăng tải các hình ảnh, video, hoặc những bình luận, tin nhắn nhạy cảm, người dùng phải đối mặt với nhiều rủi ro khi các nguồn dữ liệu đó bị xâm nhập và phát tán một cách trái phép.

- Bảo vệ an toàn cá nhân không bị lừa đảo, không bị lợi dụng để phát tán các thông tin giả mạo, lừa đảo chiếm đoạt tài sản. Một số phương thức lừa đảo trên mạng xã hội được đề cập như: cung cấp thông tin, chuyển tiền để nhận mã trúng thưởng, giả mạo Bộ Công An, luật sư đe dọa, tống tiền. Hiện nay đáng báo động hơn là việc lừa đảo sử dụng công nghệ trí tuệ nhân tạo nạn nhân trực tiếp giao tiếp với đối tượng qua hình thức cuộc gọi trực tuyến nhưng đối tượng đội lốt, được chỉnh sửa khuôn mặt trông giống với người thân cận của nạn nhân, từ đó tiến hành hành vi phạm pháp một cách công khai.

4.1.3. Thời cơ và thách thức đối với sinh viên trong thời đại 4.0 về vấn đề an toàn thông tin trên không gian mạng

Phát biểu tại ngày An toàn thông tin Việt Nam với chủ đề “An toàn, an ninh mạng – Yếu tố then chốt để thúc đẩy chuyển đổi số quốc gia”, Bộ trưởng Bộ Thông tin và Truyền thông Nguyễn Mạnh Hùng nhận định rằng “Cuộc di chuyển vĩ đại nhất trong lịch sử nhân loại là cuộc di chuyển từ thế giới thực sang thế giới ảo. Nhưng tất cả các quốc gia đều lo lắng về an toàn, an ninh mạng trong thế giới ảo. Niềm tin số sẽ trở thành yếu tố quyết định cho sự thành công của cuộc di chuyển này”. Đối với bản thân mỗi sinh viên cần nhận thức rõ cơ hội và những thách thức của bản thân nhằm tìm ra giải pháp tối ưu, nắm bắt thời cơ, không ngừng phát triển bản thân mình, đồng thời giải quyết triệt để những vấn đề nảy sinh trong thời kỳ chuyển đổi số này.

Cơ hội đối với sinh viên

Thứ nhất, sinh viên có cơ hội tìm kiếm những trải nghiệm đa dạng về thông tin, môi trường học tập, các cuộc thi dành cho sinh viên, các hội nghị, tọa đàm, tìm kiếm việc làm trên nền tảng trực tuyến. Đó là cơ hội để sinh viên có thể mở rộng kiến thức

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

bản thân, giải đáp những thắc mắc về những vấn đề đã được học, tìm kiếm chuyên sâu về tài liệu học tập, các bài báo cáo chuyên đề, các báo cáo nghiên cứu khoa học trên đa lĩnh vực, từ đó sinh viên tự tin hơn bao giờ hết về những kiến thức được xây đắp ngày một nhiều hơn, học hỏi qua những kết quả đã qua nghiên cứu, xây dựng nền tảng cơ sở cho những bước tiến lớn hơn trong tương lai.

Thứ hai, sự xuất hiện của Công nghệ 4.0 vô hình chung đã cắt giảm, thay thế nhiều nhân sự trong lĩnh vực công nghiệp, dịch vụ, tuy nhiên cũng rất nhiều công việc liên quan đến thời kỳ số hoá từ đó mà xuất hiện, mà điển hình cơ bản nhất là các công việc liên quan đến nhà sáng tạo nội dung trên các nền tảng mạng xã hội, các chuyên viên về phân tích dữ liệu, các nhà phát triển ứng dụng thông minh và nguồn nhân lực để vận hành chuỗi vận tải thông minh trên không gian mạng như tài xế Grab, Bee,...

Thứ ba, tính năng động, sáng tạo, khả năng thích ứng với sự thay đổi của cuộc cách mạng 4.0, sinh viên trong giai đoạn hiện nay có đầy đủ năng lực, hiểu biết và đam mê về công nghệ, hiện đại hoá. Chính niềm yêu thích, đam mê này giúp họ tự nâng vị thế của mình trong môi trường cạnh tranh khốc liệt, trở thành ứng viên sáng giá trong mắt nhà tuyển dụng. Sinh viên thời kỳ số hóa nhận thức được tầm quan trọng của những kỹ năng cần thiết đáp ứng khung yêu cầu năng lực số của UNESCO bao gồm: năng lực thông tin và dữ liệu, năng lực vận hành thiết bị và phần mềm, năng lực giao tiếp và hợp tác, năng lực sáng tạo nội dung số, an ninh, giải quyết vấn đề và các năng lực liên quan đến nghề nghiệp, nhằm bắt kịp và theo đuổi những đam mê trong cuộc Cách mạng 4.0

Thách thức đối với sinh viên

Thách thức lớn nhất của bản thân mỗi sinh viên trong thời kỳ chuyển đổi số là thách thức về khả năng theo đuổi kiến thức nền tảng, sự phát triển vượt bậc của kiến thức được cập nhật từng ngày từng giờ, những phát minh công nghệ ra đời hàng tuần hàng tháng, mỗi phát minh nhỏ kết hợp trong kỷ nguyên số đem đến những sự bùng nổ, ảnh hưởng mạnh mẽ đến nhận thức của mỗi cá nhân. Yêu cầu đặt ra là, làm sao mỗi cá nhân sinh viên nhận thức được tầm quan trọng của việc theo đuổi các kiến thức, cập nhật kỹ năng, trau dồi bản thân không ngừng nghỉ, liên tục cập nhật kiến thức thông qua nguồn dữ liệu mở trên Internet, không để suy nghĩ bị lỗi thời trước những tác động to lớn của cuộc Cách mạng 4.0.

Bên cạnh đó, theo báo cáo của tổ chức McKinsey công bố năm 2018 về khả năng việc làm được tự động hóa, robot hoá làm gia tăng tỷ lệ thất nghiệp, đến năm 2030 khoảng 70% công ty trên khắp thế giới sẽ sử dụng trí tuệ nhân tạo, tỷ lệ tự động hoá đối với tất cả các công việc ở Hoa Kỳ là 38%, ở Nhật Bản nằm mức 24% và Hàn Quốc là 22%, trung bình ở các nước thuộc Tổ chức hợp tác và phát triển kinh tế OECD sẽ là 14%. Đây là điều không mới của những cuộc cách mạng công nghiệp, bản chất của mỗi lần cải cách là phát minh những công cụ mới giúp thực hiện công việc dễ dàng hơn,

nhanh và hiệu quả hơn, giúp tiết kiệm thời gian và công sức. Đồng thời, đặt ra cho bậc giáo dục đại học cần thiết giải quyết những yêu cầu về hiện đại hoá kiến thức, chương trình giáo dục, đặt mục tiêu cho giáo dục nhanh hơn, chính xác hơn, đề ra những tiêu chuẩn đánh giá mới để đào tạo nguồn nhân lực hiện đại đáp ứng nhu cầu của cuộc Cách mạng 4.0.

Cuối cùng, thách thức lớn nhất đối với sinh viên hiện nay là khả năng tiếp nhận, xử lý thông tin và bảo đảm an ninh thông tin trên không gian mạng. Những thay đổi về cách thức giao tiếp trên Internet cũng đặt con người vào nhiều nguy hiểm tài chính, sức khỏe tâm thần, an toàn trên không gian mạng. Thông tin cá nhân nếu không được bảo vệ một cách an toàn sẽ dẫn đến những hệ lụy khôn lường. Các thông tin được tự do đăng tải trên mạng xã hội chưa được kiểm duyệt chặt chẽ về nội dung vô tình trở thành liều thuốc đầu độc tư duy của giới trẻ, một bộ phận sinh viên tiếp xúc với những nguồn tin độc, tin giả, những luận điệu xuyên tạc về Đảng, Nhà nước nhưng không đủ khả năng phản biện hay nhận thức và bài trừ các nội dung đó. Sự xâm nhập của các mã nguồn độc thông qua các trang web là mối nguy ngại ảnh hưởng trực tiếp đến tính bảo mật thông tin cá nhân, các đối tượng có thể thu thập và giả mạo thông tin nhằm chiếm đoạt các tài khoản điện tử, kiểm soát hành vi bản thân nạn nhân, thậm chí ăn cắp các thông tin về ngân hàng, tín dụng tạo ra những rủi ro không lường về mất cắp và nợ tín dụng. Không dừng lại ở đó, các thế lực thù địch, phân tử cơ hội lợi dụng đưa các tin, bài viết sai lệch, bịa đặt những hạn chế của Đảng, Nhà nước nhằm phủ nhận những thành quả cách mạng to lớn mà ông cha ta đã dày công gây dựng.

Để đương đầu với những thách thức trong thời đại mới, thời đại số hóa phát triển mạnh mẽ, bản thân là sinh viên cần chuẩn bị kỹ lưỡng cho bản thân những tri thức về công nghệ, ngoại ngữ, kỹ năng mềm và tích góp càng nhiều kinh nghiệm từ thực tế để mở ra cánh cửa toàn năng bước vào sân chơi toàn cầu hoá.

4.3. Đề xuất một số giải pháp

Mặc dù các chuyên gia an ninh mạng làm việc chăm chỉ để thu hẹp các lỗ hổng bảo mật, nhưng những kẻ tấn công luôn tìm kiếm những cách mới để thoát khỏi sự kiểm soát đó, trốn tránh các biện pháp phòng thủ và khai thác các điểm yếu mới xuất hiện. Các mối đe dọa an ninh mạng mới nhất đang tạo ra một vòng xoáy mới cho các mối đe dọa cũ, lợi dụng môi trường làm việc tại nhà, các công cụ truy cập từ xa và các dịch vụ đám mây. Những mối đe dọa nay đang thâm nhập dần vào cuộc sống thường nhật của tất cả mọi người. Để bảo đảm an toàn, an ninh thông tin trên không gian mạng cho, nhằm tạo cơ hội nắm bắt những thời cơ, điều kiện phát triển trong thời kỳ chuyển đổi số, khắc phục những hạn chế, đương đầu với thách thức hướng đến mục tiêu phát triển toàn diện. Tác giả đề xuất một số giải pháp như sau:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thứ nhất, không ngừng ra sức học tập, trau dồi kiến thức kỹ năng về các lĩnh vực công nghệ, kỹ thuật mới, nâng cao trình độ ngoại ngữ, trang bị cho bản thân những kỹ năng mềm cần thiết cùng những kinh nghiệm làm việc thực tế mà ta có thể tích lũy, qua các cơ hội làm việc trực tuyến. Trong cuộc cách mạng 4.0, sinh viên cần chủ động sáng tạo chuẩn bị đầy đủ cho bản thân những vốn tri thức cần thiết để tự mở ra cánh cửa bước vào sân chơi của tri thức và công nghệ.

Thứ hai, bản thân mỗi người phải có trách nhiệm tự bảo vệ thông tin cá nhân và tự chịu trách nhiệm khi sử dụng, cung cấp thông tin bản thân trên không gian mạng. Đồng thời, hạn chế đưa các thông tin quan trọng lên mạng xã hội, thay đổi mật khẩu mặc định bằng các mật khẩu từ 8 ký tự trở lên, kết hợp số, chữ cái in hoa cùng các ký tự đặc biệt. Sử dụng mật khẩu để bảo vệ các tập tin chứa nội dung quan trọng, thường xuyên cập nhật các bản vá lỗi của các phần mềm, các ứng dụng để tăng tính bảo mật cá nhân.

Thứ ba, không ngừng học tập trau dồi nâng cao bản lĩnh chính trị, kịp thời đấu tranh, kiên quyết phê phán, phản bác mạnh mẽ bài viết có nội dung tin giả, tin đồn thất thiệt, thổi phồng, bóp méo, xuyên tạc sự thật trên không gian mạng. Nhận biết, đấu tranh phản bác mọi hành vi lợi dụng “dân chủ”, “nhân quyền” để phát tán tài liệu vu cáo, vu khống Đảng và Nhà nước. Tăng cường công tác quản lý nội bộ, kịp thời đấu tranh và xử lý đối với những cán bộ, đảng viên có biểu hiện suy thoái về tư tưởng chính trị, đạo đức, lối sống, “tự diễn biến”, “tự chuyển hóa”, kịp thời phát hiện, ngăn chặn những phần tử cơ hội và bất mãn chính trị đưa ra thông tin giả, tin đồn thất thiệt tuyên truyền chống phá Đảng và Nhà nước trên mạng xã hội.

Thứ tư, bản thân người tiêu dùng thông tin, khi tiếp nhận dữ liệu phải biết thẩm định, đánh giá độ xác thực của nó. Cần xác định thông tin trong bài viết mới xảy ra hay đã cũ, video và hình ảnh trong bài viết đã được kiểm chứng chưa. Nếu nghi ngờ về tính xác thực của thông tin, hãy thử tìm kiếm từ khóa về sự kiện được nêu trong bài viết trên các phương tiện tìm kiếm trực tuyến nhằm xem xét thời điểm chính xác thông tin đó được đăng. Những thông tin chính thống, đúng sự thật thường chứa đường dẫn tới các nguồn tin đáng tin cậy, hiển thị thời gian cụ thể. Những thông tin khác có thể là giả mạo, sai sự thật. Mỗi cư dân mạng phải thể hiện trách nhiệm với chính bản thân mình và cộng đồng khi tiếp nhận thông tin trên không gian mạng, vừa là bảo vệ bản thân khỏi những rủi ro không đáng có, vừa là để trở thành cánh tay nối dài về những thông tin chính xác đến với gia đình, bạn bè và xã hội

Cuối cùng, tránh kết nối Wifi ở các khu vực công cộng, các địa chỉ Wifi bảo mật kém, việc sử dụng Wifi tại các nhà ga, trạm xe, sân bay có thể vô tình cho các mã độc cơ hội xâm nhập và kiểm soát thông tin cá nhân trên thiết bị di động của chúng ta. Để hạn chế những rủi ro đó, khi truy cập các kết nối không dây tại nơi công cộng ta hãy sử dụng mạng ảo thông

qua các VNP giả lập nếu có thể, tránh trao đổi các thông tin nhạy cảm, mã hoá các tập tin khi đang truy cập kết nối đó.

5. Kết luận

Đề tài tập trung khảo sát nghiên cứu về thực trạng an ninh thông tin sinh viên trong thời kỳ chuyển đổi số, đặc biệt so sánh, đối chiếu mức độ ảnh hưởng của các tác nhân đó đến mọi mặt của đời sống sinh viên giai đoạn hiện nay. Từ đó, khẳng định mức độ tác động sâu rộng của các nhân tố, đánh giá ưu điểm, hạn chế làm rõ nguyên nhân, làm rõ những thời cơ, thách thức, hướng đến xây dựng giải pháp bảo đảm an ninh sinh viên trên không gian mạng.

Sự phát triển càng nhanh của công nghệ lại càng mở ra hàng vạn những thách thức và nguy cơ mới về an toàn, an ninh thông tin. Bản chất liên kết của các hoạt động trên không gian mạng và tốc độ chuyển đổi kỹ thuật số đồng nghĩa với việc các cuộc tấn công gây ra có thể ảnh hưởng rộng lớn đến tất cả các lĩnh vực và đời sống xã hội. Chính vì vậy, an ninh thông tin và bảo đảm an ninh thông tin dần trở thành một yêu cầu bức thiết, một bộ phận quan trọng của an ninh quốc gia. Là sinh viên trong thời kỳ chuyển đổi số, luôn đối mặt với vô vàn thách thức và thời cơ, đồng thời có thể bị kiểm soát, ảnh hưởng bởi các nguồn thông tin khác nhau. Bài báo cáo tập trung phân tích làm rõ những thực trạng, ảnh hưởng về vấn đề an ninh thông tin ở Việt Nam đặc biệt là đối với sinh viên, chỉ rõ những vấn đề đặt ra trong bảo đảm an ninh thông tin, đề xuất giải pháp trọng tâm nâng cao hiệu quả bảo đảm an ninh thông tin trong thời gian tới. Trong đó có năm nhóm giải pháp nhằm nâng cao nhận thức, trách nhiệm, tận dụng mọi nguồn lực dữ liệu phong phú đa dạng, các thủ thuật nâng cao bảo mật thông tin, bảo vệ bản thân, gia đình trước khỏi những tấn công trên không gian mạng.

LỜI CẢM ƠN

Để có được sự thành công của đề tài này, tác giả đã kế thừa kết quả các nghiên cứu đã được công bố trước đó về vấn đề “An toàn thông tin trên không gian mạng”, đồng thời là sự quan tâm, tạo điều kiện, góp ý và gợi ý chỉnh sửa từ quý thầy cô. Đề tài được xây dựng và phát triển độc lập trên ý tưởng của tác giả, mọi thông tin có liên quan được trích dẫn khoa học cụ thể, tác giả xin cam đoan về tính xác thực và tranh chấp về mọi thông tin được trình bày trong đề tài.

Tác giả xin cảm ơn sự đóng góp, ủng hộ từ quý thầy cô và các cộng sự đã làm nên sự thành công của đề tài.

DANH MỤC TÀI LIỆU THAM KHẢO

Quốc hội (2018), Luật An ninh mạng

Nguyễn Thị Quế, Vũ Công Giao, Ngô Minh Hương, Lã Khánh Tùng (2018), *Quyền về sự riêng tư*, NXB. Chính trị Quốc gia Sự thật, Hà Nội.

TS. Lê Văn Phùng (2018), *An toàn thông tin Việt Nam*, NXB Thông tin và truyền thông.

- Ths. Lâm Đông Hồ (2023), *Thực trạng an toàn thông tin mạng hiện nay ở Việt Nam và giải pháp phòng chống vi phạm pháp luật trên không gian mạng*, Tạp chí công thương.
- Pam Nigro (2022), *Cybersecurity governance: A path to cyber maturity*, International Journal of Smart Grid and Clean Energy, 1(1), 1–6.
- Ani, U. P. D., He, H., & Tiwari, A. (2017), *Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective*, Journal of Cyber Security Technology, 1(1), 32–74.

**CÁC MÔI ĐE DOẠ AN NINH MẠNG MÀ HỌC SINH,
SINH VIÊN ĐANG PHẢI ĐỐI MẶT TRONG THỜI KỲ
CHUYỂN ĐỔI SỐ**

**CYBER SECURITY THREATS THAT STUDENTS ARE FACED
IN THE PERIOD OF DIGITAL TRANSFORMATION**

Trần Thị Quỳnh Như

Trường Đại học Sư Phạm - Đại học Đà Nẵng

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> MXH: Mạng xã hội SV: Sinh viên	Tình hình an ninh thông tin ở Việt Nam đã và đang có những diễn biến phức tạp. Tại các tổ chức giáo dục dường như vấn đề này vẫn chưa thực sự được quan tâm nhiều, trong khi đây cũng là môi trường chứa nhiều thông tin nhạy cảm. Môi trường Đại học là môi trường cởi mở và tự do thông tin. Hơn nữa, đặc trưng của cấp đào tạo Đại học, Cao đẳng, đặc biệt là những trường có danh tiếng trên thế giới là khả năng nghiên cứu. Một môi trường mở như vậy không tránh khỏi các lỗ hổng. Bên cạnh những vấn đề hữu ích, thực tế cho thấy, mạng xã hội còn tồn tại các mặt tiêu cực như sự lan truyền các thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, “đổi trắng, thay đen”, phủ nhận Chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, chống phá đường lối, chính sách của Đảng, Nhà nước. Những thông tin này được xem là thông tin phi chính trị trên mạng xã hội. Nghiên cứu này nhằm khắc họa bức tranh tổng thể về thực trạng sử dụng mạng xã hội ở Việt Nam trong giai đoạn hiện nay, trong đó có đối tượng là học sinh, sinh viên Việt Nam, qua đó giúp học sinh, sinh viên nhận diện và phòng tránh các thông tin xấu, độc trên mạng xã hội, tránh bị các thế lực xấu lợi dụng. ABSTRACT The information security situation in Vietnam has been experiencing complicated developments. At educational institutions, it seems that this issue has not really received much attention, while this is also an environment containing a lot of sensitive information. The University environment is an environment of openness and freedom of information.
<i>Keywords:</i> MXH: social network SV: student	

Furthermore, a characteristic of University and College training levels, especially prestigious schools in the world, is research ability. Such an open environment cannot avoid failures. Besides useful issues, reality shows that social networks also have negative aspects such as the spread of fabricated information, distorting the truth, distorting issues, "changing white and black". , denying Marxism-Leninism, Ho Chi Minh's ideology, opposing the guidelines and policies of the Party and State. This information is considered non-political information on social networks. This study aims to portray an overall picture of the current situation of social network use in Vietnam in the current period, including Vietnamese students, thereby helping students recognize Identify and prevent bad and toxic information on social networks, avoid being taken advantage of by bad forces.

1. Đặt vấn đề:

Mạng xã hội là dịch vụ kết nối các thành viên cùng sở hữu trên internet với nhau nhiều mục tiêu khác nhau không phân biệt thời gian và thời gian (còn gọi là mạng xã hội ảo). Trong những năm gần đây, mạng xã hội có bước phát triển mạnh mẽ, hoạt động lớn đến mọi mặt đời sống kinh tế, xã hội ở hầu hết các quốc gia trên thế giới, trong đó có Việt Nam. Về thời gian sử dụng, người Việt Nam vào MXH hơn 2,5 giờ mỗi ngày. Đối tượng sử dụng mạng internet thường xuyên nhất là nhóm nhẹ nhàng từ 15-40 tuổi. Nhóm đối tượng này chủ yếu là học sinh, sinh viên và người lao động. Nhìn chung, họ là những người trẻ, có điều kiện cận kề với máy tính và mạng internet, nhanh nhạy trong công việc tiếp theo những tiến bộ khoa học công nghệ cũng như những buổi trào lưu mới trên thế giới. Ngoài ra, riêng đối với sinh viên, những tiện ích mà MXH mang lại còn nhiều ý nghĩa tích cực khác như nâng cao hiệu quả học tập, giao tiếp và tìm kiếm cơ hội nghề nghiệp,... Thông qua MXH, sinh viên có thể liên kết hợp tác với các nhóm cùng sở thích, cùng quan tâm, cùng ý nguyện có thể gặp gỡ, trao đổi trên mạng, làm cơ sở thực hiện những hành động thực tiễn, có ý nghĩa tích cực như: tổ chức các hoạt động từ thiện nhân những ngày Tết, giúp đỡ trẻ em đường phố, tổ chức những hoạt động sinh hoạt văn hóa lành mạnh.

Bên cạnh những tiện ích nêu trên, MXH còn tồn tại nhiều mặt tiêu cực, mang thông tin xuyên đố, kích động, bôi nhọ, nói xấu,... Đặc biệt, các thế lực thù địch và tội phạm lợi dụng MXH làm công cụ đạt năng lực cho các hoạt động hòa hiệp tư tưởng, “diễn biến hòa bình” chống phá Đảng, Nhà nước ta, điều đó đặt ra không ít khó khăn,

quy thức cho công tác quản lý thông tin trên MXH. Bên cạnh sự năng động, nhiệt huyết của học sinh, sinh viên hiện tại vẫn có chế độ xác định hạn chế nhất. Trong đó, hạn chế phát hiện và ngăn chặn các thông tin xấu trên mạng xã hội hiện nay, trước hạn chế này các đối tượng chống phá Đảng và Nhà nước lợi dụng học sinh, sinh viên để thực hiện mục tiêu của chúng. Đặc biệt hơn, mỗi đe dọa đang ngày càng phức tạp và có mức độ nguy hiểm cao đó là khi chính chúng ta dùng những lời lẽ thô tục, khiển trách, chê bai giữa những người xung quanh chúng ta thậm chí là những người mà chúng ta không hề quen biết, dùng những từ ấy để bôi nhọ họ, khiến cho họ rơi vào hệ lụy, thậm chí là tìm đến cái chết. Vấn đề này đang gặp phải rất nhiều trong môi trường học đường từ Trung học cơ sở đến cấp bậc Đại học. Và đây cũng chính là lí do bài tham luận này xuất hiện để tìm hiểu về nguyên nhân những vụ việc này diễn ra như thế nào và nó đã được khắc phục bằng cách nào mà hiện nay hầu hết các trường hợp tìm đến cái chết hoặc rơi vào trầm cảm đều xuất phát từ vấn đề an ninh mạng này.

2. Phương pháp nghiên cứu

Thông tin tiêu cực trên mạng internet đã xuất hiện từ lâu. Tuy nhiên, từ khi cuộc cách mạng công nghệ số bùng nổ với số lượng các MXH phát triển nhanh, thêm vào đó là số lượng người dùng tăng trong đó học sinh, sinh viên là đối tượng sử dụng chiếm tỷ lệ cao, các thế lực phản động đã sử dụng MXH để thực hiện âm mưu của mình. Trước tình hình đó đã có những nghiên cứu để nhằm đưa những số liệu cụ thể về thực trạng sử dụng MXH, cũng như giúp cho người sử dụng MXH phòng tránh trước những thông tin không chính xác.

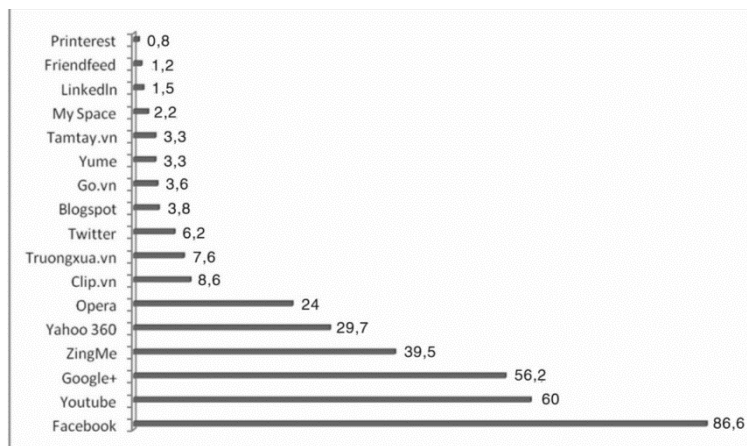
Nghiên cứu của nhóm tác giả Nguyễn Thị Kim Hoa, Nguyễn Lan Nguyên (2014) đã trình bày nghiên cứu đánh giá về “Tác động của mạng xã hội facebook đến sinh viên hiện nay”. Nghiên cứu dựa trên kết quả khảo sát của 212 sinh viên và phỏng vấn sâu 21 sinh viên trường Đại học Khoa học xã hội và nhân văn, trong đó chỉ ra thực trạng Internet, mạng xã hội đã để lại nhiều ảnh hưởng tích cực lẫn tiêu cực đến tư tưởng, đời sống, quá trình học tập và rèn luyện của sinh viên. Mục đích nghiên cứu nhằm tìm hiểu về thái độ của sinh viên đối với mạng xã hội họ đang sử dụng. Nghiên cứu được tiến hành bằng phương pháp sử dụng bảng hỏi và phỏng vấn. Tác giả Nguyễn Nhâm, “Phòng chống thông tin xấu độc trên mạng xã hội” đã nghiên cứu đưa ra thực trạng sử dụng và nhận diện thông tin xấu trên MXH để giúp cán bộ, đảng viên có cách nhìn tổng quát và tránh những thông tin trái chiều trên MXH hiện nay. Cũng nghiên cứu về vấn đề này PGS, TS Trần Nam Chuân -Ths Lê Văn Nam cũng đã đưa ra những giải pháp “ngăn chặn thông tin xấu độc trên MXH” nhằm giúp các cá nhân sử dụng chủ động phòng tránh. Nhìn chung các công trình nghiên cứu nêu trên đã trình bày được một số vấn đề về công tác quản trị an ninh mạng xã hội, an ninh thông tin mạng xã hội và ảnh hưởng của mạng xã hội đối với sinh viên. Tuy nhiên, nội dung, đối tượng, phạm vi nghiên cứu

của các công trình trên chỉ nêu lên được một phần nội dung, cho đến nay vẫn chưa có công trình nghiên cứu.

3. Thực trạng sử dụng mạng xã hội trong sinh viên

3.1. Các mạng xã hội phổ biến, số người và số giờ sử dụng trong ngày

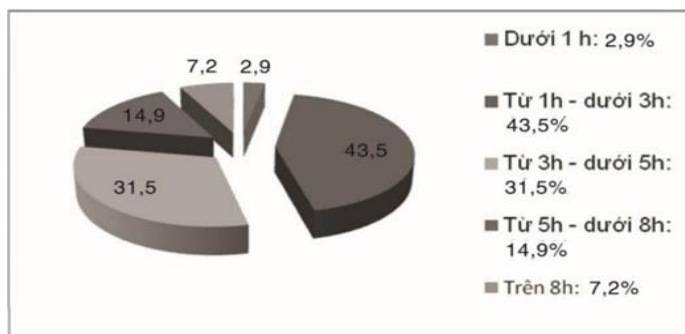
Biểu đồ 1: Các mạng xã hội được sinh viên sử dụng (%)



Biểu đồ 1 cho thấy Facebook hiện đang là MXH được ưa dùng nhất trong SV - chiếm 86,6%. Không chỉ được ưa dùng ở Việt Nam mà trên toàn thế giới, Facebook đang được xếp thứ nhất trong số 11 MXH lớn. Do Facebook có tính tương tác cao, kho lưu trữ ứng dụng

lớn, đa ngôn ngữ và phát triển sớm trên mạng di động nên mức độ sử dụng của Facebook đối với SV là rất cao. Xếp ở vị trí thứ hai trong nghiên cứu này là Youtube, với 60% SV sử dụng. Những SV tham gia cộng đồng mạng này không chỉ giải trí bằng các bộ phim, bài hát mà còn có thể học hỏi được các chủ đề đa dạng như lịch sử, ngoại ngữ hay các kỹ năng sống, cách lựa chọn trang phục, kiểu tóc v.v.. Google+ xếp hạng ở vị trí thứ 3 trong số các MXH được SV Việt Nam ưa dùng với tỉ lệ 56,2%. Các SV Việt Nam, do yêu cầu của hoạt động học tập, nên cần phải lập thư điện tử (gmail) để liên lạc với giảng viên, các thành viên trong các nhóm học tập, bạn bè v.v.. Tài khoản Google của họ được mặc định là một tài khoản của MXH Google+, ngay cả khi họ không bao giờ đăng nhập vào nó. Xem xét những khó khăn thường gặp phải khi sử dụng MXH, kết quả khảo sát cho thấy: chỉ có 24,5% SV cho rằng họ có gặp khó khăn khi sử dụng MXH. Trong đó, hai khó khăn lớn nhất mà SV gặp phải là sự hạn chế về ngoại ngữ (chiếm 39,6%) và không nắm vững chức năng của MXH (chiếm 22,2%). Ngoài ra, những khó khăn khác cũng được sinh viên nhắc tới, đó là: sử dụng MXH chưa thuần thục (chiếm 16,1%) và SV cảm thấy lúng túng trước một lượng thông tin lớn trên mạng (chiếm 13,8%). Một số cản trở nhỏ khác (trong tổng số 9,9%) được SV nêu ra về phía khách quan như mạng yếu, mạng bị chặn và khó khăn chủ quan là thiếu thời gian và không làm chủ được thời gian để vào MXH. Nghiên cứu cũng đề cập đến khía cạnh thời gian SV dành ra mỗi ngày để truy cập MXH. Kết quả về thời gian sử dụng MXH trong ngày của SV được trình bày ở biểu đồ 2.

Biểu đồ 2: Số giờ sử dụng mạng xã hội trong ngày (%)



Biểu đồ 2 cho thấy tỉ lệ SV thường sử dụng MXH từ 1 giờ đến dưới 3 giờ/ngày là cao nhất (chiếm 43,5%), và từ 3 giờ đến dưới 5 giờ/ngày (chiếm 31,5%). Đáng lưu ý là: có 7,2% SV cho biết họ thường bỏ ra trên 8 giờ/ngày để vào MXH. Lượng thời gian này là đáng báo động về một trong những dấu hiệu cho thấy nguy cơ nghiện MXH trong SV. Theo nghiên cứu của Tiffany A và cộng sự (2009), SV đại học Hoa Kỳ sử dụng Facebook trung bình từ 10 đến 30 phút mỗi ngày. Trong nghiên cứu của chúng tôi, kết quả cho thấy có đến trên 50% SV sử dụng MXH nhiều hơn 3 giờ mỗi ngày. Khi các nhu cầu của giới trẻ không được đáp ứng một cách toàn diện thì việc ngồi nhiều thời gian trên MXH để họ học tập, tán gẫu, giải trí, tìm cảm giác mạnh thông qua các trò chơi điện tử là điều dễ hiểu. Mặc dù vậy, hiệu quả của việc đáp ứng các nhu cầu đã chiếm nhiều thời gian từ một môi trường ảo đang gây nhiều ồn ào, bàn tán là điều đáng để quan tâm nghiên cứu.

Tại Việt Nam, với sự phát triển mạnh mẽ của công nghệ, MXH đóng góp một phần không nhỏ đưa người Việt Nam hòa nhập với thế giới. Theo số liệu của ComScore -một trong những công ty dẫn đầu thế giới về đo lường và đánh giá hiệu quả các giải pháp marketing trực tuyến, báo cáo về thị trường trực tuyến tại Việt Nam và châu Á đã công bố, Việt Nam hiện là một trong những quốc gia có dân số trực tuyến lớn nhất tại khu vực ASEAN. Học sinh, sinh viên Việt Nam đang sử dụng các MXH có độ phủ sóng toàn cầu như Facebook, Instagram, Youtube, Twitter, Myspace... với nhiều tiện ích đáp ứng được các nhu cầu cá nhân trước những tiện ích MXH mang lại. Trong danh sách các MXH kể trên có lẽ nổi bật nhất vẫn là Facebook, sau đó tới youtube với tính năng hỗ trợ xem và chia sẻ video hiện là trang mạng có lượng người dùng lớn thứ hai ở Việt Nam (56,3%); đứng thứ ba là Instagram (24,5%) chuyên xem và chia sẻ ảnh; Zingme (16,8%); các mạng Viber, Zalo chiếm tỷ lệ 10% và các MXH chiếm tỷ lệ thấp về người dùng như Twitter, Myspace, Gov.vn. Theo số liệu mới nhất từ Liên Hợp Quốc, tính đến ngày 22/04/2019, dân số Việt Nam là 97.249.676 người. Tính đến tháng 10 năm 2018, Việt Nam có 64 triệu người dùng internet chiếm 67% dân số. Về sử dụng MXH, Việt Nam có đến 55 triệu người dùng đang hoạt động, đạt tỉ lệ 57% người dùng internet. Tuy nhiên, nếu chỉ xét riêng về MXH Facebook, Việt Nam xếp thứ 7 trong số các quốc gia

có người dùng, với 59 triệu người dùng vào tháng 7 năm 2018. Số liệu người dùng MXH ở Việt Nam được thể hiện cụ thể như sau:



3.2. Nhu cầu sử dụng mạng xã hội

Mục đích của mỗi người khi tham gia MXH hết sức phong phú, đa dạng, song có những mục đích cơ bản như sau: tìm kiếm, cập nhật thông tin xã hội (66,3%); làm quen với bạn mới, giữ liên lạc với bạn cũ (60%); liên lạc với gia đình, bạn bè (59%). Những nhu cầu này chủ yếu xuất hiện thanh, thiếu niên bởi vì họ đang trong độ tuổi năng động, nhạy bén, sáng tạo, luôn hướng tới cái mới, cái khác biệt và đặc biệt. Phần lớn học sinh, sinh viên sống xa gia đình (đi học, đi làm) nên việc kết nối, thiết lập và duy trì các mối quan hệ (trực tuyến) với người thân, bạn bè sẽ trở thành nhu cầu thiết yếu của mỗi cá nhân. Mục đích chiếm tỷ lệ cao chủ yếu nhằm phục vụ cho nhu cầu giải trí, đây là nhu cầu được các chuyên gia tâm lý nhận định là có chỉ số cao trong giai đoạn phát triển tâm lý ở lứa tuổi này. Bằng cách tận hưởng những thú vui cuộc sống và khẳng định cái tôi bản thân, đó là chia sẻ thông tin (hình ảnh, video, status) với mọi người (54,0%) và để giải trí (49,5%). Mục đích tiếp theo, MXH được xem là một công cụ hỗ trợ cho học tập và làm việc, chiếm (44,7%). Ngoài ra, một bộ phận học sinh, sinh viên còn sử dụng MXH với nhiều mục đích khác như: mua sắm online (30,7%); tìm kiếm việc làm (21,7%), hoặc bán hàng online (13,7%).... Như vậy, với nhiều ứng dụng tiện ích khác nhau, các trang MXH đã đáp ứng được gần như đầy đủ các mục đích, nhu cầu của học sinh, sinh viên trong thời đại công nghệ số hiện nay.

Nghiên cứu việc sử dụng MXH của bất cứ nhóm người nào, các tác giả trên thế giới đều tập trung xác định những nhu cầu của người sử dụng khi tham gia vào MXH. Kiểm định độ tin cậy của toàn thang đo về nhu cầu sử dụng MXH của SV cho kết quả α Cronbach = 0,826 (cho thấy thang đo có độ tin cậy đảm bảo). Sau khi tiến hành phân tích nhân tố để cấu trúc lại số liệu định lượng của thang đo từ 20 nhu cầu bằng phương pháp Varimax, chúng tôi thu được 5 nhóm nhu cầu về sử dụng MXH (giải thích 54,074% sự biến thiên của biến) có tên tương ứng với các nội dung như sau:

1/ Nhóm nhu cầu chia sẻ ($\alpha = 0,702$), bao gồm các nội dung liên quan đến: bày tỏ cảm xúc, ý kiến; thăm dò, hỏi đáp thắc mắc; gửi quà tặng, lời chúc, ..

2/ Nhóm nhu cầu thể hiện bản thân và tìm kiếm việc làm ($\alpha = 0,685$), bao gồm: quảng cáo sản phẩm; tham gia cuộc thi trên mạng; chat sex, chụp hình nude; và tìm kiếm việc làm.

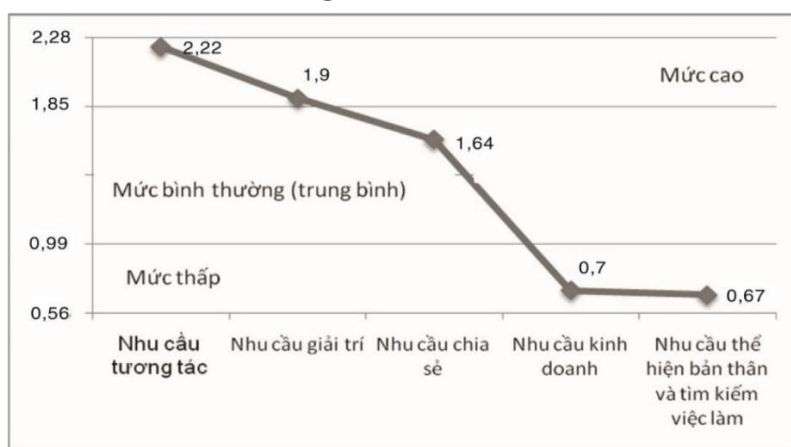
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

3/ Nhóm nhu cầu giải trí ($\alpha = 0,617$), gồm: nghe nhạc, xem phim; chơi game; cập nhật thông tin, sự thật xảy ra trong xã hội và đọc truyện.

4/ Nhóm nhu cầu kinh doanh ($\alpha = 0,766$), gồm: mua hàng; bán hàng và các hoạt động thu hút liên quan đến quảng cáo.

5/ Nhóm nhu cầu tương tác ($\alpha = 0,616$), gồm: giao lưu, kết bạn; tìm kiếm người thân, bạn bè và chat, gửi tin nhắn. Giá trị trung bình của từng nhóm nhu cầu được trình bày ở biểu đồ 4, cho thấy: khi sử dụng MXH, SV có nhu cầu tương tác (ĐTB = 2,22) và nhu cầu giải trí (ĐTB = 1,90) ở mức cao; nhóm nhu cầu chia sẻ nằm trong mức bình thường (ĐTB = 1,64). Trong khi đó, nhóm nhu cầu kinh doanh (ĐTB = 0,7) và nhu cầu thể hiện bản thân, tìm kiếm việc làm (ĐTB = 0,67) nằm ở mức thấp.

Biểu đồ 4: Điểm trung bình các nhóm nhu cầu sử dụng mạng xã hội



Xét về đặc điểm hoạt động của SV, ngoài việc học tập thì phát triển, gìn giữ các mối quan hệ xã hội cũng là hoạt động chủ đạo và có ý nghĩa quan trọng trong việc phát triển các đặc điểm tâm lý cá nhân. Do vậy, việc các SV sử dụng nhiều nhất MXH như công cụ để trò chuyện, tương tác với người khác là điều dễ nhận thấy. Ngoài mục đích giao tiếp, kết nối với bạn bè, SV cũng là những người có nhu cầu giải trí cao khi những mối bận tâm về gia đình, công việc còn chưa chiếm nhiều tâm trí và thời gian của họ. Nhìn chung, hầu hết các MXH đều được khen ngợi vì tính năng cung cấp nguồn giải trí cho người sử dụng như nghe nhạc, xem phim, chơi game trực tuyến. Chỉ cần một chiếc máy tính hay điện thoại di động có kết nối internet, các SV dễ dàng xem phim, nghe nhạc, đọc truyện, chơi game, v.v. trong bất cứ thời gian và địa điểm nào. Có lẽ đây là lý do khiến việc thực hiện nhu cầu giải trí cũng nằm mức độ cao trong nghiên cứu này. Nhóm nhu cầu kinh doanh và nhu cầu thể hiện bản thân, tìm kiếm việc làm nằm ở mức thấp cho thấy việc kinh doanh qua MXH không phải là mối bận tâm của SV. Bên cạnh đó, 80% SV trong nghiên cứu này đang học đại học năm thứ I, thứ II và thứ III đại học, nên có thể họ chưa bị áp lực về công việc tương lai nên việc tìm kiếm công việc trên MXH chưa phải là nhu cầu cao của họ.

3.3. Địa điểm và phương tiện sử dụng mạng xã hội

Học sinh, sinh viên có thể sử dụng MXH ở bất cứ nơi đâu có kết nối internet, đặc biệt khi công nghệ wifi đang ngày càng trở nên phổ biến ở khắp nơi. Tỷ lệ sử dụng MXH cao thuộc về những không gian mà ở đó sinh viên có quỹ thời gian rảnh rỗi khá nhiều như: Tại nhà chiếm tỷ lệ cao nhất (95,8%), trường học (17,3%). Hai địa điểm có tỷ lệ truy cập MXH thấp nhất là quán net (9,5%) khi mục đích của phần lớn các sinh viên đến đây để chơi game online và thư viện (2,8%). Tần suất sử dụng MXH của học sinh, sinh viên đang có xu hướng ngày càng gia tăng, bởi họ có thể truy cập mọi lúc, mọi nơi nhờ sở hữu các thiết bị công nghệ hiện đại. Học sinh, sinh viên truy cập MXH nhiều nhất thông qua điện thoại di động thông minh chiếm (85,3%). Ngoài ra, còn truy cập với các thiết bị công nghệ khác như: Máy tính xách tay (24%), máy tính để bàn (20,5%), hoặc máy tính bảng (6,8%).

3.4. Ngôn ngữ sử dụng mạng xã hội

Học sinh, sinh viên sử dụng ngôn từ trên MXH khi viết dòng trạng thái, tán gẫu, bình luận theo những cách riêng của họ đang được xem như một sự thể hiện cá tính hay sự khác biệt với những người khác trong cộng đồng mạng. Hiện nay học sinh, sinh viên thường sử dụng hoàn toàn tiếng Việt để giao tiếp trên MXH chiếm tỷ lệ cao nhất (45,7%). Tuy nhiên, cần lưu ý tiếng Việt dùng để giao tiếp trên MXH của học sinh, sinh viên hiện nay không thuần nhất như vốn tiếng Việt truyền thống mà họ đã tự “sáng tạo” cho mình một kiểu/loại ngôn ngữ riêng không theo quy chuẩn của tiếng Việt, được gọi nôm na là ngôn ngữ teen. Trong nhiều trường hợp, tiếng Việt được các bạn trẻ thay đổi từ cách viết đến cấu trúc câu, cao hơn là cố tình viết chệch âm, sai lỗi chính tả... Kết hợp tiếng Việt với ngôn ngữ khác (tiếng Anh...) chiếm tỉ lệ (38,8%), hoặc những cách viết sáng tạo, viết tắt, sử dụng tiếng lóng hoặc kết hợp nhiều loại ký hiệu khác nhau (29,7%). Ví dụ, trên MXH có thể dễ dàng bắt gặp một số xu hướng sử dụng ngôn ngữ của học sinh, sinh viên để diễn đạt lời nói, cảm nghĩ, ý tưởng... của mình như: wá (quá), wen (quen), wên (quên), u (bạn, mày), ni (nay), gato (ghen ăn tức ở)... hay diễn đạt theo xu hướng phức tạp hóa ngôn ngữ: dzui (vui), thoai (thôi), nóa (nó), đóa (đó), dzia (về), roài (rồi), khoai (khó)... hoặc cố tình viết chệch âm nhằm tạo sự vui vẻ, tình nghịch trong lời nói như: hem (không), lun (luôn), bunn (buồn), bitk? (biết không?), xienn (tiền)... Một số khác thích sử dụng các từ tiếng Anh viết tắt để diễn đạt như: lol= laugh out loud (cười lớn), tks=thanks (cảm ơn), pm=private message (nói chuyện riêng), ib = inbox (nhắn tin riêng)... Nhận định về các kiểu/loại ngôn ngữ riêng mà học sinh, sinh viên đã sáng tạo ra và sử dụng làm công cụ giao tiếp trên MXH hiện có không ít người phê phán cho rằng đó là thứ ngôn ngữ xa lạ với tiếng phổ thông, thậm chí là làm mất đi sự trong sáng, cái hay, cái đẹp của tiếng Việt, do vậy cần phải có giải pháp khắc phục tình trạng này.

4. Các mối đe dọa an ninh mạng mà học sinh, sinh viên đang phải đối mặt trong thời kỳ chuyển đổi số.

Lợi ích tích cực mà mạng Internet đưa lại là điều không ai có thể phủ nhận và chúng ta vẫn đang tận dụng điều đó hàng ngày. Tuy nhiên với quy luật vận động thì sự phát triển chóng mặt của mạng Internet cũng sẽ mang lại nhiều hệ lụy. Rõ ràng nhất hiện nay là sự gia tăng của những tin độc, tin giả, thông tin thất thiệt, sai sự thật trên mạng xã hội. Những thông tin này không chỉ ảnh hưởng tới sự phát triển, hình thành nhân cách, đạo đức xã hội; xâm phạm đến danh dự, uy tín, lợi ích kinh tế của cá nhân, tổ chức mà nó còn gây nên những tác động tiêu cực trong dư luận xã hội, gia tăng tội phạm, mất trật tự an ninh xã hội; làm giảm uy tín của Nhân dân đối với một bộ phận cán bộ, đảng viên và của Nhân dân đối với Đảng, Nhà nước và chế độ xã hội chủ nghĩa. Có thể nói mạng xã hội đang là phương tiện nguy hiểm nhất, với đặc tính lan truyền nhanh, có khả năng mở rộng phạm vi tác động, vượt qua rào cản ngôn ngữ, khoảng cách địa lý, gây tác hại trên diện rộng hơn bất cứ hình thức chống phá nào khác của các thế lực thù địch.

Theo quy định về mặt pháp luật Việt Nam, việc nhận diện thông tin tiêu cực, xấu đã được thể hiện tại Điều 5 Nghị định 72/2013/NĐCP và trong Luật An ninh mạng vừa mới được thông qua. Đó là: (a) Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; (b) Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; (c) Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp Luật quy định; (d) Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân; (đ) Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm; (e) Giả mạo tổ chức, cá nhân và phát tán thông tin giả mạo, thông tin sai sự thật xâm hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân. Từ phân tích thực trạng, đã xác định được mục đích và thời gian sử dụng của học sinh, sinh viên đó là tìm kiếm, cập nhật thông tin xã hội; làm quen với bạn mới, giữ liên lạc với bạn cũ; liên lạc với gia đình, bạn bè; tận hưởng những thú vui cuộc sống và khẳng định cái tôi bản thân, đó là chia sẻ thông tin (hình ảnh, video, status) với mọi người và để giải trí. Thời gian sử dụng MXH hàng ngày của học sinh, sinh viên thể hiện 3 khoảng thời gian chiếm tỷ lệ rất cao nằm trong khoảng từ 1-3 tiếng chiếm 35,7%; từ 3-5 tiếng chiếm 25,7%; trên 5 tiếng chiếm 22,6%. Nắm bắt được thực trạng này, các đối tượng phản động, các thế lực thù địch trong và ngoài nước xác định đối tượng dễ tiếp cận là học sinh, sinh viên để tiến hành các hoạt động phá hoại, tuyên truyền xuyên tạc, chống phá gây mất ổn định chính trị, kinh tế, xã hội. Đưa các thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, kích động bạo lực,

bôi nhọ đời tư, vu khống... Đây là những thông tin xấu, mang tính tiêu cực trên MXH cần được nghiên cứu giúp học sinh, sinh viên Việt Nam nhận diện và phòng tránh.

4.1. Nhận diện

Về nội dung và bản chất, có thể nhận diện thông tin xấu, độc tán phát trên Internet và mạng xã hội là những thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, “đổi trắng, thay đen”, làm lẫn lộn đúng sai, thật giả hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng luận điệu thù địch. Đó là các dạng thông tin có nội dung không phù hợp về chuẩn mực đạo đức, văn hóa, thuần phong mỹ tục như: kích động bạo lực, bôi nhọ đời tư, vu khống, tin đồn thất thiệt, thông tin nhảm nhí, rùng rợn...; thông tin cổ vũ, lôi kéo tham gia vào các tệ nạn xã hội như ma túy, mại dâm,.. Bên cạnh đó là những thông tin sai trái, độc hại có tính chất chính trị, phân tích và định hướng dư luận bằng luận điệu sai trái, thù địch, kích động nhân dân... Về thủ đoạn tán phát thông tin xấu, độc thì các đối tượng lợi dụng các trang mạng lớn trên thế giới như Google, Facebook, kênh Youtube làm công cụ phát tán thông tin xuyên tạc, bịa đặt. Nguồn phát chủ yếu từ một số tổ chức, cá nhân phản động ở nước ngoài hướng vào trong nước. Không chỉ tung tin xấu độc trên 3 nền tảng Facebook, YouTube, TikTok, có nhiều sự kiện với mục đích thông tin nhanh hơn nên các đối tượng sử dụng tính năng livestream.

Để phát tán thông tin xấu, độc lên không gian mạng, những tổ chức, cá nhân phản động thực hiện dưới 3 thủ đoạn.

Một là, dùng tài khoản mạo danh - lập ra những tài khoản mang tên các lãnh đạo cấp cao hoặc các cơ quan ban ngành như Ban Tuyên giáo Trung ương, VTV, Bộ Y tế, Ban Nội chính Trung ương, Bộ Công an...

Hai là, lập các tài khoản lấy tên giống như cơ quan báo chí (Tintức Vietnam, Tintức 24h, Tin Chính trị Việt nam...) hoặc các tổ chức (Nhật ký yêu nước, Con đường VN...) gây nhầm tưởng là cơ quan báo chí hoặc tổ chức yêu nước.

Ba là, dùng tài khoản chính danh như Tổ chức Việt Tân, RFA, Thoibao.de...

Đây là những thủ đoạn đã xuất hiện trên không gian mạng trong thời gian qua. Gần đây các nhóm, các đối tượng thù địch sản xuất theo mức độ, tốc độ chuyên nghiệp và nhanh chóng hơn.

Mục đích phát tán thông tin xấu, tiêu cực nhằm hướng nội dung tác động đến các đối tượng như: công nhân trong vấn đề cho phép hình thành tổ chức công đoàn độc lập: nông dân trong việc triển khai chủ trương tích tụ ruộng đất,.. Các đối tượng chống phá còn tập trung lựa chọn những nhân tố “điển hình”, “sám hối”, “trở cò”, suy thoái về tư tưởng chính trị đạo đức, lối sống, “tự diễn biến”, “tự chuyển hoá” trong nội bộ làm ngọn cò trên địa bàn để tập hợp lực lượng chống đối từ bên trong. Bên cạnh đó, đưa những thông tin sai trái, bịa đặt, bóp méo, xuyên tạc sự thật, lẫn lộn đúng sai, thật giả, hoặc có

một phần sự thật nhưng được đưa tin với dụng ý xấu, thông tin có những ngôn từ thô tục, nội dung phản cảm, soi mói, xúc phạm danh dự, nhân phẩm cá nhân, vi phạm chuẩn mực đạo đức, văn hóa, thuần phong mỹ tục; kích động đòi truy, bạo lực... được coi là thông tin xấu, độc. Hình thức phát tán thông tin xấu, độc trên MXH rất đa dạng, tinh vi. Hiện nay, ở nước ta đang đang có những thông tin được coi là xấu, độc cụ thể như sau: Thông tin chống phá nền tảng tư tưởng của Đảng và cách mạng Việt Nam, phủ định chủ nghĩa Mác – Lênin và tư tưởng Hồ Chí Minh; Xuyên tạc đường lối xây dựng CNXH, đường lối bảo vệ Tổ quốc và đường lối đối ngoại của Đảng ta, phủ nhận những thành tựu của sự nghiệp đổi mới; Lừa đảo trên mạng, đánh cắp thông tin, mật khẩu, phát tán virus...

4.2. Các biểu hiện cụ thể của các mối đe dọa an ninh mạng đối với học sinh, sinh viên xuất hiện thời gian gần đây

Thứ nhất, tổ chức lưu vong ở nước ngoài lôi kéo thực hiện chống phá Đảng và Nhà nước. Đầu tiên, tổ chức khủng bố “Chính phủ quốc gia Việt Nam lâm thời” tiền thân là tổ chức “Tân Dân Chủ”, trụ sở đặt tại 2807 Anaheim, CA 92814, Mỹ với mục đích lật đổ Nhà nước CHXHCN Việt Nam, khôi phục chế độ Việt Nam cộng hòa. Từ tháng 01/2018, Bộ Công an đã xác định tổ chức “Chính phủ quốc gia Việt Nam lâm thời” là tổ chức khủng bố. Cầm đầu là Đào Minh Quân (nguyên Trung úy Ngụy), sinh năm 1952, quê quán tại Kỳ Hương, Tam Kỳ, Quảng Nam. Hiện tại, Đào Minh Quân đang sống tại bang California, Mỹ. Ngày 06/06/2009, Đào Minh Quân công bố bản “Hiến ước lâm thời” thể hiện cương lĩnh và điều lệ hoạt động của tổ chức, với mục đích nhằm xóa bỏ vai trò lãnh đạo của Đảng Cộng sản Việt Nam, Nhà nước CHXHCN Việt Nam bằng bạo động vũ trang với khẩu hiệu hành động “lấy lại đất tổ, không làm khổ dân”. Bằng phương thức, thủ đoạn lợi dụng internet, chúng tạo lập, duy trì các trang web, blog, địa chỉ email như “chinhphuquocgia.com”, “cuutuchinhtri.org”... để tuyên truyền, lôi kéo, phát triển lực lượng, chỉ đạo thực hiện các hoạt động chống phá Nhà nước Việt Nam dưới nhiều hình thức như hoạt động khủng bố, phá hoại tư tưởng, rải truyền đơn kích động biểu tình, phá hoại nhân dịp các ngày lễ, Tết của đất nước. Bên cạnh đó, tổ chức “Triều đại Việt” (hay “Triều đại Việt Nguyễn”) có trụ sở chính tại Canada, do đối tượng Ngô Văn Hoàng Hùng cùng với các đối tượng Trần Thanh Đình, Ngô Cường, Trần Công Tuấn, Huỳnh Thanh Hoàng, Lê Thái Hoàng và Nguyễn Thanh Long nguyên là thành viên cốt cán của tổ chức khủng bố “Chính phủ quốc gia Việt Nam lâm thời”, Các đối tượng chủ trương hoạt động bạo động vũ trang, lật đổ Đảng và Nhà nước ta với phương châm “đốt sạch”, “giết sạch”, “phá sạch”, “cướp sạch” và lấy cớ ngũ sắc làm quốc kỳ. Thực hiện âm mưu chống phá Việt Nam, Ngô Văn Hoàng Hùng cùng các đối tượng lên MXH Facebook, Youtube đăng tải gần 200 video, clip dưới hình thức livestream với nội dung xuyên tạc lịch sử, xuyên tạc Nhà nước Việt Nam, kêu gọi người

dân đứng lên đấu tranh bạo động, lật đổ chế độ, ủng hộ “Triều Đại Việt” về lãnh đạo đất nước. Thứ hai, lợi dụng vấn đề ô nhiễm môi trường biển tại các tỉnh miền Trung năm 2016. Các đối tượng phản động đã đăng tải các video, hình ảnh không đúng sự thật lên MXH, dưới sự chỉ đạo của các tổ chức phản động, đối tượng cực đoan nhằm xuyên tạc, bôi nhọ lãnh đạo Đảng, Nhà nước Việt Nam mà còn tích cực khoét sâu và thổi phồng các vấn đề nóng như sự cố môi trường, lũ lụt trên địa bàn Hà Tĩnh, Nghệ An, Quảng Bình để kích động nhân dân, làm giảm sự uy tín của Đảng, Nhà nước, hòng làm suy giảm khối đại đoàn kết toàn dân, bóp méo sự thật, bàn về vấn đề nhân quyền ở nước ta. Sau khi cơ quan chức năng khởi tố vụ án hình sự để xử lý các đối tượng cầm đầu thì xuất hiện một số trang MXH ở nước ngoài đã đăng tin Việt Nam vi phạm quyền tự do tôn giáo, vi phạm tự do dân quyền và còn cho rằng Việt Nam đàn áp tôn giáo. Trường hợp điển hình: Những kẻ có mưu đồ xấu đã kích động, tụ tập giáo dân ở các tỉnh Nghệ An, Hà Tĩnh tuần hành, gây rối trật tự công cộng khiến dư luận bất bình. Cụ thể, ngày 10/2/2017, linh mục Nguyễn Đình Thục-Quản xứ Song Ngọc (xã Quỳnh Ngọc, huyện Quỳnh Lưu, Nghệ An) soạn thảo “thư ngỏ” kêu gọi các linh mục và cộng đoàn các Giáo xứ Hiệp Thông, cầu nguyện cho giáo dân Giáo xứ Song Ngọc đi gửi đơn khởi kiện Công ty TNHH Hưng Nghiệp Formosa tại Tòa án Nhân dân Thị xã Kỳ Anh (tỉnh Hà Tĩnh) vào ngày 14/2. Trong quá trình tập kết vào bãi đất trống, linh mục Thục đã chỉ đạo dừng xe ô tô 7 chỗ ngồi ngay giữa quốc lộ 1A. Khi xe dừng, các đối tượng ngồi trong xe không chịu mở cửa buộc lực lượng CSGT phải cầu xe và người ngồi trên xe để giải phóng ách tắc giao thông. Cũng trong năm 2017, Linh mục Đặng Hữu Nam xuyên tạc lịch sử, kích động trẻ em ra đường. Tối 30/4, trong bài rao giảng tại nhà thờ, Đặng Hữu Nam đã có những lời lẽ kích động, bóp méo sự thật về ngày 30/4/1975, chia rẽ mỗi đoàn kết dân tộc. Một vụ việc khác, kích động 2.000 người bao vây trụ sở UBND huyện. Khoảng 8h ngày 3/4/2017, có khoảng 2.000 người dân (chủ yếu là Giáo dân ở xã Thạch Bàng và xã Thạch Kim, huyện Lộc Hà, Hà Tĩnh) do Bạch Hồng Quyền cầm đầu, kích động mang theo băng rôn, khẩu hiệu kéo đến UBND huyện Lộc Hà để khiếu nại, đòi bồi thường thiệt hại sự cố môi trường biển. Thứ ba, bóp méo, xuyên tạc các vụ án hình sự khởi tố và xử lý kịp thời, đúng người, đúng tội các vụ án hình sự là trách nhiệm của cơ quan pháp luật. Điều này có ý nghĩa rất quan trọng đối với công tác đấu tranh phòng, chống tội phạm, đảm bảo an ninh trật tự xã hội, mang lại sự bình yên cho nhân dân ở bất kỳ quốc gia nào. Tuy nhiên, có những phần tử cơ hội, bất mãn chính trị đã lợi dụng những vụ án mà trắng đen đã rõ mười mươi, để thực hiện những thủ đoạn đơm đặt, dựng chuyện, cố tình làm sai lệch bản chất sự việc. Mục đích là nhằm hạ uy tín của các cơ quan công quyền, cơ quan thực thi pháp luật, gây nhiễu thông tin, lèo lái dư luận ngả theo quan điểm sai trái, bất mãn.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Hay ngay cả trong trường học, các trường học phổ thông có thể không phải là mục tiêu đầu tiên xuất hiện trong đầu khi bạn nghĩ đến các cuộc tấn công mạng, nhưng đối với các bằng đảng mạng, trường học có thể là một mỏ vàng.

Thứ nhất, các trường học phổ thông chứa một lượng lớn dữ liệu nhạy cảm. Thông thường, tên, địa chỉ, ngày sinh và số an sinh xã hội của học sinh và cán bộ nhà trường có thể được tìm thấy trong cơ sở dữ liệu của trường học. Kẻ tấn công có thể đánh cắp dữ liệu và bán nó trên web đen (dark web) hoặc mã hóa nó, yêu cầu học khu một khoản tiền chuộc cắt cổ để lấy lại quyền truy cập.

Ngoài ra, hầu hết các trường học ngày càng phụ thuộc rất nhiều vào công nghệ và mạng để vận hành các hệ thống hoạt động hàng ngày. Việc chuyển sang học từ xa trong thời kỳ đại dịch cũng thúc đẩy sự phụ thuộc vào học tập trên môi trường số. Các giáo viên và học sinh, nhiều người hiện được trang bị các thiết bị 1:1, đang tận dụng các công cụ và tài nguyên học tập trực tuyến để nâng cao hướng dẫn, hoàn thành bài đánh giá và giao tiếp bên ngoài lớp học. Tin tặc nhận thức được sự phụ thuộc ngày càng tăng này và đang khai thác các lỗ hổng mạng để làm ngừng các hoạt động học khu cũng như việc học tập.

Hơn nữa, nhiều trường học đang phải đối mặt với tình trạng thiếu nhân lực và cạnh tranh việc làm với hoạt động kinh doanh của doanh nghiệp. Các chuyên gia an ninh mạng đóng một vai trò quan trọng trong việc đảm bảo rằng cơ sở hạ tầng mạng quan trọng và đảm bảo an toàn cho các hệ thống thông tin phức tạp. Nhưng với 30% lực lượng lao động hiện tại có kế hoạch chuyển đổi nghề nghiệp thì tương lai của an ninh mạng trong các trường học vẫn đang ở mức cân bằng.

Và đặc biệt, nắm được điểm yếu của lứa tuổi học sinh, sinh viên là ở độ tuổi muốn đi làm, muốn tự lập hay là muốn khám phá, họ sẽ gửi những link qua gmail, Facebook, Instagram,.. đầy đủ các nền tảng để chiêu dụ mọi người bấm vào link hay đăng kí một thứ gì đó, điều đó có thể làm mất đi tài khoản mà chính bản thân các bạn đang dùng. Hoặc là, chính con người với con người cũng đã lừa nhau qua an ninh mạng như việc lừa đảo những sinh viên đang muốn tìm kiếm một suất dạy gia sư, hay là đánh văn bản, làm content,.. nhưng không trả lương cho các bạn.

5. Giải pháp

Để phòng, chống các mối đe dọa trên mạng xã hội cần thực hiện tốt một số giải pháp sau:

- Đẩy mạnh tuyên truyền, giáo dục, định hướng nâng cao nhận thức cho cán bộ, đảng viên, nhân dân về những thông tin xấu độc trên mạng xã hội; khuyến khích xây dựng môi trường văn hoá lành mạnh trong cơ quan, đơn vị, trường học, tổ chức, doanh nghiệp để dần hình thành “miền dịch tâm lý” đối với tin đồn trong nhân dân bằng một nền tảng tri thức đủ sức đề kháng với mọi loại tin đồn độc hại, thất thiệt, sai sự thật.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Tăng cường sự lãnh đạo của cấp ủy đảng, vai trò của đội ngũ cán bộ, đảng viên các cấp trong phòng, chống thông tin xấu độc trên mạng xã hội; Các bộ, ban, ngành cần phối hợp chặt chẽ, thống nhất, đồng bộ trong việc quản lý Internet; Tăng cường kiểm tra, giám sát, xử phạt nghiêm khắc các sai phạm trên mạng xã hội.

- Các cơ quan quản lý Nhà nước cần đẩy mạnh việc xây dựng, triển khai và hoàn thiện cơ sở dữ liệu, sử dụng chứng minh thư nhân dân điện tử để quản lý thông tin và người sử dụng trên Internet.

- Các cơ quan báo chí, phát thanh, truyền hình Trung ương, các địa phương, người đứng đầu cơ quan, đơn vị, địa phương cần cung cấp thông tin chính thống một cách đầy đủ, toàn diện, kịp thời cho người dân. Đồng thời, cần tăng cường tuyên truyền pháp luật, cảnh báo các hành vi vi phạm pháp luật; chỉ rõ những thủ đoạn, nội dung thông tin giả mạo, tính chất nguy hại của nó đối với cá nhân và xã hội. Qua đó, giúp người dùng am hiểu pháp luật, tránh những hành vi vi phạm cũng như nhận diện các thủ đoạn, nội dung thông tin giả mạo, biết tự sàng lọc, tiếp nhận thông tin hữu ích, chính thống, “miễn dịch” với những thông tin giả mạo làm nhiễu loạn môi trường xã hội.

- Đặc biệt, với mỗi người dân, nhất là giới trẻ cần tự trang bị cho mình vốn hiểu biết và những kỹ năng cần thiết trong việc chọn lọc, nhận diện thông tin; kỹ năng công nghệ-thông tin để chặn, lọc, xóa, báo xấu,...các thông tin độc hại khi phát hiện, không để thông tin đó lan truyền; nắm vững và tuân thủ các quy định pháp luật và quy tắc ứng xử văn hóa trên môi trường mạng xã hội; rèn luyện tư duy biện chứng, tư duy phản biện khi tiếp xúc với các thông tin trên mạng xã hội để xem xét sự vật, hiện tượng một cách khách quan đa chiều, nhìn thấu được bản chất ẩn giấu sau hiện tượng bề ngoài, mục đích sâu sa ẩn đằng sau những ngôn ngữ, hình ảnh; thường xuyên cập nhật kiến thức xã hội để nâng cao “sức đề kháng” trước những thông tin xấu, độc, sai trái, không dễ bị mắc lừa, dụ dỗ. Mỗi người dân phải cảnh giác và sẵn sàng tham gia đấu tranh với những thông tin sai trái, nhận thức không đúng, ngộ nhận, mơ hồ trước các thông tin sai trái, thù địch, trái với quan điểm, đường lối của Đảng, chính sách và pháp luật của Nhà nước, không vô tình tiếp tay cho hành vi sai trái; phát hiện, tố giác các thông tin độc, hại với cơ quan chức năng.

Đặc biệt hơn là, đối với học sinh, sinh viên cần chú ý những điều sau:

Một là, đối với bản thân học sinh, sinh viên cần phải xác định mục tiêu đúng đắn khi tiếp cận MXH. Phải chắc chắn rằng hành động này nhằm mang lại sự hiểu biết tri thức, hỗ trợ tích cực cho việc học tập, làm việc và vui chơi một cách tích cực. Luôn chủ động nâng cao kiến thức xã hội về mọi mặt nhằm xây dựng cho mình nhận thức chính trị đúng đắn để xem xét, tiếp cận thông tin một cách khách quan, đầy đủ, chính xác từ những nguồn thông tin chính thống, tránh tiếp cận thông tin phiến diện, một chiều. Nâng cao tinh thần cảnh giác, sẵn sàng tham gia đấu tranh với những nhận thức không đúng, ngộ nhận, mơ hồ trước các nguồn thông tin sai trái, thù địch với quan điểm, đường lối của Đảng, chính sách

và pháp luật của Nhà nước. Học sinh, sinh viên phải có ý thức tự giác, kỷ luật trong quá trình tiếp xúc thông tin; chấp hành tốt các quy định về quyền thông tin, phạm vi thông tin của công dân theo quy định của Hiến pháp năm 2013, Luật Tiếp cận thông tin năm 2016 và Luật An ninh mạng vừa mới được Quốc hội thông qua. Đồng thời tích cực tham gia vạch trần, cảnh báo đến người dùng MXH những biểu hiện xáo trộn thông tin, lưu truyền thông tin xấu, độc, thông tin thất thiệt.

Hai là, đối với nhà trường cần tăng cường giáo dục nâng cao nhận thức, trách nhiệm, bản lĩnh chính trị cho học sinh, sinh viên. Chú trọng giáo dục Chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, đường lối của Đảng, chính sách và pháp luật của Nhà nước, làm rõ âm mưu, thủ đoạn mới của các thế lực thù địch, của các đối tượng xấu trên MXH. Đề cập những vấn đề, sự kiện mà chúng lợi dụng xuyên tạc, mức độ nguy hại, ảnh hưởng của các thông tin xấu, độc. Phổ biến các quy định của pháp luật đến học sinh, sinh viên về tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông tại Điều 288 của Bộ luật Hình sự 2015; Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ và Thông tư số 09/2014/BTTTT ngày 19/8/2014 của Bộ Thông tin và Truyền thông về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và MXH, những hành vi bị nghiêm cấm trong sử dụng MXH. Đồng thời nhà trường phải có trách nhiệm trong quản lý thông tin có liên quan tới học sinh, sinh viên trên MXH. Yêu cầu học sinh, sinh viên lên tiếng khi tài khoản cá nhân (Facebook, Zalo...) bị hack hoặc bị giả mạo, để tránh bị lừa đảo, chiếm đoạt tài sản, bôi nhọ, vu khống, hoặc bị lợi dụng phát tán thông tin xấu, độc cho người thân, bạn bè và cộng đồng mạng.

Không thể phủ nhận mạng xã hội là một thành tựu khoa học - công nghệ của nhân loại, tạo thêm không gian để chia sẻ, trao đổi thông tin và kết nối, hợp tác trên phạm vi toàn cầu, là kênh thông tin quan trọng và hữu ích. Tuy nhiên, trước sự phát triển nhanh chóng của mạng xã hội, chúng ta cần phải nhận diện đúng những thông tin xấu, độc khi tiếp cận nhằm phát huy những mặt tích cực, ngăn ngừa những tác động tiêu cực, góp phần ổn định chính trị xã hội của đất nước và xây dựng một môi trường sống an toàn và nâng cao chất lượng cuộc sống của mỗi chúng ta.

6. Kết luận

Sinh viên là những người trẻ, năng động nên việc họ sử dụng MXH là điều tất yếu. Không thể phủ nhận những lợi ích của MXH khi giúp sinh viên tăng cường các mối quan hệ, tăng cường tri thức hiểu biết, cung cấp nguồn giải trí lớn cho người sử dụng. Mặc dù vậy, với những kết quả trình bày ở trên, cho thấy rằng cần có sự định hướng cho sinh viên trong việc sử dụng MXH liên quan đến thời gian, mục đích sử dụng, cũng như những cách thức bảo vệ bản thân khi tham gia vào cộng đồng mạng. Việc sinh viên (trong nghiên cứu này) đã sử dụng MXH cho những mối tương tác xã hội và giải trí cá nhân vượt mức cho phép (mức chuẩn). Điều này đặt ra những câu hỏi cho các nghiên

cứu tiếp theo: Phải chăng sinh viên hiện nay có xu hướng chú trọng đến việc duy trì các mối quan hệ của bản thân thông qua MXH hơn là bằng con đường giao tiếp trực tiếp ngoài đời thực? Những tương tác trên MXH có giúp sinh viên giảm bớt sự căng thẳng từ việc bị chối bỏ hay thất bại trong những mối quan hệ trong thế giới thực? Liệu có phải những sân chơi phục vụ cho việc giải trí, thư giãn của sinh viên còn quá ít nên họ tìm đến MXH để hiện thực hóa nhu cầu của bản thân?

Có thể nói, MXH kết nối con người trên toàn thế giới, rút ngắn không gian, thời gian và thúc đẩy sự giao lưu hợp tác quốc tế. Những giá trị tích cực của MXH mang lại là không hề nhỏ đó là: (1) Là một trong những cách tốt nhất để giới thiệu bản thân đến tất cả mọi người, bày tỏ cảm xúc của bản thân, chia sẻ quan điểm cá nhân, gắn kết cộng đồng giúp thích nghi tốt hơn với sự thay đổi và vượt qua những áp lực và căng thẳng trong cuộc sống, tìm kiếm những cơ hội phát triển khả năng của mình, gặp gỡ và giao lưu với tất cả mọi người trên thế giới. Là kho thông tin phong phú giúp cho cá nhân dần cải thiện kỹ năng sống và trau dồi kiến thức và là kênh giải trí hữu hiệu.

MXH còn là một môi trường kinh doanh lí tưởng, đầy tiềm năng, giúp người sử dụng bán hàng online hay quảng cáo những sản phẩm của công ty, doanh nghiệp và tìm kiếm khách hàng tiềm năng. Bên cạnh những giá trị tích cực thì MXH được ví như con dao hai lưỡi ẩn chứa nhiều vấn đề bất cập và hiểm họa khó lường đối với người sử dụng không đúng mục đích như sau: Thông tin xấu độc tán phát trên MXH là những thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, “đổi trắng, thay đen”, làm lẫn lộn đúng sai, thật giả; hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng luận điệu sai trái, thù địch. Xuyên tạc sự thật lịch sử, phủ nhận Chủ nghĩa Mác - Lê-nin, tư tưởng Hồ Chí Minh, chống phá đường lối, chủ trương, chính sách của Đảng, Nhà nước, phủ nhận thành tựu của công cuộc đổi mới, bịa đặt, vu cáo, nói xấu các đồng chí lãnh đạo cấp cao của Đảng, Nhà nước, gây chia rẽ đoàn kết nội bộ, tìm mọi cách thúc đẩy “tự diễn biến”, “tự chuyển hóa” nội bộ ta trên mọi lĩnh vực.. Trước những ưu điểm và hạn chế của MXH, học sinh, sinh viên trong giai đoạn hiện nay cần chủ động trong việc nhận diện và phòng tránh những thông tin xấu độc trên MXH để từ đó phát huy những mặt tích cực trong học tập, nghiên cứu và nhu cầu giải trí của bản thân. Chủ động trước những hạn chế của MXH để tránh được sự lợi dụng của các lực lượng phản động trong thời kỳ bùng nổ công nghệ số.

Là một sinh viên, em cũng hiểu rõ tầm quan trọng của MXH nhưng em may mắn dùng nó với những mục đích chính đáng, không sao nhãng trong tập cũng như không bị động trước các trang mạng MXH hay không dùng nó để làm vui cho chính bản thân mà dùng những câu từ thô thiển, hành động tiêu cực đến mọi người xung quanh. Mong rằng, sau bài tham luận này, các bạn học sinh, sinh viên hãy trang bị cho mình một hành trang cũng như bản lĩnh để có thể đối mặt với những mối đe dọa và những ai đã và đang sử

dụng an ninh mạng một cách không chính đáng, theo hướng tiêu cực thì hãy suy nghĩ về những việc mình làm và quay đầu lại khi còn có thể nhé!

TÀI LIỆU THAM KHẢO

<https://antoanthongtin.vn/chinh-sach---chien-luoc/cac-moi-de-doa-an-ninh-mang-hang-dau-nam-2023-108626>

<https://www.studocu.com/vn/document/truong-dai-hoc-ngoai-thuong/phat-trien-kinh-nang/nguyen-cuu-khoa-hoc-nckh/30618275>

<https://jst.iuh.edu.vn/index.php/jst-iuh/article/view/1342/455>

Luật An ninh mạng năm 2018, Điều 8 (Các hành vi bị nghiêm cấm về an ninh mạng);

Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng

Thông tư số 09/2014/BTTTT ngày 19/8/2014 của Bộ Thông tin và Truyền thông quy định chi tiết về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội.

CHUYỂN ĐỔI SỐ TẠI TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN

Trần Anh Thành

Trường Đại học An ninh nhân dân

Email: tatthanh1998kg@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> chuyển đổi số, Đại học An ninh nhân dân, quản lý giáo dục.	Ngày nay, với sự thay đổi nhanh chóng của công nghệ thông tin và truyền thông, thời đại của kỹ thuật số với sự toàn cầu hóa đã ảnh hưởng đến hầu hết tất cả các lĩnh vực và lĩnh vực giáo dục cũng không ngoại lệ. Việc áp dụng công nghệ vào giáo dục có vai trò vô cùng to lớn, nó tạo ra một bước ngoặt lớn cho giáo dục, tạo ra nhiều phương thức giáo dục mới, thông minh hơn, hiệu quả hơn, tiết kiệm chi phí hơn. Ngày 25/01/2022, Thủ tướng Chính phủ ban hành quyết định số 131/QĐ-TTg về việc phê duyệt Đề án 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 đó xác định rõ mục tiêu chung là tận dụng tiến bộ của công nghệ để thúc đẩy đổi mới sáng tạo trong dạy và học, xây dựng nền giáo dục mở thích ứng trên nền tảng số, góp phần phát triển Chính phủ số, kinh tế số và xã hội số. Chuyển đổi số trong giáo dục đã là một khái niệm phổ biến trong cuộc sống hiện nay, bài viết phân tích một số nội dung cơ bản của chuyển đổi số trong trường Đại học An ninh nhân dân, các yếu tố đảm bảo chuyển đổi số thành công, thực trạng hiện nay, kết quả đạt được và tồn tại, khó khăn, từ đó đề xuất một số giải pháp định hướng trong giai đoạn tới.

1. Đặt vấn đề

Chúng ta đang sống trong thời đại thông tin, với sự biến đổi đa chiều trong cấu trúc của cá nhân và xã hội. Nguồn tri thức đã được đổi chủ, các hoạt động dạy và học bắt đầu phân biệt với các phương pháp tiếp cận truyền thống. Có thể nói, những thay đổi diễn ra trong thời đại thông tin dưới tác động của toàn cầu hóa và công nghệ, đòi hỏi phải có những thay đổi và cải tiến trong hệ thống, phương pháp tiếp cận và cả quy trình giáo dục. Các phương thức giáo dục từ xa, giáo dục có sự hỗ trợ của máy tính, học trực tuyến (e-

learning), môi trường học tập ảo... có thể chỉ ra những khía cạnh mới của giáo dục trong việc phát triển công nghệ thông tin.

Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số. Chuyển đổi số không chỉ giúp tăng năng suất, giảm chi phí mà còn mở ra không gian phát triển mới, tạo ra các giá trị mới ngoài các giá trị truyền thống vốn có. Đối với lĩnh vực giáo dục và đào tạo, việc phát huy trong chuyển đổi số để thúc đẩy năng lực học tập, tăng khả năng tự học, tạo ra các phương thức học mới, hiệu quả, tiết kiệm, thuận tiện là đóng góp thiết thực của công nghệ thông tin và chuyển đổi số. Sự phát triển không ngừng của internet và các thiết bị công nghệ số đã mở ra cơ hội tiếp cận thông tin, kiến thức đa dạng, dễ dàng, nhanh chóng, ở mọi lúc, mọi nơi trong môi trường số; cá nhân hóa việc học, góp phần tạo ra xã hội học tập và học tập suốt đời.

Tại Việt Nam, Nghị quyết số 52-NQ/TW của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc Cách mạng công nghiệp lần thứ tư đã khẳng định: “Đổi mới cách dạy và học trên cơ sở áp dụng công nghệ số... Khuyến khích các mô hình giáo dục, đào tạo mới dựa trên các nền tảng số”. Văn kiện Đại hội lần thứ XIII của Đảng ta nêu rõ “Thực hiện chuyển đổi số quốc gia một cách toàn diện để phát triển kinh tế số, xây dựng xã hội số. Phấn đấu đến năm 2030, hoàn thành xây dựng chính phủ số”. Quán triệt thực hiện Nghị quyết Đại hội lần thứ XIII của Đảng, Thủ tướng Chính phủ phê duyệt chương trình “Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”, với mục tiêu Việt Nam gia nhập nhóm 50 nước dẫn đầu về Chính phủ điện tử (EGDI). Riêng về lĩnh vực giáo dục và đào tạo, chuyển đổi số tập trung “phát triển nền tảng hỗ trợ dạy và học từ xa, ứng dụng triệt để công nghệ số trong công tác quản lý, giảng dạy và học tập; số hóa tài liệu, giáo trình; xây dựng nền tảng chia sẻ tài nguyên giảng dạy và học tập theo cả hình thức trực tiếp và trực tuyến...”. Chuyển đổi số trong giáo dục, có thể hiểu đơn giản là việc áp dụng công nghệ kỹ thuật tiên bộ vào mục đích đào tạo và giảng dạy giúp nâng cao trải nghiệm của người học; cải thiện phương pháp giảng dạy, tạo môi trường học tập thuận tiện nhất. Trong đó có ba hình thức áp dụng chính là Chuyển đổi số trong các cơ sở giáo dục tại trường Đại học An ninh nhân dân nên tập trung vào ba nội dung chủ đạo là chuyển đổi số trong quản lý điều hành, quản lý giáo dục và chuyển đổi số trong dạy, học, kiểm tra, đánh giá, nghiên cứu khoa học.

Trước bối cảnh đó, Trường Đại học An ninh nhân dân đã chủ động thay đổi tư duy, nhận thức về tính tất yếu của chuyển đổi số, đáp ứng yêu cầu, nhiệm vụ của Nhà trường trong thời kỳ mới, thời kỳ bùng nổ công nghệ thông tin, đẩy mạnh công nghiệp hóa, hiện đại hóa đất nước và hội nhập quốc tế sâu rộng; không chần chừ, do dự, quyết liệt nắm bắt những thời cơ, vận hội mới để xử lý các yêu cầu, nhiệm vụ đặt ra trong công tác giáo dục đào tạo của Nhà trường nhằm đem lại sự đổi thay, khác lạ, một diện mạo

mới cho Trường Đại học An ninh nhân dân trong thời đại cuộc cách mạng Công nghiệp lần thứ 4.

2. Nội dung nghiên cứu

2.1. Phương pháp nghiên cứu

Bài viết sử dụng phương pháp thu thập, phân tích và xử lý dữ liệu đã được công bố. Bài viết còn sử dụng phương pháp nghiên cứu lý luận, nghiên cứu các văn bản, tài liệu về các khái niệm công cụ, về hoạt động chuyển đổi số đối với giáo dục tại trường Đại học An ninh nhân dân đáp ứng yêu cầu hội nhập và mở rộng hợp tác quốc tế để xây dựng khung lý thuyết cơ bản, làm nền tảng để tiến hành khảo sát đánh giá đúng thực trạng và đề xuất giải pháp hoàn thiện. Sử dụng phương pháp nghiên cứu thực tiễn, phân tích văn bản để tìm ra hạn chế và nguyên nhân của những hạn chế đó, qua đó làm cơ sở đề xuất các biện pháp quản lý theo đặc thù giáo dục tại trường.

2.2. Chuyển đổi số tại trường Đại học An ninh nhân dân đáp ứng yêu cầu hội nhập và mở rộng hợp tác quốc tế

Trường Đại học An ninh nhân dân là cơ sở đào tạo trình độ đại học và sau đại học có uy tín của ngành Công an. Với 60 năm từ khi thành lập, Nhà trường luôn quan tâm đào tạo, bồi dưỡng, phát triển đội ngũ cán bộ, giảng viên, xem đây là yếu tố then chốt, quyết định đến sự phát triển của Nhà trường nói chung, đến công tác giáo dục - đào tạo nói riêng. Tiếp nối truyền thống đó, nhiệm kỳ 2020 - 2025, Đảng ủy Trường Đại học An ninh nhân dân đã xây dựng và ban hành Nghị quyết số 11-NQ/ĐU ngày 1/7/2021 về lãnh đạo công tác giáo dục, đào tạo giai đoạn 2021 - 2025 và tầm nhìn 2030; Nghị quyết số 12-NQ/ĐU ngày 1/7/2021 về lãnh đạo công tác nghiên cứu, phát triển khoa học và công nghệ tại Trường Đại học An ninh nhân dân giai đoạn 2021 - 2025 và tầm nhìn 2030 với nhiều quyết nghị quan trọng về công tác đào tạo, bồi dưỡng đội ngũ giảng viên. Từ chủ trương của Đảng ủy, Nhà trường đã xây dựng và ban hành Kế hoạch Nghiên cứu, xây dựng Đề án “Xây dựng Trường Đại học An ninh nhân dân đến 2030 cách mạng, chính quy, tinh nhuệ, hiện đại” mà một nội dung quan trọng là xây dựng đội ngũ giảng viên “cách mạng, chính quy, tinh nhuệ, hiện đại”. Đây là cơ sở cho toàn thể giảng viên Nhà trường đoàn kết, quyết tâm thi đua phấn đấu, rèn luyện để trở thành giảng viên Công an nhân dân vừa “hồng”, vừa “chuyên” theo lời dạy của Chủ tịch Hồ Chí Minh vĩ đại. Hiện nay, đội ngũ cán bộ, giảng viên của Nhà trường đã đạt chuẩn 100% đồng chí có trình độ đại học và trên đại học. Với sứ mạng đào tạo nguồn nhân lực chất lượng cao, trung tâm nghiên cứu khoa học, tham mưu chiến lược có uy tín cao, lực lượng dự bị, sẵn sàng chiến đấu của lực lượng Công an, Trường Đại học An ninh nhân dân xác định tầm nhìn đến 2030, xây dựng Nhà trường “cách mạng, chính quy, tinh nhuệ, hiện đại và hội nhập”.

Ngày nay, với thời đại công nghệ 4.0, chuyển đổi số trong giáo dục chính là xu hướng tất yếu của xã hội. Ứng dụng chuyển đổi số sẽ tạo ra mô hình giáo dục thông minh, giúp người học dễ dàng tiếp thu kiến thức hơn, chủ động về thời gian cũng như

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

không gian, hỗ trợ đắc lực trong việc cá nhân hóa trong học tập. Sự bùng nổ của nền tảng công nghệ IoT, Big Data, AI, SMAC (Social - Xã hội, Mobile - Di động, Analytics - Phân tích, dựa trên Dữ liệu lớn và Cloud - Đám mây) đang hình thành hạ tầng giáo dục số. Theo đó, nhiều mô hình giáo dục thông minh đang được phát triển trên nền tảng ứng dụng công nghệ thông tin. Chuyển đổi số trong giáo dục tập trung vào hai nội dung chính là chuyển đổi số trong quản lý giáo dục và chuyển đổi số trong dạy, học, đánh giá, nghiên cứu khoa học.

Trong bối cảnh cuộc cách mạng công nghiệp lần thứ tư, vấn đề có tính chất then chốt, tạo sức bật, tiền đề hiện đại hóa từng khâu, mũi, bộ phận, nhằm tiến đến hiện đại hóa toàn diện cả hệ thống chính là “chuyển đổi số” (Digital Transformation). Nếu đạt hiệu quả, chuyển đổi số sẽ tối ưu hóa cách vận hành Trường Đại học An ninh nhân dân, tăng hiệu quả hợp tác giữa các bộ phận, tổ chức, cá nhân cấu thành, gia tăng năng suất lao động, cùng với đó là gia tăng giá trị phục vụ xã hội.

Bước căn bản đầu tiên của chuyển đổi số, đòi hỏi quyết tâm cao độ trong chỉ đạo và điều hành, chính là “số hóa” (Digitization) - chuyển mọi thông tin điều hành, quản lý, tổ chức, hoạt động của Nhà trường sang dạng kỹ thuật số. Bước này đã và đang thực hiện có hiệu quả tại Trường với việc đưa vào sử dụng phần mềm quản lý đào tạo từ tháng 01/2018 và hệ thống Văn phòng điện tử (E-Office) từ tháng 11/2019.

Thời gian tới, Nhà trường tiếp tục quan tâm, chỉ đạo quyết liệt đến từng đơn vị trong toàn Trường thực hiện đúng, đầy đủ nội dung được phân công và lộ trình đã đặt ra của Đề án 1646/ĐA-T47 ngày 12/12/2016 về “Tin học hóa và cải cách thủ tục hành chính” và Đề án 2121/ĐA-T47 ngày 14/11/2017 về “Nhà trường điện tử”, coi đây là vấn đề then chốt, quyết định đến sự phát triển, hội nhập của Nhà trường trong tương lai. Hệ thống tài nguyên thông tin của Trường đang từng bước hình thành, tuy nhiên dữ liệu các bộ phận cấu thành còn rời rạc, cần đầu tư có lộ trình để Big Data xuất hiện và có thể khai thác. Để thực hiện được vấn đề này, chủ động nghiên cứu, nâng cấp hệ thống mạng LAN của Nhà trường có đường truyền mạnh, đáng tin cậy, bảo mật, kết nối và mạng nội bộ Bộ Công an. Tiếp tục kiến nghị Bộ Công an đầu tư kinh phí cho một số hạng mục, đặc biệt là đầu tư hạ tầng công nghệ thông tin, đảm bảo thiết thực, hiệu quả, tiết kiệm, chú trọng việc đảm bảo nguồn kinh phí xây dựng và triển khai 04 phần mềm còn lại trong 06 bộ phần mềm, gồm: Phần mềm quản lý khoa học và tạp chí; phần mềm quản lý thư viện điện tử và xuất bản số; phần mềm quản lý tổ chức nhân sự; phần mềm quản lý hậu cần, tài chính, nhà ăn.

Chuyển đổi số đã không còn là vấn đề “nên có” hay “cần có” tại Trường Đại học An ninh nhân dân trong thời đại kỹ thuật số mà đó là quy luật tất yếu, buộc phải thực hiện để phát triển. Với tinh thần đổi mới, sáng tạo và phát triển, tin tưởng rằng Trường Đại học An ninh nhân dân sẽ viết tiếp trang sử hào hùng của một tập thể đã trải qua

muôn vản thử thách trong cả thời chiến lẫn thời bình, xứng đáng với truyền thống Anh hùng để vững bước tiến lên là nơi tổ chức các hoạt động giáo dục đào tạo cho các hệ đại học, thạc sĩ và tiến sĩ nhằm trang bị trình độ học vấn, năng lực chuyên môn nghiệp vụ; phẩm chất chính trị, đạo đức, ý thức phục vụ nhân dân để cung cấp nguồn nhân lực cho ngành Công an, đáp ứng yêu cầu xây dựng lực lượng Công an Nhân dân thật sự trong sạch, vững mạnh, chính quy, tinh nhuệ, hiện đại, đáp ứng yêu cầu, nhiệm vụ trong tình hình mới.

3. Điều kiện chuyển đổi số trong trường Đại học An ninh nhân dân để phù hợp với thực tiễn hiện nay

Trường Đại học An ninh nhân dân với bề dày truyền thống hướng đến mục đích đào tạo đội ngũ sĩ quan nghiệp vụ có chất lượng cao phục vụ sự nghiệp bảo vệ an ninh, trật tự, đảm bảo an ninh quốc phòng cho đất nước - nguồn nhân lực số đủ khả năng đối đầu với những vấn đề cấp bách trong giai đoạn cách mạng công nghiệp đang diễn ra mạnh mẽ. Vì vậy, để đảm bảo thành công chuyển đổi số, trước tiên cần phải tuyên truyền, thống nhất, thông suốt về nhận thức trong toàn lực lượng đến từng cán bộ, giảng viên, công nhân viên và học viên. Mỗi cá nhân luôn phải có ý thức và nhận thức đây là “nhiệm vụ chính trị mang tính cấp thiết” trong thời gian tới. Nhận định chuyển đổi số là xu thế tất yếu của ngành và toàn xã hội, nó diễn ra với tốc độ rất nhanh, do đó cần có sự chuẩn bị, đầu tư xứng tầm, tạo sức mạnh cộng hưởng và quyết tâm cao.

Các cấp lãnh đạo cần tạo cơ chế, chính sách, hành lang pháp lý phải được hoàn thiện, tạo tiền đề thuận lợi cho chuyển đổi số trong các cơ sở giáo dục Công an Nhân dân. Đó là các chính sách liên quan đến học liệu như sở hữu trí tuệ, bản quyền tác giả; liên quan đến chất lượng việc dạy học trên môi trường mạng (nội bộ và Internet) như an toàn thông tin mạng; liên quan đến chính trị, tư tưởng, đạo đức người dạy, người học như bảo vệ thông tin cá nhân, an ninh thông tin; các quy định liên quan đến điều kiện tổ chức dạy - học trên mạng, khảo thí và kiểm định chất lượng, tính pháp lý và công nhận kết quả khi dạy - học trực tuyến và sử dụng công nghệ thông tin.

Nền tảng hạ tầng công nghệ thông tin hiện đại: phải được trang bị đồng bộ trong các cơ sở giáo dục đại học và toàn lực lượng, đảm bảo việc quản lý điều hành, quản lý giáo dục, dạy - học, kiểm tra, đánh giá có thể được thực hiện một cách bình đẳng giữa các đơn vị có đặc thù khác nhau; đảm bảo môi trường mạng thông suốt, ổn định, an toàn thông tin. Thực hiện việc này cần huy động được các nguồn lực trong, ngoài ngành và nguồn lực từ quốc tế chung tay hỗ trợ trang thiết bị đầu cuối và tham gia cung cấp các hệ thống, giải pháp đáp ứng yêu cầu chuyển đổi số. Chuyển đổi số yêu cầu tất cả những chương trình, phần mềm riêng lẻ, tách biệt phải tương thích và kết nối với nhau, tích hợp trên cùng một nền tảng số. Có thể tạm hiểu là nền tảng số cho phép các hoạt động

giảng dạy, quản lý, học tập, kiểm tra, đánh giá, thi cử, quản lý người học, việc giảng dạy,... cũng như toàn bộ việc tương tác giữa người học với người dạy và nhà trường cùng diễn ra.

Yếu tố nhân lực: cần bồi dưỡng được đội ngũ nhân lực (cán bộ quản lý, giảng viên, học viên, cán bộ phục vụ) có kiến thức, kỹ năng đáp ứng yêu cầu chuyển đổi số. Trước hết, là kỹ năng sử dụng thành thạo công nghệ thông tin, kỹ năng an toàn thông tin, kỹ năng khai thác, sử dụng hiệu quả các ứng dụng phục vụ công tác giáo dục đại học trong trường.

Ngoài ra, giáo dục trong Công an Nhân dân có đặc thù về dữ liệu, đối tượng, hạ tầng nên có nhiều khó khăn và đặt ra những yêu cầu riêng trong bối cảnh chuyển đổi số và cần có những cách tiếp cận đặc biệt khác để đáp ứng xu hướng tương lai và đảm bảo tuân thủ các quy định. Một trong những điểm đặc biệt tạo nên sự khác biệt lớn với các trường ngoài ngành là trong các trường Công an Nhân dân có nhiều nội dung thuộc quản lý, giảng dạy và nghiên cứu thuộc danh mục bí mật Nhà nước. Do đó, trường Đại học An ninh nhân dân hạ tầng kỹ thuật đảm bảo lưu trữ, xử lý, khai thác dữ liệu phải được triển khai thành nhiều nhóm độc lập, chưa đồng bộ, liên thông với nhau và có điều kiện quản lý với nhiều ràng buộc để đảm bảo yêu cầu bảo vệ bí mật Nhà nước.

4. Khó khăn, tồn tại trong việc thực hiện chuyển đổi số tại trường Đại học An ninh nhân dân hiện nay

Chuyển đổi số tại trường Đại học An ninh nhân dân hiện nay còn gặp nhiều khó khăn, tồn tại và thách thức cần tiếp tục được tập trung khắc phục, hoàn thiện, cụ thể như sau:

Một là, do đặc thù lực lượng công an có nhiều nội dung tài liệu thuộc danh mục bí mật Nhà nước. Hệ thống văn bản quy định để có thể triển khai chuyển đổi số về cơ chế chính sách và cơ sở pháp lý của Bộ Công an trong việc chuyển đổi số của một số lĩnh vực còn gặp nhiều bất cập, chưa theo kịp được với thực tế. Bên cạnh đó, hệ thống văn bản quy định của hoạt động chuyển đổi số còn thiếu nhất quán, đôi khi còn hiện tượng ban hành cho có và mâu thuẫn giữa văn bản sau và văn bản trước. Sức ép để phải thực hiện chuyển đổi số chưa đủ lớn cũng như nhận thức chưa đầy đủ về ý nghĩa của chương trình chuyển đổi số, còn ngại thay đổi và tiếp cận những vấn đề mới.

Hai là, hạ tầng mạng, trang thiết bị công nghệ thông tin (như máy tính, camera, máy in, máy quét), đường truyền, dịch vụ Internet còn chưa được đầu tư tương xứng để đáp ứng với thực tiễn. Nhiều đơn vị chưa đáp ứng yêu cầu cho chuyển đổi số (cả về quản lý điều hành, quản lý giáo dục và dạy - học).

Ba là, số hóa, xây dựng, cập nhật học liệu số, thẩm định, chia sẻ học liệu số đòi hỏi sự đầu tư lớn về nhân lực (gồm cả nhân lực quản lý và nhân lực triển khai) và vấn đề bảo vệ bí mật nhà nước trong việc để đảm bảo kho học liệu số đầy đủ, đạt chất lượng, phục vụ yêu cầu học tập, nghiên cứu, tham khảo của cán bộ, giảng viên và học viên ở

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

các cấp học, ngành học, môn học. Vì vậy, hiện nay, vấn đề xây dựng học liệu số (như sách điện tử, thư viện điện tử, ngân hàng câu hỏi, bài giảng điện tử, phần mềm học điện tử, phần mềm ứng dụng mô phỏng, phần mềm quản lý điều hành) còn phát triển tự phát, chưa có hệ thống, khó kiểm soát chất lượng và nội dung.

Bốn là, trong yêu cầu hội nhập và mở rộng hợp tác quốc tế thì vấn đề “Thu thập, chia sẻ, khai thác dữ liệu quản lý giáo dục và học liệu số” cần hành lang pháp lý chung phù hợp với các quy định về bản quyền tác giả, sở hữu trí tuệ, an ninh thông tin, giao dịch điện tử và luật chia sẻ cung cấp thông tin, cụ thể như: Quy định quyền tác giả cho các bài giảng điện tử; quy định khai thác cơ sở dữ liệu, kho học liệu số quy định tính pháp lý của hồ sơ điện tử nói chung và sở điểm, sổ đầu bài điện tử, bảng điểm điện tử nói riêng.

5. Giải pháp nâng cao hiệu quả chuyển đổi số tại Trường Đại học An ninh nhân dân

Một là, Đảng ủy, Ban Giám hiệu tiếp tục quan tâm, chỉ đạo quyết liệt, hiệu quả, linh hoạt, sáng tạo việc chuyển đổi số, cần xác định đây là nhiệm vụ trọng tâm, hàng đầu cần ưu tiên. Theo đó, tiếp tục triển khai Đề án 1646/ĐA-T47 ngày 12/12/2016 về “Tin học hóa và cải cách thủ tục hành chính”, Đề án 2121/ĐA-T47 ngày 14/11/2017 về Nhà trường điện tử và những văn bản khác có liên quan.

Trường cần xây dựng và ban hành các cơ chế, chính sách thuận lợi cho chuyển đổi số, liên quan đến học liệu như sở hữu trí tuệ, bản quyền tác giả; liên quan đến chất lượng việc dạy học trên môi trường mạng như an toàn thông tin mạng; liên quan đến chính trị, tư tưởng, đạo đức người dạy, người học như bảo vệ thông tin cá nhân, an ninh thông tin trên môi trường mạng; và các quy định liên quan đến điều kiện tổ chức dạy - học trên mạng, kiểm định chất lượng, tính pháp lý và công nhận kết quả khi dạy - học trực tuyến.

Hai là, chủ động tổ chức triển khai Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030; xây dựng cơ sở pháp lý cho hình thức giảng dạy trên nền tảng số. Xây dựng quy trình và văn bản hướng dẫn cách làm, bước đi cần thiết trong quá trình chuyển đổi số tại Trường, đồng thời đảm bảo bí mật nhà nước theo quy định.

Ba là, tổ chức tuyên truyền, nâng cao nhận thức cho lãnh đạo và cán bộ, giảng viên, học viên, tất cả mọi người về sự cấp thiết của chuyển đổi số, nội dung chuyển đổi số, qua đó đổi mới căn bản, toàn diện giáo dục và đào tạo. Tổ chức tập huấn, bồi dưỡng về chuyển đổi số nhằm trang bị kiến thức về mạng máy tính, kỹ năng ứng dụng công nghệ thông tin vào lĩnh vực công tác.

Đây là yếu tố quyết định trực tiếp tới hiệu quả dạy và học trong môi trường ứng dụng công nghệ toàn diện, ảnh hưởng trực tiếp đến hiệu suất giảng dạy của giảng viên, học tập của học viên, việc tìm kiếm, tra cứu nguồn tài liệu học tập cũng như khả năng

kết nối tri thức trong môi trường công nghệ rộng lớn. Do đó, Nhà trường cần chủ động đào tạo, bồi dưỡng đội ngũ cán bộ quản lý, nhà giáo và học viên những kiến thức, kỹ năng về công nghệ thông tin, an toàn thông tin cần thiết để có thể tự tin nghiên cứu, học tập và khai thác dữ liệu trên môi trường học tập được số hóa, đáp ứng yêu cầu hội nhập và mở rộng hợp tác quốc tế. Tuy nhiên, để đạt được mục tiêu dài hạn, dưới góc độ quản lý nhà nước, trường Đại học An ninh nhân dân cần chủ động và tập trung trang bị cho cán bộ, giảng viên, học viên những kỹ năng về chuyển đổi số ở mọi cấp học, ngành học và môn học. Việc rèn luyện kỹ năng số phải được triển khai từ sớm, đồng bộ ở các dạng thức đơn giản, phù hợp với lứa tuổi, mọi cấp học, ngành học. Nhà trường cũng cần chủ động xây dựng khung năng lực số cho cán bộ, giảng viên và học viên trong đó không chỉ dừng lại ở những kỹ năng sử dụng kiến thức công nghệ mà hướng đến phát triển năng lực tư duy, khả năng sáng tạo, thích ứng với môi trường công nghệ tiên tiến của thế giới.

Bốn là, cần xây dựng cơ chế chính sách và cơ sở pháp lý tham mưu cho Bộ Công an về hội nhập và mở rộng hợp tác quốc tế trong bối cảnh chuyển đổi số; kiến nghị Bộ Công an đầu tư kinh phí cho từng hạng mục, nhất là hạ tầng công nghệ thông tin; tăng cường hợp tác, trao đổi qua đó học tập kinh nghiệm chuyển đổi số của cơ sở giáo dục và đào tạo trong và ngoài nước. Chủ động hợp tác với cơ quan tư vấn, nhà thầu để có thể mua hoặc nhận chuyển giao phần mềm phục vụ công tác của Nhà trường đáp ứng yêu cầu phát triển trong bối cảnh cuộc cách mạng công nghiệp lần thứ 4, góp phần bảo vệ an ninh quốc gia tình hình mới.

6. Kết luận

Như vậy, bối cảnh chuyển đổi số đặt ra cho giáo dục nói chung và giáo dục đại học nói riêng những thách thức vô cùng lớn. Đó là nhu cầu đào tạo nguồn nhân lực chất lượng cao, có khả năng thích nghi, đáp ứng nhu cầu sử dụng của xã hội. Để từng bước thực hiện chuyển đổi số thành công, thời gian qua Trường Đại học An ninh nhân dân đã tích cực, chủ động trong việc triển khai quá trình chuyển đổi số tại Trường, trong đó Nhà trường đã tập trung xây dựng và triển khai Kế hoạch chuyển đổi số đến năm 2025, tầm nhìn đến năm 2030. Công cuộc chuyển đổi số là tất yếu, phù hợp với yêu cầu của Chính phủ và phù hợp với xu thế chung của thế giới. Tuy nhiên, để có thể chuyển đổi số thành công cần phải giải quyết rất nhiều khó khăn về cơ sở hạ tầng, về yêu cầu quản lý và triển khai trong Nhà trường. Do đó, để công cuộc chuyển đổi số được triển khai thực hiện thì trước hết bản thân Nhà trường cần phải tự xây dựng một kế hoạch chuyển đổi số phù hợp, khoa học, tận dụng mọi tài nguyên, nguồn nhân lực và hỗ trợ từ Bộ Công an và xã hội.

T.A.T

DANH MỤC TÀI LIỆU THAM KHẢO

- Đảng Cộng sản Việt Nam (2021), Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, Tập I, Nxb. Chính trị quốc gia Sự thật, Hà Nội.
- Đảng Cộng sản Việt Nam, Văn kiện Đại hội đại biểu Đảng bộ Trường Đại học An ninh nhân dân lần thứ XV, nhiệm kỳ 2020 – 2025, Thành phố Hồ Chí Minh, 10/2020.
- Hồ Chí Minh (2011) toàn tập, Tập 6, Nxb Chính trị quốc gia, Hà Nội.
- Thủ tướng Chính phủ, Quyết định số 749/QĐ – TTg ngày 3/6/2020 phê duyệt “Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”.

**KỸ NĂNG BẢO MẬT THÔNG TIN KHI SỬ DỤNG INTERNET
CỦA SINH VIÊN CÁC TRƯỜNG CÔNG AN NHÂN DÂN
PHÍA NAM**

**INFORMATION SECURITY SKILLS WHEN USING THE
INTERNET OF STUDENTS OF SOUTHERN PEOPLE'S
PUBLIC SECURITY UNIVERSITIES**

Thạc sĩ Dương Văn Quế, Trần Minh Hải, Nguyễn Đình Lộc, Nguyễn Minh Tú

Trường Đại học An ninh nhân dân

*Tác giả liên hệ: duongvanque2087@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> kỹ năng bảo mật thông tin, Internet, sinh viên, các trường Công an nhân dân phía Nam	Bài viết khảo sát thực trạng kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường Công an nhân dân phía Nam trên ba phương diện nhận thức, thái độ và hành động. Kết quả khảo sát 434 sinh viên cho thấy: sinh viên có thái độ ở mức rất tốt, nhận thức và hành động ở mức khá tốt. Tuy nhiên, một số biểu hiện mặt nhận thức và hành động còn hạn chế và sinh viên vẫn còn thực hiện một số hành động rủi ro cao trong bảo mật thông tin. Do vậy, nhóm tác giả kiến nghị một số vấn đề đối với các trường Công an nhân dân phía Nam, đội ngũ giảng viên, cán bộ quản lý và sinh viên nhằm cải thiện kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường Công an nhân dân phía Nam trong thời gian tới.
<i>Keywords:</i> information security skills, Internet, students, Southern People's Public Security Universities	ABSTRACT The article surveys the current state of information security skills when using the Internet of students at the Southern People's Public Security Universities in three aspects: awareness, attitude and action. Survey results of 434 students show that: students have very good attitudes, awareness and actions at quite good levels. However, some cognitive and action manifestations are still limited

and students still perform some high-risk actions in information security. Therefore, the authors propose a number of issues for Southern People's Public Security Universities, lecturers, administrators and students to improve students' information security skills when using the Internet in the near future.

1. Giới thiệu

Ở nước ta, theo số liệu thống kê của Bộ Thông tin và Truyền thông cho thấy, tính tới tháng 9/2022, số lượng người dùng Internet tại Việt Nam vào khoảng 70 triệu người, chiếm khoảng 70% dân số cả nước. Người dùng Việt Nam dành trung bình 7 tiếng mỗi ngày để tham gia các hoạt động liên quan đến Internet. Bên cạnh đó, số lượng người dùng ở Việt Nam tham gia các mạng xã hội như Facebook, Zalo, Tiktok,... ngày càng tăng nhanh. Tuy nhiên, vấn đề bảo mật thông tin khi sử dụng Internet chưa được người dùng quan tâm đúng mức. Chính vì thế, các thế lực thù địch, bọn tội phạm triệt để lợi dụng lỗ hổng bảo mật để đánh cắp thông tin của người dùng và tiến hành hoạt động vi phạm pháp luật.

Hiện nay, sinh viên các trường Công an nhân dân (CAND) sử dụng Internet và mạng xã hội rất phổ biến với nhiều mục đích khác nhau như: tìm hiểu thông tin, tài liệu phục vụ học tập; giải trí, thể hiện quan điểm, suy nghĩ của bản thân; kết nối và chia sẻ với mọi người;... Bên cạnh những sinh viên có ý thức bảo mật thông tin tốt, vẫn còn một bộ phận sinh viên nhận thức chưa đúng đắn và vẫn còn vi phạm những quy định về bảo mật thông tin khi sử dụng Internet. Dẫn đến tình trạng lộ lọt thông tin nội bộ của Ngành, của Trường và thông tin cá nhân,... trên Internet mà nhất là mạng xã hội. Chính vì thế, vấn đề đặt ra, cần thiết phải nghiên cứu, làm rõ kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường CAND phía Nam, trên cơ sở đó đưa ra một số ý kiến đề xuất nhằm cải thiện kỹ năng này cho sinh viên.

2. Cơ sở lý thuyết

2.1. Kỹ năng

Hiện nay, khi bàn về khái niệm kỹ năng có hai quan niệm khác nhau. Quan niệm thứ nhất coi kỹ năng là mặt kỹ thuật, thao tác của hành động, hoạt động. Quan niệm thứ hai cho rằng kỹ năng không đơn thuần là mặt kỹ thuật của hành động mà còn là biểu hiện một mức độ năng lực của con người. Đó là quá trình con người vận dụng tri thức vào một lĩnh vực hoạt động cụ thể, đảm bảo cho hoạt động ấy diễn ra có kết quả. Tuy nhiên, quan niệm thứ hai được đa số các nhà nghiên cứu đồng tình, điển hình như:

Theo Vũ Dũng, “*Kỹ năng là năng lực vận dụng có kết quả những tri thức về phương thức hành động đã được chủ thể lĩnh hội để thực hiện những nhiệm vụ tương ứng. Ở mức độ kỹ năng, công việc được hoàn thành trong những điều kiện, hoàn cảnh không thay đổi, chất lượng chưa cao, thao tác chưa thuần thục, và còn phải tập trung chú ý căng thẳng. Kỹ năng được hình thành qua luyện tập*” (Vũ Dũng, 2008).

Huỳnh Văn Sơn cho rằng “*Kỹ năng là khả năng thực hiện có kết quả một hành động nào đó bằng cách vận dụng những tri thức, những kinh nghiệm đã có để hành động phù hợp với những điều kiện cho phép. Kỹ năng không chỉ đơn thuần về mặt kỹ thuật của hành động, mà còn là biểu hiện năng lực của con người*” (Huỳnh Văn Sơn, 2012).

Kỹ năng bao giờ cũng gắn với một hành động cụ thể. Nó là kết quả của việc vận dụng tri thức, kỹ xảo vào hoạt động thực tiễn và được thể hiện qua kết quả cao của hành động đó. Tính đúng đắn, sự thành thạo, linh hoạt, mềm dẻo của các thao tác là tiêu chuẩn để đánh giá về sự phát triển của kỹ năng.

2.2. Bảo mật thông tin khi sử dụng Internet

Theo Cambridge Dictionary, Internet là “*hệ thống lớn máy tính được kết nối khắp thế giới cho phép mọi người chia sẻ thông tin và liên lạc với nhau*”.

Theo Wikipedia, “*Internet hay Mạng là một hệ thống thông tin toàn cầu có thể được truy nhập công cộng gồm các mạng máy tính được liên kết với nhau*”.

Vì vậy, có thể hiểu Internet là thông tin toàn cầu, được liên kết thông qua các trang mạng máy tính giúp mọi người chia sẻ thông tin và liên lạc với nhau. Đồng thời Internet thuộc quyền sở hữu chung của mọi người, mỗi phần của mạng được liên kết với nhau nhằm tạo nên một mạng toàn cầu.

- Về thuật ngữ bảo mật

Theo Đại từ điển Tiếng Việt: bảo có nghĩa là chăm sóc, giữ gìn, phụ trách, chịu trách nhiệm..., mật có nghĩa là kín, cần phải giữ kín, không để lộ ra (tin mật, tài liệu mật, mật lệnh...). Theo đó “*bảo mật là giữ bí mật những điều được coi là hệ trọng, bí mật cơ quan, tổ chức*” (Nguyễn Như Ý, 1998).

Bên cạnh đó, bảo mật là khái niệm được sử dụng phổ biến trong lĩnh vực an ninh mạng. Theo Từ điển bách khoa Việt Nam “*bảo mật là sự hạn chế khả năng lạm dụng tài nguyên và tài sản*” (Hội đồng quốc gia chỉ đạo biên soạn Từ điển bách khoa Việt Nam, 1995).

Như vậy, chúng ta có thể hiểu bảo mật chính là bảo vệ những điều được coi là quan trọng, bí mật nhằm tránh khỏi sự lạm dụng tài nguyên và tài sản.

- Theo Từ điển bách khoa Việt Nam thông tin được định nghĩa như sau “*thông tin: một khái niệm cơ bản của khoa học hiện đại, khái quát về các điều hiểu biết, tri thức thu được qua nghiên cứu, khảo sát hoặc trao đổi thông tin giữa các đối tượng với nhau*” (Hội đồng quốc gia chỉ đạo biên soạn Từ điển bách khoa Việt Nam, 1995).

- Bảo mật thông tin khi sử dụng Internet

Có thể hiểu bảo mật thông tin là bảo vệ những thông tin, dữ liệu của cá nhân hay cơ quan, tổ chức nhằm tránh khỏi sự đánh cắp của những đối tượng xấu hoặc tin tặc. Bảo mật thông tin được thể hiện qua việc duy trì tính bảo mật, tính sẵn sàng và tính toàn vẹn của thông tin. Để bảo mật thông tin cần thực hiện được các yếu tố chính sau: Bảo mật ứng dụng; Bảo mật đám mây; Mã hóa; Phục hồi sau sự cố; Ứng phó sự cố; Bảo mật hạ tầng; Quản lý lỗ hổng (A. Farooq, J. Isoaho, S. Virtanen & J. Isoaho, 2015).

Trong cuộc sống, mỗi cá nhân, tổ chức hay một quốc gia đều có những bí mật cần được cất giữ, bảo mật an toàn. Đối với cá nhân đó có thể là bí mật về đời sống tình cảm hoặc lý lịch bản thân. Với một tổ chức, có thể là cơ cấu tổ chức, chính sách, phương hướng phát triển riêng và cần được bảo mật. Đối với một quốc gia, đó là những tin về vụ, việc, tài liệu, vật, địa điểm, thời gian, lời nói có nội dung quan trọng thuộc lĩnh vực chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ, các lĩnh vực khác mà Nhà nước không công bố hoặc chưa công bố và nếu bị tiết lộ thì gây nguy hại cho Nhà nước. Vì vậy bảo mật những thông tin bí mật có vai trò quan trọng đối với sự phát triển của một cá nhân, tổ chức và cả một quốc gia.

Như vậy, có thể hiểu bảo mật thông tin khi sử dụng mạng Internet tức là bảo vệ, giữ bí mật không cho phát tán, tuyên truyền những điều được coi là hệ trọng, bí mật của cá nhân, cơ quan, tổ chức, Nhà nước lên các trang mạng.

2.3. *Kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các Trường CAND phía Nam*

Sinh viên các trường CAND thường xuyên tiếp xúc với bí mật Nhà nước, bí mật công tác. Do vậy, sinh viên cần phải có ý thức giữ gìn bí mật Nhà nước, bí mật công tác; thông tin bí mật của Ngành, tài liệu nghiệp vụ; thông tin bí mật của Nhà trường, lớp và những thông tin cá nhân... khi sử dụng Internet để tránh bị các thế lực thù địch, đối tượng thu thập thông tin, phục vụ hoạt động xấu.

Kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường CAND phía Nam là khả năng thực hiện hiệu quả hoạt động bảo mật thông tin khi sử dụng Internet dựa trên nền tảng kiến thức, thái độ và năng lực thực hành của sinh viên.

Kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường CAND phía Nam bao gồm các kỹ năng cơ bản như sau: Kỹ năng lập trình, mã hóa thông tin; kỹ năng phòng ngừa, phát hiện nguy cơ mất an toàn thông tin; kỹ năng bảo vệ thông tin, tài khoản cá nhân; kỹ năng giải quyết vấn đề liên quan đến an toàn thông tin; kỹ năng cung cấp, đăng tải, chia sẻ thông tin. Kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các Trường CAND phía Nam được biểu hiện ở 3 khía cạnh: nhận thức, thái độ và hành động, cụ thể:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

+ Về nhận thức: Nhận thức về tầm quan trọng việc bảo mật thông tin khi sử dụng Internet; Nhận thức về mức độ cần thiết của các thông tin cần bảo mật khi sử dụng Internet; Nhận thức về hậu quả, tác hại của việc đăng tải thông tin cần bảo mật lên Internet và các trang mạng xã hội; Nhận thức về các kỹ năng cơ bản của kỹ năng bảo mật thông tin khi sử dụng Internet.

+ Về thái độ: Mức độ quan tâm đối với việc bảo mật thông tin khi sử dụng Internet; Mức độ lên án, phê phán khi phát hiện đồng đội đăng tải những thông tin cần bảo mật lên Internet; Mức độ tích cực bản thân trong bảo mật thông tin khi sử dụng mạng Internet; Mức độ tích cực khi thực hiện các hành động góp phần bảo mật thông tin khi sử dụng Internet.

+ Về hành động: Mức độ thường xuyên thực hiện các hành động dẫn đến nguy cơ lộ lọt thông tin khi sử dụng Internet; Mức độ thường xuyên tham gia hoạt động góp phần bảo mật thông tin khi sử dụng Internet; Mức độ thường xuyên thực hiện các thao tác của kỹ năng bảo mật thông tin khi sử dụng Internet.

3. Phương pháp nghiên cứu

Để tìm hiểu thực trạng kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các Trường CAND phía Nam, tác giả sử dụng một số phương pháp cụ thể sau đây:

- *Một là, phương pháp nghiên cứu tài liệu:* Nhóm tác giả tiến hành nghiên cứu tài liệu từ sách, tạp chí, các công trình nghiên cứu... có liên quan về kỹ năng, bảo mật thông tin, ý thức bảo mật thông tin khi sử dụng Internet của sinh viên. Thông qua đó, hệ thống hóa tài liệu, xác định và xây dựng cơ sở lý luận, làm rõ các khái niệm công cụ về kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các Trường CAND phía Nam.

- *Hai là, phương pháp điều tra xã hội học:* Đây là phương pháp cơ bản và quan trọng nhất mà tác giả sử dụng để thực hiện nghiên cứu đề tài này. Thực hiện phương pháp này nhằm tìm hiểu kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường CAND phía Nam trên 03 mặt: nhận thức và thái độ và hành động của sinh viên về vấn đề bảo mật thông tin khi sử dụng Internet.

+ Xây dựng bảng hỏi: Căn cứ vào lý luận cơ bản, các khái niệm công cụ, tiêu chí và lĩnh vực đánh giá để thiết kế bảng hỏi. Đồng thời tiến hành khảo sát thử và chỉnh sửa, hoàn chỉnh bảng hỏi. Nội dung xoay quanh một số vấn đề sau: Nhận thức, thái độ và hành động của sinh viên về vấn đề bảo mật thông tin khi sử dụng Internet.

+ Về địa bàn khảo sát: Nhóm tác giả tiến hành phát phiếu khảo sát và gửi link khảo sát bằng Google Form đến sinh viên của các trường CAND phía Nam (Trường Đại học An ninh nhân dân, Trường Đại học Cảnh sát nhân dân, Trường Cao đẳng An ninh nhân dân II) để tiến hành khảo sát.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

+ Chọn mẫu:

Xác định cỡ mẫu: Cỡ mẫu được tính theo công thức sau:

$$n = \frac{N}{1 + N(e)^2}$$

Trong đó:

n: Cỡ mẫu

N: Dân số

e: Sai số tiêu chuẩn (+-5%)

Các trường CAND phía Nam bao gồm: Trường Đại học An ninh nhân dân và Trường Đại học Cảnh sát nhân dân và Trường Cao đẳng An ninh nhân dân II với khoảng 10300 sinh viên. Như vậy, số lượng mẫu cần khảo sát là 385. Đồng thời, nhóm tác giả sử dụng phương pháp chọn mẫu: chọn mẫu ngẫu nhiên, mang tính đại diện.

+ Tiến hành điều tra chính chức: Nhóm tác giả sử dụng ứng dụng Google Form để khảo sát đối với sinh viên các Trường CAND phía Nam, nhóm tác giả đã thu về 479 mẫu hỏi. Loại trừ các mẫu không hợp lệ, số mẫu được chọn để thống kê còn 434 mẫu.

Ba là, phương pháp thống kê toán học: Nhóm tác giả sử dụng phần mềm SPSS for Windows 24.0 để xử lý số liệu bằng cách tính tỉ lệ phần trăm (%), điểm trung bình (ĐTB), thống kê tần số. Những câu hỏi khảo sát mức độ sẽ được tính điểm từ 1 điểm tới 5 điểm tương ứng với các mức từ 1 đến 5 trong đó mức 1 là mức tiêu cực nhất và mức 5 là mức tích cực nhất. Kết quả khảo sát thu được tùy thuộc vào cách phân chia mức độ như sau để đưa ra kết luận về kỹ năng của sinh viên các trường Công an nhân dân phía Nam về vấn đề bảo mật thông tin khi sử dụng mạng Internet, cụ thể như sau:

- Từ 1.00 đến 1.80 điểm: Mức rất tiêu cực.
- Từ 1.81 đến 2.60 điểm: Mức tiêu cực.
- Từ 2.61 đến 3.40 điểm: Mức trung tính.
- Từ 3.41 đến 4.20 điểm: Mức khá tích cực.
- Từ 4.21 đến 5.00 điểm: Mức rất tích cực.

4. Kết quả nghiên cứu

4.1. Về nhận thức

- Một là, nhận thức của sinh viên các trường CAND về tầm quan trọng của việc bảo mật thông tin khi sử dụng Internet

Khảo sát nhận thức về tầm quan trọng của việc bảo mật thông tin khi sử dụng Internet của sinh viên các trường CAND, nhóm tác giả thu được kết quả ở Bảng 1, cụ thể: Nhận thức của sinh viên về tầm quan trọng của việc bảo mật thông tin khi sử dụng Internet ở mức rất tích cực với ĐTB là 4.76, trong đó 76% sinh viên cho rằng việc bảo mật thông tin khi sử dụng Internet là “Rất quan trọng”, 24% sinh viên cho rằng việc bảo

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

mật thông tin khi sử dụng Internet là “Khá quan trọng”. Điều này cho thấy, 100% sinh viên đều có nhận thức đúng đắn và đánh giá cao tầm quan trọng việc bảo mật thông tin khi sử dụng Internet.

Bảng 1: Nhận thức của học viên về tầm quan trọng việc bảo mật thông tin khi sử dụng Internet

STT	Mức độ	Tỷ lệ (%)	ĐTB
1	Rất quan trọng	76	4.76
2	Khá quan trọng	24	
3	Bình thường	0	
4	Ít quan trọng	0	
5	Không quan trọng	0	

- Hai là, nhận thức về mức độ cần thiết cần phải bảo mật của những thông tin quan trọng khi sử dụng Internet

Khảo sát nhận thức của sinh viên về mức độ cần thiết phải bảo mật của những thông tin quan trọng khi sử dụng Internet, nhóm tác giả thu được kết quả ở Bảng 2, cụ thể: Nhận thức của sinh viên về mức độ cần thiết phải bảo mật của những thông tin khi sử dụng Internet ở mức rất tích cực, với ĐTB chung là 4.62. Tất cả 08 thông tin được đề xuất đều được sinh viên đánh giá là cần thiết và điểm trung bình đều ở mức rất tích cực (từ 4.43 đến 4.75), trong đó: Xếp vị trí thứ nhất là thông tin về chủ trương, đường lối, chính sách của Đảng và Nhà nước có điểm trung bình cao nhất (4.75); Ở vị trí thứ hai đó là thông tin về quân số của lớp, của khoa, lý lịch của cán bộ, đảng viên (ĐTB là 4.73); Ở vị trí thứ ba đó là thông tin về chương trình học tập, đề cương chi tiết học phần, lịch học (ĐTB là 4.71); 02 thông tin có điểm số thấp nhất đó là: Thông tin về tiêu chuẩn sức khỏe, chuẩn đầu ra, đầu vào của Trường; Thông tin, lý lịch cá nhân của sinh viên với ĐTB lần lượt là 4.43 và 4.51. Tuy nhiên, một số thông tin quan trọng như: thông tin về những thông tin bí mật của Ngành, tài liệu nghiệp vụ và thông tin, lý lịch cá nhân của sinh viên lại có ĐTB đứng thứ 6 và thứ 7.

Bảng 2: Nhận thức về mức độ cần thiết phải bảo mật của những thông tin quan trọng khi sử dụng Internet

STT	Nội dung	ĐTB	Thứ bậc
1	Những bí mật về chủ trương, đường lối, chính sách của Đảng và Nhà nước	4.75	1
2	Những thông tin bí mật của Ngành, tài liệu nghiệp vụ	4.52	6
3	Những thông tin về tiêu chuẩn sức khỏe, chuẩn đầu ra, đầu vào của Trường	4.43	8
4	Chương trình học tập, đề cương chi tiết học phần, lịch học	4.71	3

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

5	Thông tin về quân số của lớp, của khóa, lý lịch của cán bộ, đảng viên	4.73	2
6	Thông tin, hoạt động của các lớp, Câu Lạc bộ, Đoàn thanh niên, Hội phụ nữ	4.63	5
7	Thông tin, lý lịch cá nhân của sinh viên	4.51	7
8	Hình ảnh mặc quân phục, hoạt động của giáo viên, sinh viên	4.70	4
ĐTB chung		4.62	

- Ba là, nhận thức về tác hại của việc lộ, đăng tải thông tin cần bảo mật của sinh viên các trường Công an phía Nam lên Internet và mạng xã hội

Khảo sát nhận thức về vấn đề này, nhóm tác giả thu được kết quả ở Bảng 3 như sau:

Bảng 3: Nhận thức về tác hại việc lộ, đăng tải thông tin cần bảo mật của sinh viên các trường Công an phía Nam lên Internet và các trang mạng xã hội

STT	Nội dung	ĐTB	Thứ bậc
1	Là cơ sở để các thế lực thù địch tuyên truyền xuyên tạc chống phá Đảng, Nhà nước, Ngành Công an	4.73	2
2	Các thế lực thù địch thu thập thông tin, hình ảnh bôi nhọ lực lượng Công an	4.52	4
3	Là nguồn thông tin để các loại tội phạm tìm hiểu cơ cấu tổ chức của Ngành ta, đội ngũ cán bộ, phương pháp nghiệp vụ của ta gây khó khăn trong công tác	4.74	1
4	Lộ, lọt bí mật, tài liệu nghiệp vụ	4.29	6
5	Lộ thông tin, hình ảnh cá nhân, người thân dễ bị các đối tượng xấu thu thập, sử dụng vào hoạt động xấu	4.52	4
6	Bị xử lý kỷ luật	4.27	7
7	Làm xấu đi hình ảnh của Trường, của sinh viên	4.72	3
ĐTB chung		4.54	

Kết quả ở Bảng 3 cho thấy: Nhận thức của sinh viên về 07 tác hại được đề xuất của việc lộ, đăng tải thông tin cần bảo mật lên Internet và các trang mạng xã hội đều ở mức rất tích cực, với ĐTB chung là 4.54. Trong đó, sinh viên cho rằng: “Là nguồn thông tin để các loại tội phạm tìm hiểu cơ cấu tổ chức của Ngành ta, đội ngũ cán bộ, phương pháp nghiệp vụ của ta gây khó khăn trong công tác” có ĐTB cao nhất (4.74); tiếp theo đó là là cơ sở để các thế lực thù địch tuyên truyền xuyên tạc chống phá Đảng, Nhà nước, Ngành Công an (4.73); 02 tác hại là làm lộ, lọt tài liệu nghiệp vụ và bị xử lý kỷ luật là

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

hạn chế nhất với ĐTB lần lượt là 4.29 và 4.27. Nhìn chung, sinh viên có nhận thức tốt về tác hại của việc lộ, đăng tải thông tin cần bảo mật lên Internet và các trang mạng xã hội (ĐTB từ 4.29 đến 4.74).

- Bốn là, nhận thức của sinh viên các trường CAND phía Nam về các kỹ năng bộ phận của kỹ năng bảo mật thông tin khi sử dụng Internet

Khảo sát nhận thức của sinh viên về các kỹ năng bộ phận của kỹ năng bảo mật thông tin khi sử dụng Internet, nhóm tác giả thu được kết quả ở Bảng 4 như sau: Nhận thức về các kỹ năng cơ bản của kỹ năng bảo mật thông tin khi sử dụng Internet ở mức khá tích cực, với ĐTB chung là 3.74, cụ thể trong 06 kỹ năng được đề xuất, sinh viên nhận thức rất tích cực ở 01 kỹ năng; nhận thức khá tích cực ở 03 kỹ năng; nhận thức ở mức trung tính ở 02 kỹ năng. Trong đó, sinh viên có nhận thức tốt nhất ở kỹ năng “Kỹ năng bảo vệ thông tin, tài khoản cá nhân” với ĐTB là 4.28, thứ hai là kỹ năng “Kỹ năng phòng ngừa, phát hiện nguy cơ mất an toàn thông tin” với ĐTB là 3.84; sinh viên nhận thức về “Kỹ năng lập trình, mã hóa thông tin” là hạn chế nhất với ĐTB là 2.94.

Bảng 4: Nhận thức về các kỹ năng bộ phận của kỹ năng bảo mật thông tin khi sử dụng Internet

STT	Kỹ năng bộ phận	ĐTB	Thứ bậc
1	Kỹ năng phòng ngừa, phát hiện nguy cơ mất an toàn thông tin	3.84	4
2	Kỹ năng lập trình, mã hóa thông tin	2.94	6
3	Kỹ năng bảo vệ thông tin, tài khoản cá nhân	4.28	1
4	Kỹ năng giải quyết vấn đề liên quan đến bảo mật thông tin	3.40	5
5	Kỹ năng cung cấp, đăng tải, chia sẻ thông tin	4.10	2
6	Kỹ năng bảo vệ và kiểm soát truy cập	3.90	3
ĐTB chung		3.74	

- Năm là, nhận thức về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin của sinh viên khi sử dụng Internet

Khảo sát nhận thức về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin của sinh viên khi sử dụng Internet, nhóm tác giả thu được kết quả ở Bảng 5 như sau: Nhận thức về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin của sinh viên khi sử dụng Internet ở mức trung bình, với ĐTB chung là 3.29. Trong 10 yếu tố được đề xuất, sinh viên cho rằng 01 yếu tố có mức độ ảnh hưởng ở mức rất cao; 03 yếu tố ở mức khá cao; 05 yếu tố ở mức trung bình và 01 yếu tố ở mức yếu, cụ thể yếu tố công tác tuyên truyền, giáo dục ý thức bảo mật cho sinh viên còn hạn chế có điểm trung bình cao nhất (4.48), tiếp theo là yếu tố do sinh viên nhận thức chưa đúng đắn về hậu quả, tác hại của việc lộ

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

lọt thông tin trên Internet (3.56); yếu tố có ảnh hưởng thấp nhất đó là do nhận thức hạn chế của sinh viên về thủ thuật bảo mật thông tin có ĐTB thấp nhất (2.42).

Bảng 5: Các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin của sinh viên khi sử dụng Internet

STT	Yếu tố ảnh hưởng	ĐTB	Thứ bậc
1	Nhận thức hạn chế của sinh viên về thủ thuật bảo mật thông tin	2.42	10
2	Sinh viên còn hạn chế về kỹ năng sử dụng Internet an toàn	3.56	4
3	Nhận thức của sinh viên về âm mưu, phương thức thủ đoạn hoạt động của các thế lực thù địch còn hạn chế	3.33	6
4	Sinh viên nhận thức chưa đúng đắn về hậu quả, tác hại của việc lộ lọt thông tin trên Internet	3.58	2
5	Tâm lý chủ quan của sinh viên	3.34	5
6	Ảnh hưởng của tâm lý đám đông	2.89	7
7	Do công tác tuyên truyền, giáo dục ý thức bảo mật cho sinh viên còn hạn chế	4.48	1
8	Việc phát hiện, nhắc nhở, chấn chỉnh những hành vi tiêu cực của sinh viên trên Internet còn hạn chế	3.57	3
9	Công tác tập huấn, phổ biến về kỹ năng bảo mật thông tin còn hạn chế	2.87	8
10	Hình thức xử lý của trường hợp vi phạm còn nhẹ, tính răn đe không cao	2.86	9
ĐTB chung		3.29	

Tóm lại, kết quả khảo sát nhận thức của sinh viên trên 05 phương diện cho thấy: Mức độ nhận thức của sinh viên về kỹ năng bảo mật thông tin ở mức khá tích cực nhưng tiệm cận mức rất tích cực với ĐTB chung là 4.19, cụ thể nhận thức của sinh viên trên 03 phương diện ở mức rất tích cực; 02 phương diện ở mức khá tích cực. Trong đó nhận thức của sinh viên về tầm quan trọng của bảo mật thông tin khi sử dụng Internet là tốt nhất; nhận thức của sinh viên về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin khi sử dụng Internet là hạn chế nhất (xem Bảng 6).

Bảng 6: Bảng tổng hợp kết quả về nhận thức

STT	Nội dung	ĐTB
1	Nhận thức của sinh viên về tầm quan trọng việc bảo mật thông tin khi sử dụng Internet	4.76
2	Nhận thức về mức độ cần thiết phải bảo mật của những thông tin quan trọng khi sử dụng Internet	4.62
3	Nhận thức về tác hại việc lộ, đăng tải thông tin cần bảo mật của sinh viên các trường Công an phía Nam lên Internet và các trang mạng xã hội	4.54
4	Nhận thức về các kỹ năng bộ phận của kỹ năng bảo mật thông tin khi sử dụng Internet	3.74
5	Nhận thức về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin của sinh viên khi sử dụng Internet	3.29
ĐTB chung		4.19

4.2. Về thái độ

- Thứ nhất, mức độ tích cực của sinh viên các Trường CAND phía Nam trong bảo mật thông tin khi sử dụng mạng Internet

Tiến hành khảo sát mức độ tích cực của sinh viên về vấn đề này, tác giả thu được kết quả ở Bảng 7, như sau:

Bảng 7: Mức độ tích cực của sinh viên trong vấn đề bảo mật thông tin khi sử dụng Internet

STT	Mức độ	Tỷ lệ (%)	ĐTB
1	Rất tích cực	71.20	4.70
2	Khá tích cực	26.90	
3	Bình thường	1.90	
4	Ít tích cực	0	
5	Không tích cực	0	

Kết quả ở Bảng 7 cho thấy: Đa số các sinh viên có thái độ rất tích cực trong việc bảo mật thông tin khi sử dụng Internet với 71.20% sinh viên lựa chọn mức độ “Rất tích cực” và 26.90% sinh viên lựa chọn mức “Khá tích cực”, chỉ 1.90% lựa chọn mức “Bình thường”. Theo đó mức độ tích cực của sinh viên trong vấn đề bảo mật thông tin khi sử dụng Internet ở mức rất tích cực với ĐTB là 4.70.

- Thứ hai, mức độ quan tâm của sinh viên trong việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet

Khảo sát về độ quan tâm của sinh viên trong việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet, nhóm tác giả thu được kết quả ở Bảng 8, cụ thể: Mức độ

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

quan tâm của sinh viên trong việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet ở mức rất tích cực với ĐTB là 4.70, trong đó 72.96% sinh viên lựa chọn mức “Rất quan tâm”; 24.70% lựa chọn mức “Khá quan tâm” và chỉ có 2.34% lựa chọn mức “Bình thường”. Điều này cho thấy, đại đa số sinh viên rất quan tâm đến việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet.

Bảng 8: Mức độ quan tâm của sinh viên trong việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet

STT	Mức độ	Tỷ lệ (%)	ĐTB
1	Rất tích cực	72.96	4.70
2	Khá tích cực	24.70	
3	Bình thường	2.34	
4	Ít tích cực	0	
5	Không tích cực	0	

- Thứ ba, mức độ lên án, phê phán của sinh viên khi phát hiện đồng chí, đồng đội đăng tải những thông tin cần bảo mật lên Internet và mạng xã hội

Kết quả khảo sát ở Bảng 9 cho thấy: Khi phát hiện đồng chí, đồng đội đăng tải những thông tin cần bảo mật lên mạng xã hội và Internet, đa số sinh viên đều có thái độ tích cực “Kịch liệt lên án, phê phán” và “Khá lên án, phê phán” với 75.10% sinh viên lựa chọn, với ĐTB là 4.43 đạt mức rất tích cực. Tuy nhiên, kết quả cho thấy, có một bộ phận sinh viên có thái độ thiếu tích cực khi phát hiện đồng chí, đồng đội đăng tải thông tin cần bảo mật lên Internet và mạng xã hội với 24.90% sinh viên lựa chọn thái độ “Bình thường”. Đây là thái độ chưa tích cực cần phải khắc phục của sinh viên.

Bảng 9: Mức độ lên án, phê phán của sinh viên khi phát hiện đồng chí đồng đội đăng tải những thông tin cần bảo mật lên mạng xã hội và Internet

STT	Mức độ	Tỷ lệ (%)	ĐTB
1	Kịch liệt lên án, phê phán	73.70	4.43
2	Khá lên án, phê phán	1.40	
3	Bình thường	24.90	
4	Ít phê phán, lên án	0	
5	Không lên án, phê phán	0	

- Thứ tư, mức độ tích cực tham gia các hoạt động góp phần cải thiện kỹ năng bảo mật thông tin khi sử dụng Internet

Kết quả ở Bảng 10 cho thấy: Mức độ tích cực tham gia các hoạt động góp phần cải thiện kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên ở mức khá tốt với ĐTB chung là 3.96, trong 05 hoạt động được đề xuất có 01 hoạt động ở mức rất tích cực, 03 hoạt động ở mức khá tích cực và 01 hoạt động ở mức trung bình. Đồng thời,

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

sinh viên tích cực nhất khi thực hiện hoạt động “Tìm hiểu kiến thức tin học, cách thức bảo mật thông tin khi sử dụng Internet, mạng xã hội” với ĐTB là 4.43; đứng vị trí thứ 2 là hoạt động “Tham gia các khóa tập huấn về kỹ năng bảo mật thông tin khi sử dụng Internet” với ĐTB là 4.10; sinh viên ít tích cực nhất khi thực hiện hoạt động “Tham gia các câu lạc bộ, hội, nhóm về kiến thức tin học và bảo mật thông tin” với ĐTB là 3.38.

Bảng 10: Mức độ tích cực tham gia các hoạt động góp phần nâng cao năng lực cá nhân trong bảo mật thông tin trên Internet

STT	Hoạt động	ĐTB	Thứ bậc
1	Tuyên truyền cho đồng đội về vấn đề bảo mật thông tin khi sử dụng mạng Internet	3.89	4
2	Tham gia các khóa tập huấn về kỹ năng bảo mật thông tin khi sử dụng Internet	4.10	2
3	Tìm hiểu kiến thức tin học, cách thức bảo mật thông tin khi sử dụng Internet, mạng xã hội	4.43	3
4	Chia sẻ những bài viết, thông tin cảnh báo về những nguy cơ, tác hại của việc lộ, lọt thông tin cá nhân, thông tin mật	4.00	1
5	Tham gia các câu lạc bộ, hội nhóm về kiến thức tin học và bảo mật thông tin	3.38	5
ĐTB chung		3.96	

Tổng hợp kết quả khảo sát trên 04 phương diện về thái độ của sinh viên các trường CAND phía Nam cho thấy: Biểu hiện mặt thái độ của kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên ở mức rất tích cực với ĐTB chung là 4.45, cụ thể có 03 biểu hiện ở mức rất tích cực, 01 biểu hiện ở mức khá tích cực. Trong đó, sinh viên có thái độ tích cực nhất trong vấn đề bảo mật thông tin khi sử dụng Internet và quan tâm việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet; sinh viên ít tích cực nhất khi tham gia các hoạt động góp phần nâng cao năng lực cá nhân trong bảo mật thông tin trên Internet (xem Bảng 11).

Bảng 11: Bảng tổng hợp kết quả về thái độ

STT	Nội dung	ĐTB
1	Mức độ tích cực của sinh viên trong vấn đề bảo mật thông tin khi sử dụng Internet	4.70
2	Mức độ quan tâm của sinh viên trong việc rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet	4.70
3	Mức độ lên án, phê phán của sinh viên khi phát hiện đồng chí đồng đội đăng tải những thông tin cần bảo mật lên mạng xã hội và Internet	4.43
4	Mức độ tích cực tham gia các hoạt động góp phần nâng cao năng lực cá nhân trong bảo mật thông tin trên Internet	3.96
ĐTB chung		4.45

4.3. Hành động

- Một là, mức độ thường xuyên thực hiện các hành động tiêu cực khi sử dụng Internet của sinh viên

Khảo sát về vấn đề này, nhóm tác giả thu về được kết quả ở Bảng 12, như sau: Mức độ thường xuyên thực hiện các hành động tiêu cực khi sử dụng Internet của sinh viên ở mức của sinh viên ở mức khá tích cực với ĐTB chung là 3.54. Trong 10 hành động được đề xuất có 02 hành động sinh viên rất hiếm khi thực hiện (Phát tán tài liệu mật; Cung cấp những thông tin của Trường, của Ngành với ĐTB lần lượt là 4.70 và 4.5); 02 hành động sinh viên ít thực hiện (Đăng tải hình ảnh mặc đồ ngành của cá nhân; Đăng tải chương trình học tập, đề cương chi tiết học phần, lịch học với ĐTB là 3.82 và 3.81); 06 hành động sinh viên thực hiện ở mức trung bình. Theo đó, 03 hành động mà sinh viên thường xuyên thực hiện nhất đó là Đăng tải thông tin về tiêu chuẩn sức khỏe, chuẩn đầu ra, đầu vào của Trường (ĐTB là 2.61); Thông tin về quân số của lớp, của khóa, lý lịch cá nhân (ĐTB là 2.67); Đăng tải hình ảnh của sinh viên, của Trường, của Ngành (ĐTB là 3.14).

Bảng 12: Mức độ thường xuyên thực hiện các hoạt động có nguy cơ ảnh hưởng đến bảo mật thông tin trên Internet

STT	Hành động	ĐTB	Thứ bậc
1	Đăng tải hình ảnh mặc đồ ngành của cá nhân	3.82	3
2	Cung cấp những thông tin thật của cá nhân	3.33	7
3	Cung cấp những thông tin của Trường, của Ngành	4.50	2
4	Đăng tải hình ảnh của sinh viên, của Trường, của Ngành	3.14	8
5	Phát tán tài liệu mật	4.74	1
6	Sử dụng máy tính có tài liệu mật lên mạng	3.37	5
7	Sử dụng thiết bị ghi nhớ có tài liệu mật để truy cập Internet	3.35	6
8	Đăng tải thông tin về tiêu chuẩn sức khỏe, chuẩn đầu ra, đầu vào của Trường	2.61	10
9	Đăng tải chương trình học tập, đề cương chi tiết học phần, lịch học	3.81	4
10	Thông tin về quân số của lớp, của khóa, lý lịch cá nhân	2.67	9
ĐTB chung		3.54	

(Ghi chú: điểm càng cao, sinh viên càng ít thực hiện hành động đó)

- Hai là, mức độ thường xuyên tham gia các hoạt động tích cực nhằm rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Khảo sát về mức độ thường xuyên tham gia các hoạt động tích cực của sinh viên các trường CAND phía Nam, nhóm tác giả thu được kết quả ở Bảng 13 như sau:

Bảng 13: Mức độ thường xuyên thực hiện các hoạt động tích cực nhằm rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet

STT	Nội dung	ĐTB	Thứ bậc
1	Tuyên truyền, vận động đồng đội về ý thức bảo mật thông tin khi sử dụng mạng Internet	4.28	3
2	Nhắc nhở, yêu cầu đồng đội xóa những thông tin, bài viết không được phép đăng tải	4.40	2
3	Tham gia các khóa tập huấn về kỹ năng bảo mật thông tin khi sử dụng Internet	3.87	6
4	Tìm hiểu kiến thức tin học, cách thức bảo mật thông tin khi sử dụng Internet, mạng xã hội	4.10	4
5	Tìm hiểu âm mưu, phương thức thủ đoạn, hoạt động của các thế lực thù địch	3.92	5
6	Chia sẻ những bài viết, thông tin cảnh báo về những nguy cơ, tác hại của việc lộ, lọt thông tin cá nhân, thông tin mật	4.52	1
7	Tham gia các câu lạc bộ, hội nhóm về kiến thức tin học và bảo mật thông tin	3.32	7
ĐTB chung		4.06	

Kết quả ở Bảng 13 cho thấy: Mức độ thường xuyên tham gia các hoạt động tích cực nhằm rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên ở mức khá tốt với ĐTB chung là 4.06, trong đó có 03 hành động ở mức rất tốt (Chia sẻ những bài viết, thông tin cảnh báo về những nguy cơ, tác hại của việc lộ, lọt thông tin cá nhân, thông tin mật với ĐTB cao nhất 4.52; Nhắc nhở, yêu cầu đồng đội xóa những thông tin, bài viết không được phép đăng tải có ĐTB đứng thứ 2 với 4.40; Tuyên truyền, vận động đồng đội về ý thức bảo mật thông tin khi sử dụng mạng Internet với ĐTB là 4.28, đứng vị trí thứ 3), 03 hành động ở mức khá tốt và 01 hành động ở mức trung bình (Tham gia các câu lạc bộ, hội nhóm về kiến thức tin học và bảo mật thông tin với ĐTB thấp nhất 3.32.)

- Ba là, mức độ thường xuyên thực hiện các thao tác của kỹ năng bảo mật thông tin khi sử dụng Internet

Khảo sát vấn đề này, nhóm tác giả thu được kết quả ở Bảng 14, cụ thể: Mức độ thường xuyên thực hiện các thao tác của kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên ở mức trung bình với ĐTB chung là 3.32. Trong 16 thao tác được đề xuất có: 01 thao tác ở mức rất tích cực, 06 thao tác ở mức tích cực; 05 thao tác ở mức trung bình; 04 thao tác ở mức tiêu cực. Theo đó, ở vị trí cao nhất thao tác “Cảnh giác trước

Kỹ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

thủ đoạn giả mạo để đánh cắp thông tin” có ĐTB là 4.83; Ở vị trí thứ 2 và thứ 3 lần lượt là thao tác “Không truy cập vào đường link, ứng dụng không rõ nguồn gốc trên các trang mạng xã hội, email,...” và “Chặn, ngắt kết nối với đối tượng xấu” với ĐTB lần lượt là 4.12 và 4.03. Ngược lại, 04 thao tác mà sinh viên ít thực hiện nhất đó là: Phát hiện hành vi lợi dụng gia đình, người thân để lấy cắp thông tin (ĐTB là 1.94); Nhờ chuyên gia hỗ trợ khi bị đánh cắp thông tin cá nhân, tài liệu (ĐTB là 2.15); Lưu trữ dấu vết, chứng cứ khi phát hiện bị đánh cắp thông tin và Quản lý lượt truy cập, theo dõi trên mạng xã hội, Internet với ĐTB cùng bằng 2.36.

Bảng 14: Mức độ thường xuyên thực hiện các thao tác của kỹ năng bảo mật thông tin

STT	Nội dung	ĐTB	Thứ bậc
1	Không truy cập vào đường link, ứng dụng không rõ nguồn gốc trên các trang mạng xã hội, email,...	4.12	2
2	Phát hiện những ứng dụng và dịch vụ độc hại trên mạng Internet, điện thoại thông minh,...	3.29	9
3	Cảnh giác trước thủ đoạn giả mạo để đánh cắp thông tin	4.83	1
4	Phát hiện hành vi lợi dụng gia đình, người thân để lấy cắp thông tin	1.94	16
5	Hạn chế sử dụng, cung cấp thông tin thật của cá nhân trên Internet	3.33	8
6	Đặt mật khẩu có độ khó cao và thường xuyên kiểm tra cài đặt bảo mật đối với các thiết bị lưu trữ thông tin, các tài khoản cá nhân	3.85	5
7	Tìm hiểu, chia sẻ về phương thức, thủ đoạn lừa đảo qua Internet và mạng xã hội	3.29	9
8	Cảnh giác cao đối với những tin nhắn, email từ người lạ	3.14	12
9	Cảnh giác các mối quan hệ trên mạng xã hội và xác định các mối quan hệ đáng tin cậy	3.73	6
10	Sử dụng phần mềm hỗ trợ bảo mật thông tin cá nhân	3.26	11
11	Lưu trữ dấu vết, chứng cứ khi phát hiện bị đánh cắp thông tin	2.36	13
12	Chặn, ngắt kết nối với đối tượng xấu	4.03	3
13	Nhờ chuyên gia hỗ trợ khi bị đánh cắp thông tin cá nhân, tài liệu	2.15	15
14	Báo cáo cho người, cơ quan chức năng có thẩm quyền sớm để giải quyết	3.63	7
15	Cảnh báo người thân, bạn bè khi bị đánh cắp email, tài khoản mạng xã hội	3.86	4
16	Quản lý lượt truy cập, theo dõi trên mạng xã hội, Internet	2.36	13
ĐTB chung		3.32	

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Tóm lại, tổng hợp kết quả khảo sát trên 03 phương diện về hành động cho thấy: biểu hiện mặt hành động của kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các Trường CAND phía Nam ở mức khá tốt với ĐTB chung là 3.64, cụ thể có 02 biểu hiện ở mức khá tích cực, 01 biểu hiện ở mức trung bình. Trong đó, mức độ thường xuyên tham gia các hoạt động nhằm rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet là tốt nhất; mức độ thường xuyên thực hiện các thao tác của kỹ năng bảo mật thông tin khi sử dụng Internet là hạn chế nhất (xem Bảng 15).

Bảng 15: Bảng tổng hợp kết quả về hành động

STT	Nội dung	ĐTB
1	Mức độ thường xuyên thực hiện các hoạt động có nguy cơ ảnh hưởng đến bảo mật thông tin trên Internet	3.54
2	Mức độ thường xuyên tham gia các hoạt động nhằm rèn luyện kỹ năng bảo mật thông tin khi sử dụng Internet	4.06
3	Mức độ thường xuyên thực hiện các thao tác của kỹ năng bảo mật thông tin khi sử dụng Internet	3.32
ĐTB chung		3.64

5. Kết luận và kiến nghị

5.1. Kết luận rút ra từ nghiên cứu

Tổng hợp kết quả khảo sát trên 3 phương diện nhận thức, thái độ và hành động cho thấy: Kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các Trường CAND phía Nam ở mức khá tích cực với ĐTB chung là 4.09, trong đó mặt thái độ của sinh viên là tốt nhất với ĐTB là 4.45 (ở mức rất tích cực); tiếp đến là biểu hiện mặt nhận thức với ĐTB là 4.19 và thấp nhất là biểu hiện mặt hành động với ĐTB là 4.09 (ở mức khá tích cực). Tuy nhiên, kết quả khảo sát cho thấy, nhận thức của sinh viên về một số kỹ năng bộ phận của kỹ năng bảo mật thông tin, nhận thức của sinh viên về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin ở mức trung bình; mức độ thực hiện các thao tác của kỹ năng bảo mật thông tin của sinh viên còn hạn chế (ở mức trung bình) và sinh viên vẫn còn thực hiện một số hành vi tiêu cực dễ dẫn đến nguy cơ lộ, lọt thông tin cá nhân, thông tin của lớp, Trường, của Ngành lên mạng Internet. Đây là những biểu hiện tiêu cực mà sinh viên cần khắc phục.

5.2. Kiến nghị

Để góp phần cải thiện kỹ năng bảo mật thông tin khi sử dụng Internet của sinh viên các trường CAND phía Nam, nhóm tác giả kiến nghị một số vấn đề sau:

- Về phía các Trường CAND phía Nam

Thứ nhất, đẩy mạnh hoạt động tuyên truyền, nâng cao nhận thức cho sinh viên về các yếu tố ảnh hưởng đến kỹ năng bảo mật thông tin cho sinh viên khi sử dụng Internet, tầm quan trọng của các thông tin cần bảo mật.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thứ hai, tổ chức các buổi báo cáo chuyên đề, tập huấn cho sinh viên về kỹ năng bảo mật thông tin, khi sử dụng Internet, nhất là cập nhật những phương thức, thủ đoạn hoạt động của các thế lực thù địch, bọn tội phạm thường sử dụng.

Thứ ba, các đơn vị trong Nhà trường cần mời những báo cáo viên, chuyên gia có kiến thức chuyên môn về an ninh mạng, kỹ năng bảo mật thông tin để báo cáo về tình trạng lộ, mất bí mật Nhà nước khi sử dụng Internet; hướng dẫn cho sinh viên các kỹ năng cơ bản để hạn chế tối đa nguy cơ lộ, lọt thông tin bí mật Nhà nước khi làm việc trên môi trường mạng.

Thứ tư, Khoa Ngoại ngữ - Tin học cần phát huy vai trò trong việc xây dựng nội dung chương trình, tổ chức tập huấn cho sinh viên về kỹ năng bảo mật thông tin, hướng dẫn các thủ thuật để bảo đảm an toàn thông tin khi sử dụng Internet cho sinh viên.

Thứ năm, xây dựng và duy trì hoạt động của câu lạc bộ ngoại ngữ, tin học, các hội, nhóm để giúp sinh viên có điều kiện tham gia, trao đổi, rèn luyện kỹ năng bảo mật thông tin.

- Về phía đội ngũ giảng viên và cán bộ quản lý

Đội ngũ giảng viên thông qua công tác giảng dạy đầy mạnh hơn nữa hoạt động tuyên truyền giáo dục, nâng cao nhận thức về bảo mật thông tin cho sinh viên. Cần huy vai trò của giảng viên Tin học trong việc trang bị cho sinh viên những kỹ năng, thủ thuật cần thiết nhằm bảo mật thông tin, hạn chế tình trạng lộ thông tin khi sử dụng Internet. Giáo viên chủ nhiệm cần phổ biến đầy đủ, kịp thời những quy định của Trường, của Ngành; tăng cường công tác kiểm tra, đôn đốc, nhắc nhở sinh viên chấp hành đúng những quy định về bảo mật; kịp thời phát hiện, ngăn chặn và xử lý những trường hợp vi phạm.

- Về phía sinh viên

Bản thân sinh viên cần tích cực tự giác nâng cao nhận thức, nắm vững những quy định của Trường, của Ngành về bảo mật thông tin; đề cao cảnh giác khi sử dụng Internet và chấp hành nghiêm túc những quy định về bảo mật thông tin; chủ động nhắc nhở đồng chí đồng đội cũng thực hiện và mạnh dạn lên án, đấu tranh với những hành vi vi phạm. Sinh viên là chủ thể quan trọng nhất trong quá trình bảo mật thông tin do vậy mỗi sinh viên phải nâng cao ý thức tự giác bảo mật khi sử dụng Internet, chấn chỉnh kịp thời những sai phạm của bản thân.

LỜI CẢM ƠN

Tác giả xin gửi lời cảm ơn chân thành và sâu sắc đến sự hỗ trợ nhiệt tình của các bạn sinh viên đến từ các Trường Đại học An ninh nhân dân, Trường Đại học Cảnh sát nhân dân và Trường Cao đẳng An ninh nhân dân II đã giúp tác giả hoàn thành phiếu khảo sát. Đồng thời, tác giả xin gửi lời cảm ơn lãnh đạo Khoa Tâm lý – Trường Đại học An ninh nhân dân đã tạo điều kiện cho tác giả hoàn thành tham luận một cách thuận lợi.

TÀI LIỆU THAM KHẢO

Tiếng Việt

Hội đồng quốc gia chỉ đạo biên soạn Từ điển bách khoa Việt Nam. (1995). *Từ điển Bách khoa Việt Nam tập 1*. Hà Nội: Trung tâm biên soạn Từ điển Bách khoa Việt Nam.

Nguyễn, N.Y. (1998). *Đại từ điển Tiếng Việt*. Hà Nội: Văn hóa thông tin.

Vũ, D. (2008). *Từ điển Tâm lý học*. Hà Nội: Khoa học xã hội.

Huỳnh, V. S. (2012). *Thực trạng kỹ năng giải quyết vấn đề của sinh viên Trường Đại học Sư phạm Thành phố Hồ Chí Minh trong thực tập sư phạm đợt một theo hình thức gửi thẳng*. Đề tài nghiên cứu khoa học và công nghệ cấp cơ sở. TP. Hồ Chí Minh: Trường Đại học Sư phạm Thành phố Hồ Chí Minh.

Tiếng Anh

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015, August). *Information security awareness in educational institution: An analysis of students' individual factors*. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 352-359). IEEE.

NHẬN DIỆN CÁC MỐI ĐE DỌA AN NINH ĐỐI VỚI SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

ThS. Hoàng Đức Nghi

Trường Đại học An ninh nhân dân

Tác giả liên hệ: hoangducnghi0510@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> mối đe dọa; an ninh; sinh viên; chuyển đổi số	Bài viết trình bày khái quát nhận thức, nội dung, mục tiêu chuyển đổi số trong giáo dục đại học. Trên cơ sở nghiên cứu thông tin, số liệu thực tế, một số vụ việc điển hình liên quan đến an ninh mạng và sinh viên, tác giả nhận diện, chỉ ra các mối đe dọa an ninh đối với sinh viên trong thời kỳ chuyển đổi số. Đồng thời, tác giả đưa ra một số ý kiến nghị đối với các cơ quan hữu quan góp phần bảo đảm an toàn, an ninh cho sinh viên trong thời kỳ chuyển đổi số.
<i>Keywords:</i> threat; security; student; digital transformation	ABSTRACT The article presents an overview of the awareness, content and goals of digital transformation in higher education. On the basis of researching informations, actual datas and typical cases related to cyber security and students, the author identifies and points out security threats to students during the period of digital transformation. At the same time, the author make a number of recommendations to relevant agencies to contribute to ensuring safety and security for students during the period of digital transformation.

1. Giới thiệu

Chuyển đổi số trong giáo dục, đặc biệt là trong giáo dục đại học là xu thế tất yếu của giai đoạn hiện nay. Cán bộ, giảng viên, sinh viên và hệ thống bộ máy các trường đại học, cao đẳng đều là những chủ thể tham gia vào quá trình chuyển đổi số. Bên cạnh những thay đổi mang tính tích cực giúp cho hoạt động giáo dục tại các trường đại học được diễn ra dễ dàng, thuận tiện, hiệu quả hơn so với phương thức truyền thống là dạy và học trực tiếp thì việc ứng dụng công nghệ kỹ thuật số và công nghệ thông tin Internet vào lĩnh vực giáo dục trong thời kỳ chuyển đổi số cũng đi kèm theo đó những mối đe dọa an ninh đối với hệ thống thông tin nhà trường, an ninh đội ngũ trí thức, an ninh sinh viên. Trong bài viết này, trên cơ sở trình bày nhận thức về nội dung, mục tiêu chuyển

đổi số trong giáo dục đại học, cơ hội từ quá trình chuyển đổi số mang lại, tác giả đồng thời nhận diện, chỉ ra các mối đe dọa an ninh đối với sinh viên. Qua đó, đưa ra một số ý kiến đối với các cơ quan hữu quan góp phần bảo đảm an toàn, an ninh cho sinh viên trong thời kỳ chuyển đổi số.

2. Cơ sở lý thuyết

Bài viết nghiên cứu dựa trên lý thuyết bảo vệ an ninh quốc gia, đảm bảo an ninh mạng, an ninh thông tin của lực lượng Công an nhân dân.

3. Kết quả nghiên cứu

- Nhận thức về chuyển đổi số trong giáo dục đại học

Cuộc cách mạng Công nghiệp lần thứ tư đánh dấu sự phát triển vượt bậc của khoa học, kỹ thuật, công nghệ. Tất cả các ngành, các lĩnh vực của bất kỳ quốc gia nào trên thế giới đều phải thực hiện chuyển đổi số để khai thác triệt để thành tựu của cuộc cách mạng này góp phần nâng cao năng lực, hiệu lực, hiệu quả quản trị, nâng cao chất lượng hoạt động phục vụ cho sự phát triển của đất nước. Ở Việt Nam, chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 được Thủ tướng Chính phủ phê duyệt đã thúc đẩy các ngành, các lĩnh vực chuyển mình, vươn lên mạnh mẽ để tận dụng cơ hội do cuộc cách mạng Công nghiệp lần thứ tư mang lại. Ngành giáo dục, đào tạo không thể nằm ngoài xu thế chung của cả nước.

Theo Bộ Thông tin và Truyền thông định nghĩa: “Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số” [1]. Đối với giáo dục đại học, chuyển đổi số là một phần tất yếu trong quá trình đổi mới, nâng cao chất lượng giáo dục. Chuyển đổi số trong giáo dục đại học hướng đến hai nội dung chính: (i) chuyển đổi số trong quản lý giáo dục và (ii) chuyển đổi số trong dạy, học, đánh giá và nghiên cứu khoa học. Trong quản lý giáo dục, chuyển đổi số bao gồm các bước: số hóa thông tin quản lý, tạo ra những hệ thống cơ sở dữ liệu lớn liên thông, chia sẻ; triển khai các dịch vụ công trực tuyến, ứng dụng các Công nghệ 4.0 (AI, blockchain, phân tích dữ liệu...) để quản lý, điều hành, dự báo, hỗ trợ ra quyết định trong ngành giáo dục, đào tạo một cách nhanh chóng, chính xác. Trong dạy, học, đánh giá, nghiên cứu khoa học, chuyển đổi số được triển khai từ việc số hóa học liệu (sách giáo khoa điện tử, bài giảng điện tử, kho bài giảng e-learning, ngân hàng câu hỏi thi tự luận, trắc nghiệm...), xây dựng thư viện số, phòng thí nghiệm ảo, đến việc triển khai, vận hành hệ thống đào tạo trực tuyến, thực tế ảo, trường đại học ảo... Để hiện thực hóa các nội dung trên, chuyển đổi số trong giáo dục đại học hướng đến ba mục tiêu chính: (i) phát triển nền tảng hỗ trợ dạy và học từ xa, ứng dụng triệt để công nghệ số trong công tác quản lý, giảng dạy và học tập, (ii) xây dựng nền tảng chia sẻ tài nguyên giảng dạy và học tập theo cả hình thức trực tuyến và trực tiếp và (iii) phát triển công nghệ phục vụ giáo dục, hướng tới đào tạo cá thể hóa [1].

Về bản chất, chuyển đổi số không làm thay đổi mô hình hoạt động của cơ sở giáo dục mà đó là quá trình ứng dụng công nghệ kỹ thuật số và hệ thống thông tin Internet vào cơ sở giáo dục để nâng cao chất lượng dạy, học và quản lý giáo dục.

Chuyển đổi số trong lĩnh vực giáo dục đại học vừa là cơ hội, đồng thời cũng là thách thức đối với thanh niên, sinh viên. Trong thời kỳ chuyển đổi số, thanh niên, sinh viên vừa là chủ thể vừa là đối tượng thụ hưởng và chịu tác động đa chiều. Sinh viên là lực lượng nòng cốt, đi đầu trong thời kỳ chuyển đổi số bởi: (i) nhóm tuổi này có khả năng tiếp cận với công nghệ mới, thông tin mới trên Internet và sử dụng Internet nhiều hơn các nhóm tuổi khác (độ tuổi từ 20 – 24 tuổi, chiếm hơn ¼ dân số); (ii) họ là lớp người năng động, sáng tạo, được sự định hướng từ gia đình và xã hội nên có ý thức chủ động, tích cực trong việc chuẩn bị hàng trang cho tương lai của mình; (iii) ngành khoa học, công nghệ là sự lựa chọn hấp dẫn đối với một bộ phận thanh niên, sinh viên hiện nay. Họ có năng lực, chuyên môn, nghề nghiệp, ngoại ngữ... là những yếu tố quan trọng giúp họ đáp ứng đủ và kịp thời nhu cầu của thị trường lao động trong chuyển đổi số. Trong quá trình học tập, sinh viên có thêm nhiều cách thức, điều kiện để tiếp cận thông tin, kiến thức dễ dàng, rút ngắn về khoảng cách, thu hẹp về không gian và thời gian, tham gia các lớp học trực tuyến, từ xa, lớp học ảo và có cơ hội trải nghiệm môi trường học tập mới bằng không gian ảo, tương tác thông qua các phần mềm mô phỏng công nghệ thực tế ảo... Do vậy, trong thời kỳ chuyển đổi số trong lĩnh vực giáo dục đại học, sinh viên có thể tích lũy nhiều lợi ích vô cùng to lớn cho tương lai của mình.

- Nhận diện mối đe dọa an ninh đối với sinh viên trong thời kỳ chuyển đổi số

Để bảo vệ an ninh, an toàn cho sinh viên, bảo vệ sự ổn định, hoạt động bình thường và phát triển bền vững của lĩnh vực giáo dục, đào tạo trong thời kỳ chuyển đổi số, cần thiết phải nhận diện các mối đe dọa gây mất an toàn, an ninh sinh viên.

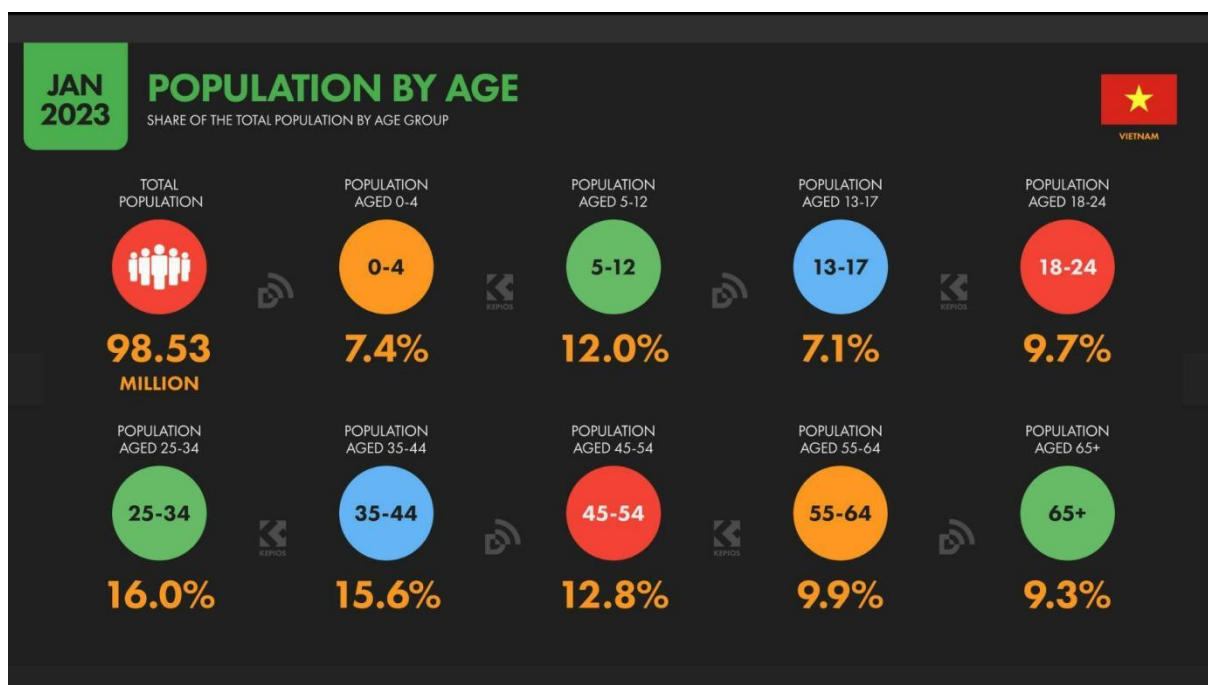
Một là, mối đe dọa gây mất an ninh, an toàn thông tin, dữ liệu cá nhân

Trong thời kỳ chuyển đổi số, dữ liệu số là cốt lõi của hầu hết các hoạt động trong các cơ sở giáo dục, chúng gắn liền với việc đảm bảo bộ máy nhà trường vận hành trơn tru, hiệu quả. Hệ thống các thông tin, dữ liệu gồm: Thông tin về chương trình đào tạo, giảng dạy, giáo trình, công trình nghiên cứu khoa học của giảng viên, sinh viên; thông tin cá nhân của cán bộ, giảng viên, nhân viên, sinh viên; thông tin, số liệu tài chính, kế toán, vật tư, trang thiết bị... được số hóa, lưu trữ tập trung thành nguồn dữ liệu lớn và được quản lý bằng công nghệ điện toán đám mây cho phép nhà trường và người dùng có thể được truy cập tìm kiếm thông tin theo yêu cầu bất kể thời gian và không gian [3]. Nguồn thông tin, dữ liệu đa dạng, bao gồm cả những thông tin có tính riêng tư như thông tin cá nhân (họ tên, hình ảnh, số định danh cá nhân, số điện thoại, địa chỉ cư trú, tài khoản email, mạng xã hội, tài khoản ngân hàng...) của sinh viên, giảng viên, nhân viên hay thông tin có tính nhạy cảm, quan trọng trong hoạt động của nhà trường như số liệu tài chính, kế toán,

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

hồ sơ học tập, hồ sơ cán bộ, công chức, viên chức, giáo trình, giáo án, công trình nghiên cứu khoa học... là loại thông tin luôn bị các đối tượng xấu quan tâm, chú ý, tìm cách thu thập, khai thác, sử dụng vào mục đích không chính đáng, dễ dẫn đến hậu quả không thể lường trước.

Với các cơ sở giáo dục đại học, mặc dù đã quan tâm và đầu tư, song cơ sở vật chất, hạ tầng mạng, trang thiết bị, đường truyền, dịch vụ Internet, cơ chế và biện pháp kỹ thuật đảm bảo an ninh, an toàn thông tin... nói chung còn thiếu, chưa đồng bộ, nhiều nơi chưa đáp ứng yêu cầu cho chuyển đổi số. Trong khi đó, các đối tượng xấu hàng ngày, hàng giờ đang sử dụng ưu thế khoa học công nghệ để tiến hành tấn công, thu thập, phá hoại cơ sở dữ liệu của nhà trường. Phương thức, thủ đoạn hoạt động của họ có thể kể đến như: thiết kế mã độc, có chủ đích nhằm vào nguồn dữ liệu của nhà trường; tấn công và chiếm quyền quản trị các máy chủ quản trị, máy chủ bảo mật trong hệ thống



thông tin nhà trường; khai thác triệt để các điểm yếu, lỗ hổng bảo mật để đánh cắp thông tin, tài liệu, dữ liệu của cán bộ, giảng viên, sinh viên nhà trường.

Hình 1. Phân loại dân số sử dụng Internet theo độ tuổi năm 2023

Nguồn: Vnetwork (2023), “Xu hướng phát triển Internet Việt Nam 2023”, từ website <https://www.vnetwork.vn/news/internet-viet-nam-2023-so-lieu-moi-nhat-va-xu-huong-phat-trien/>

Với sinh viên, khi họ sử dụng máy tính, điện thoại thông minh kết nối Internet, truy cập mạng xã hội phục vụ cho việc học tập, giải trí càng nhiều thì nguy cơ đối diện với mối đe dọa an ninh, an toàn thông tin càng lớn [5]. Rủi ro không chỉ đến từ mức độ an ninh, an toàn hệ thống thông tin của nhà trường mà rủi ro còn nảy sinh từ chính hành vi trên không gian mạng của sinh viên. Sinh viên có thể gặp rủi ro mất thông tin cá nhân, bao gồm thông tin ngân hàng, thông tin đăng nhập tài khoản, thông tin căn cước công

dân... Sinh viên có thể bị mất dữ liệu quan trọng như hình ảnh, tài liệu nghiên cứu, học tập... lưu trữ trong thiết bị điện tử dùng để kết nối Internet. Sinh viên cũng có thể bị tin tặc tấn công, xâm nhập chiếm quyền sử dụng các tài khoản mạng xã hội, email, danh bạ, tin nhắn... Những thông tin này có thể do nhà trường, sinh viên vô tình làm lộ hoặc sử dụng không đúng cách, gây ảnh hưởng đến quyền riêng tư của người khác; thông tin có thể do sinh viên mất kiểm soát hoặc không chú ý theo dõi sau khi chia sẻ lên không gian mạng dẫn đến việc không thể xóa bỏ, chỉnh sửa; thông tin có thể bị rò rỉ hoặc bị đối tượng xấu cố tình chiếm đoạt, đánh cắp vượt ra ngoài khả năng kiểm soát của sinh viên... Một khi những thông tin nhạy cảm này lọt vào tay đối tượng xấu, với số lượng rất lớn, họ có thể sử dụng vào mục đích thực hiện các hành vi lừa đảo, quảng cáo, tiếp thị việc làm, đe dọa, khống chế để trục lợi... làm ảnh hưởng trực tiếp đến đời sống của sinh viên.

Theo thông tin Ban Cơ yếu Chính phủ, vào tháng 8/2021 phát hiện tài khoản có tên xiaolin1983 đã đăng bán dữ liệu của hơn 300.000 sinh viên được cho là của 10 trường đại học tại Việt Nam bao gồm họ tên đầy đủ, địa chỉ, số điện thoại, tài khoản ngân hàng, hình ảnh chứng minh nhân dân, hộ chiếu, khóa học, lớp học được đăng tải trên diễn đàn Raidforums [6]. Trung tâm Giám sát An toàn Không gian mạng Quốc gia (NCSC) đánh giá những thông tin này có thể được sử dụng với mục đích thực hiện các hành vi lừa đảo, quảng cáo... và khuyến cáo người dùng phải thận trọng với thông tin cá nhân, không chia sẻ, cung cấp thông tin cá nhân cho những cá nhân, tổ chức chưa rõ uy tín hoặc đáng ngờ. Qua đây có thể thấy, với những thông tin tương chừng như “không thể tạo ra giá trị” của sinh viên, của nhà trường nhưng một khi bị rơi vào tay của đối tượng xấu, họ có thể sử dụng nó vào mục đích không chính đáng, hay trục lợi từ nó. Khi đối tượng xấu tiến hành cuộc tấn công mạng nhằm vào hệ thống thông tin, cơ sở hạ tầng kỹ thuật của nhà trường có thể gây tê liệt, gián đoạn hoạt động bình thường của nhà trường. Trong trường hợp, vì nguyên nhân chủ quan, thiếu trách nhiệm của nhà trường hay cố tình làm lộ, mất, mua bán dữ liệu. Điều này có thể sẽ khiến cơ sở giáo dục bị liên đới truy cứu trách nhiệm, xử phạt, bồi thường thiệt hại về kinh tế và đối diện với nguy cơ truy tố trước pháp luật.

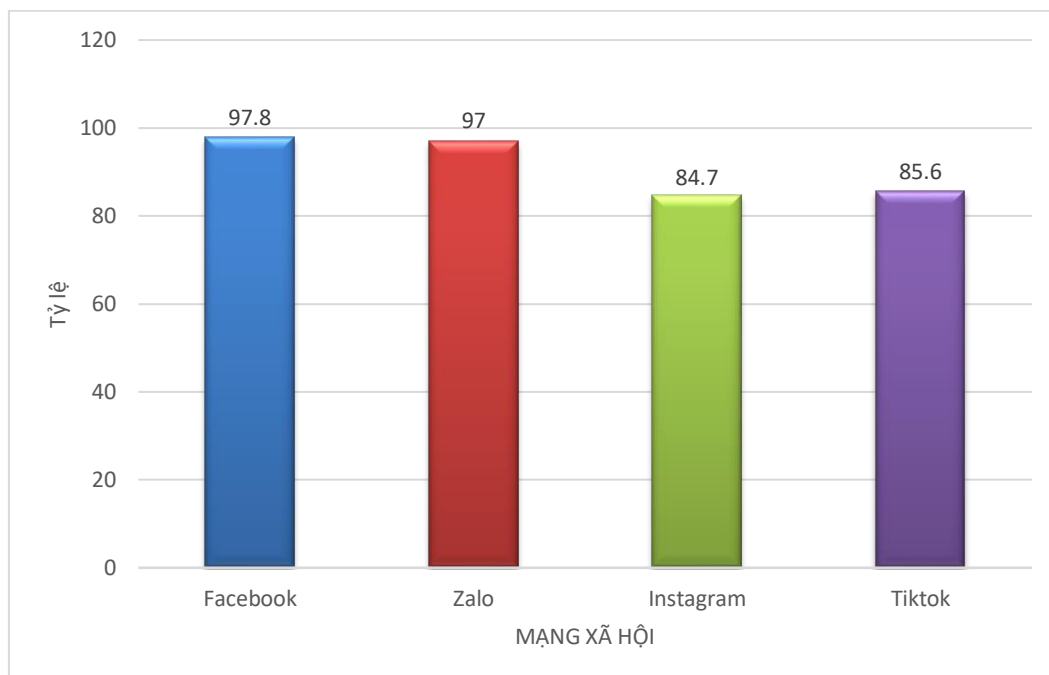
Mối đe dọa về mất an ninh, an toàn hệ thống thông tin của nhà trường, an toàn dữ liệu cá nhân của sinh viên là nguy cơ thường trực, đe dọa trực tiếp, thậm chí gây ra hậu quả rất nghiêm trọng đối với an ninh sinh viên nếu như cơ sở giáo dục không có giải pháp bảo đảm an ninh mạng đồng bộ với quá trình chuyển đổi số.

Hai là, mối đe dọa gây mất an ninh văn hóa

Trong quá trình chuyển đổi số, các cơ sở giáo dục tổ chức hoạt động quản lý và học tập cho sinh viên bằng việc khai thác không gian mạng với nhiều nội dung, hình thức khác nhau. Sinh viên tham gia học tập, nghiên cứu khoa học hầu hết thông qua các thiết bị điện tử có kết nối Internet. Trong phần lớn thời gian sử dụng Internet, sinh viên

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

khai thác và sử dụng Internet để phục vụ những nhu cầu, mục đích khác nhau như tìm kiếm tri thức, cập nhật thông tin kinh tế, chính trị, văn hóa, xã hội và tìm kiếm cơ hội việc làm hay giao lưu văn hóa, giao tiếp xã hội, giải trí...



Hình 2: Khảo sát sinh viên sử dụng mạng xã hội.

Nguồn: TPO (2023), “Hơn 85% sinh viên được khảo sát lên mạng xã hội hàng ngày với mục đích gì”, từ website <https://doanthanhvien.vn/tin-tuc/hoi-sinh-vien-viet-nam/hon-85-sinh-vien-duoc-khao-sat-len-mang-xa-hoi-hang-ngay-voi-muc-dich-gi>

Sinh viên hiện nay dành nhiều sự quan tâm cho các vấn đề chính trị, kinh tế, văn hóa, xã hội, có quan điểm và hành động phù hợp trước những vấn đề liên quan đến an ninh quốc gia. Sinh viên cũng đã có ý thức về việc tìm hiểu kiến thức về các lĩnh vực này để phục vụ cho quá trình học tập và mọi mặt đời sống của họ. Bởi lẽ, thông tin này thường được chia sẻ rộng rãi trên Internet, mạng xã hội, thu hút sự chú ý của phần đông dư luận và tác động nhất định đến đời sống ở hiện tại và tương lai của họ [2]. Tuy nhiên, cách tiếp cận với loại thông tin này còn rất thụ động. Thay vì chủ động tiếp cận, tìm hiểu thông tin từ các nguồn tin chính thức trên truyền hình, báo chí, thì hiện nay phần lớn sinh viên tìm đọc thông tin qua những bài viết được chia sẻ trên Internet, mạng xã hội chưa được kiểm chứng cụ thể. Trên Internet, mạng xã hội hiện nay ngập tràn tin giả, tin sai sự thật. Theo chương trình đánh giá an ninh mạng từ BKAV thống kê cho thấy, 63% người dùng thường xuyên đọc được tin tức giả mạo trên Facebook, trong đó có 40% là nạn nhân hàng ngày [4]. Sinh viên cũng không nằm ngoài con số này. Tin giả, tin sai sự thật không chỉ khiến người đọc hoang mang mà nó còn tạo nguy cơ gây bất ổn xã hội khi kẻ xấu cố tình đưa tin sai sự thật về tình hình kinh tế, chính trị, dẫn dắt người xem theo dòng dư luận tiêu cực. Điều này hiện hữu nguy cơ tạo ra hệ lụy không tốt cho

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

sự phát triển của nhận thức vốn còn chưa đầy đủ của sinh viên, ảnh hưởng tiêu cực đến thái độ, tình cảm, hành vi của họ, dẫn đến việc họ có những bình luận, lời nói, việc làm trái với chuẩn mực đạo đức, văn hóa và pháp luật.

Thực tế thời gian gần đây, văn hóa ứng xử trên không gian mạng, văn hóa ứng xử trong môi trường giáo dục đang là vấn đề đáng báo động, cần sự quan tâm sâu sát của nhà trường, gia đình và xã hội. Theo khảo sát của Microsoft, Việt Nam nằm trong top 5 quốc gia có chỉ số mức độ văn minh thấp nhất trên không gian mạng (DCI). Nếu tìm kiếm từ khóa “ứng xử kém văn minh” thì ngay lập tức kết quả trả về trên Google là 17.400.000 trong vòng 0,36 giây. Trong sinh viên vẫn còn tồn tại một bộ phận không nhỏ có biểu hiện tiêu cực về tư tưởng, chính trị, đạo đức lối sống khi có những phát ngôn, bình luận “thiếu văn hóa”, không phù hợp với đạo đức, thuần phong mỹ tục của dân tộc Việt Nam. Một bộ phận sinh viên bị lôi kéo vào xu hướng sính ngoại, trào lưu video ngắn có nội dung nhảm nhí, học đòi lối sống xa hoa, hưởng thụ. Một bộ phận sinh viên không có định hướng lý tưởng, có thái độ vô cảm với chính trị, xã hội, thiếu trách nhiệm với cộng đồng; họ có biểu hiện né tránh những việc ảnh hưởng đến lợi ích cá nhân, chỉ quan tâm đến lợi ích cá nhân mà quên đi lợi ích tập thể, quên đi vinh dự và trách nhiệm, tinh thần đoàn kết, tập thể cao trong học tập, công tác, rèn luyện. Nguy hại hơn, nó có thể dẫn đến sự bi quan, mất niềm tin khi gặp phải những khó khăn trong cuộc sống, tự chuyển hóa thành nhận thức lệch lạc, suy nghĩ bông bột dẫn đến những kết cục đáng tiếc đối với bản thân, gia đình và xã hội.

Ba là, mối đe dọa gây mất an ninh giáo dục, đào tạo

Trong thời kỳ thực hiện chuyển đổi số, sinh viên là chủ thể trực tiếp truy cập, tham gia vào hệ thống thông tin của nhà trường. Họ được cấp tài khoản truy cập cá nhân và thực hiện toàn bộ thao tác trên hệ thống. Tuy nhiên nếu không biết cách sử dụng an toàn, hiệu quả, chủ động xử lý sự cố sẽ rất dễ gây ảnh hưởng xấu đến hệ thống thông tin nhà trường.

Sinh viên có thể vô tình hoặc cố ý chia sẻ thông tin tài khoản, bị đối tượng xấu sử dụng truy cập trái phép vào phần thông tin cá nhân, khai thác, làm lộ thông tin điểm số, hồ sơ học tập và các thông tin nhạy cảm khác. Sinh viên có thể tò mò, cố gắng tìm cách truy cập vào các phần của hệ thống thông tin không được phép truy cập, gây ra sự cố bảo mật và gây thiệt hại cho hệ thống thông tin nhà trường. Sinh viên cũng có thể thử sửa đổi hoặc xóa dữ liệu trong hệ thống thông tin, gây sự cố nghẽn mạng hoặc mất mát dữ liệu quan trọng. Sinh viên có thể lợi dụng thông tin từ hệ thống để thực hiện các hành vi gian lận trong quá trình học tập hoặc thi cử như xem đề thi trước, sửa đổi kết quả điểm thi... Việc tò mò, truy cập trái phép vào hệ thống thông tin nhà trường hoặc thực hiện bất kỳ hành vi vi phạm nào khác đều là hành vi vi phạm pháp luật và quy định của nhà trường, đe dọa đến sự an toàn, ổn định và hoạt động bình thường của nhà trường.

Ngoài ra, sự phát triển của trí tuệ nhân tạo đã hình thành, hoàn thiện các công cụ hỏi đáp tự động được tích hợp trí tuệ nhân tạo như ChatGPT, Notion AI, Bing AI Chatbot... cũng là mối nguy cơ đe dọa đến sự phát triển của sinh viên và ngành giáo dục khi đây sẽ là “con dao hai lưỡi” thách thức đối với an ninh giáo dục. Với công cụ hỏi đáp tự động, sinh viên có thể sử dụng để gian lận và giáo viên sẽ gặp khó khăn trong việc đánh giá năng lực của sinh viên. Việc lạm dụng công cụ hỏi đáp tự động sẽ dễ làm cho sinh viên lười suy nghĩ, ngại tư duy, phụ thuộc hoàn toàn vào ứng dụng AI, làm mất dần khả năng tư duy khoa học, tư duy phản biện và động lực học tập tích cực.

Bốn là, mối đe dọa gây mất an ninh tư tưởng, an ninh chính trị, trật tự xã hội

Trong mọi thời kỳ, ở mọi chế độ, ở tất cả các quốc gia, sinh viên luôn là đối tượng quan trọng để hướng đến tác động, lôi kéo của các thế lực thù địch, phản động nhằm thực hiện mưu đồ chính trị của chúng. Các thế lực thù địch luôn muốn xây dựng những nhân tố, điều kiện cho việc thực hiện mục xóa bỏ nhà nước xã hội chủ nghĩa, hướng các nước xã hội chủ nghĩa như Việt Nam đi theo quỹ đạo của chủ nghĩa tư bản. Do vậy, chúng đặc biệt chú ý và gửi gắm “mong muốn” này vào thế hệ trẻ, thanh niên, sinh viên. Trong bối cảnh chuyển đổi số, ý đồ trên càng được các thế lực thù địch tiến hành dễ dàng hơn với ưu thế vượt trội về công nghệ thông tin.

Lợi dụng sự phát triển của công nghệ thông tin, Internet, các thế lực thù địch bên ngoài tích cực đăng tải, tuyên truyền, tán phát nhiều nội dung xấu, độc, chống Đảng, Nhà nước. Họ đã lập các diễn đàn, website, blog trên mạng Internet, lợi dụng mạng xã hội để tổ chức hội thảo, tổ chức chiến dịch tuyên truyền dưới dạng hội luận, cuộc thi tìm hiểu trực tuyến... Thông qua đó, họ tuyên truyền các luận điệu phản động, phản bác chủ nghĩa Mác – Lênin, tư tưởng Hồ Chí Minh, vai trò lãnh đạo của Đảng Cộng sản Việt Nam, phủ nhận thành quả cách mạng của nhân dân ta. Họ triệt để lợi dụng những vấn đề tiêu cực, phức tạp trong xã hội, nhất là tình trạng tiêu cực, tham nhũng của cán bộ, đảng viên; mâu thuẫn, khiếu kiện đông người; những hoạt động tôn giáo, tâm linh; việc thực hiện chế độ, chính sách liên quan đến thanh niên, sinh viên... Họ tuyên truyền hệ tư tưởng tư sản, cổ súy các “giá trị” của “văn minh”, “văn hóa”, khuếch trương cái gọi là “tự do ngôn luận”, “tự do báo chí” của phương Tây. Bằng cách khéo léo lồng ghép những vấn đề lập lờ, thật – giả, trắng – đen lẫn lộn vào bài viết, video, bài tham luận hội nghị, diễn đàn... trên Internet, họ kích thích tâm lý tò mò, hiệu ứng đám đông, khuyến khích sinh viên trao đổi, thu nhận thông tin, bày tỏ quan điểm cực đoan, làm “nóng” các vấn đề xã hội. Mục đích của họ là kích động tư tưởng chống đối, gây mâu thuẫn, chia rẽ, tạo sự mơ hồ, hoang mang dao động trong các tầng lớp nhân dân, nhất là tầng lớp trí thức, thanh niên, sinh viên; gieo rắc nhận thức sai lầm, kích động trạng thái tâm lý “quá khích”, ngấm ngấm kích động tư tưởng bất tuân, chống đối pháp luật, chuẩn mực xã

hội; xúi giục sinh viên thực hiện các hành vi bạo loạn, bạo lực, làm cơ sở cho những vụ gây rối trật tự an ninh trong đời sống sinh viên và trong xã hội.

Thời gian qua, liên quan tới việc xử lý các vụ việc phức tạp về an ninh, trật tự, Bộ Công an đã ghi nhận sự tham gia của hàng trăm sinh viên vào các đợt biểu tình trên cả nước để phản ứng về các vấn đề xã hội “nhảy cảm”, làm giảm uy tín của Đảng, Nhà nước ta như lợi dụng sự kiện Trung Quốc hạ đặt giàn khoan Hải Dương 981 trong vùng biển Việt Nam; vấn đề chủ quyền biển đảo của Việt Nam ở Hoàng Sa, Trường Sa; vụ ô nhiễm môi trường do hoạt động xả thải của Công ty Formosa (Hà Tĩnh) làm cá chết hàng loạt ở các tỉnh ven biển miền Trung... Phát hiện sinh viên là thành viên của các tổ chức phản động, tham gia vào các hội, nhóm trái pháp luật, hoạt động mang màu sắc “cách mạng màu”, thậm chí Bộ Công an đã phát hiện và xử lý hàng chục sinh viên có hành vi vi phạm pháp luật nghiêm trọng liên quan đến an ninh quốc gia.

4. Kiến nghị giải pháp góp phần bảo đảm an ninh sinh viên trong thời kỳ chuyển đổi số

Từ trước đến nay, hoạt động tuyên truyền, phá hoại tư tưởng đối với sinh viên, tác động chuyển hóa nội bộ ta thông qua lĩnh vực giáo dục, đào tạo của các thế lực thù địch dù có tinh vi, xảo quyệt đến đâu thì ý đồ đó vẫn chưa bao giờ thay đổi. Nó nằm trong chuỗi các hoạt động chống phá, thúc đẩy “tự diễn biến”, “tự chuyển hóa” trong nội bộ của các thế lực thù địch đối với Việt Nam. Thanh niên, sinh viên, với đặc điểm tâm lý đặc thù của lớp người trẻ bị lôi cuốn vào “làn sóng” thông tin tuyên truyền của các thế lực thù địch trên không gian mạng, qua đó giúp họ đạt được ý đồ chống phá. Trong khi đó, chuyển đổi số là quá trình có mối quan hệ chặt chẽ với hoạt động diễn ra trên không gian mạng. Do vậy, nhận diện nguy cơ đe dọa an ninh sinh viên trong thời kỳ chuyển đổi số thực sự cần thiết. Để góp phần đảm bảo an ninh sinh viên trong thời kỳ chuyển đổi số, đòi hỏi phải có sự chung tay vào cuộc của các cơ quan hữu quan, các ban, ngành, nhà trường và cả cán bộ, giảng viên, sinh viên, trong đó trách nhiệm chính thuộc về các cơ sở giáo dục, cơ quan An ninh đóng vai trò nòng cốt.

Một là, cơ sở giáo dục cần xây dựng, bổ sung, hoàn thiện quy định quản lý hoạt động trên Internet, mạng xã hội, bộ quy tắc ứng xử trong nhà trường và trên không gian mạng.

Hiện nay, quy định của pháp luật về việc quản lý và sử dụng không gian mạng tương đối đầy đủ, chặt chẽ, có tính răn đe, phòng ngừa những hành vi vi phạm pháp luật về an ninh mạng¹. Trên cơ sở quy định của pháp luật, các cơ sở giáo dục cần xác định nội dung cụ thể đối với hành vi sử dụng không gian mạng và ban hành quy chế quản lý

¹ Nghị định 72/2013/NĐ-CP ngày 15/7/2013 về Quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng; Luật An ninh mạng năm 2018; Nghị định số 15/2020/NĐ-CP quy định xử phạt hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử; Bộ Quy tắc ứng xử trên mạng xã hội của Bộ Thông tin và Truyền thông...

đối với hoạt động sử dụng không gian mạng đối với cán bộ, giảng viên, sinh viên như về hành vi, thái độ, bình luận được phép, được khuyến khích trên không gian mạng; những hành vi ứng xử phù hợp với giá trị đạo đức, văn hóa truyền thống của dân tộc Việt Nam; những bình luận cần sử dụng ngôn từ phù hợp, không gây chia rẽ, mất đoàn kết và ảnh hưởng đến danh dự, nhân phẩm cá nhân hay tổ chức... Cần đưa vào quy chế những hành vi không được phép như: sử dụng ngôn từ phản cảm, tung tin giả, xuyên tạc, kích động, gây hoang mang dư luận xã hội... cùng với đó là những hình thức kỷ luật tương xứng. Những biện pháp xử lý đủ mạnh sẽ mang tính chất răn đe, kịp thời ngăn chặn những hành vi, thái độ và bình luận “thiếu chuẩn mực” trên không gian mạng làm ảnh hưởng đến uy tín, danh dự của cá nhân, đơn vị trong nhà trường. Các cơ sở giáo dục cần có cơ chế kiểm tra, giám sát phù hợp để kịp thời ngăn ngừa những hành vi tiêu cực trên không gian mạng của sinh viên. Ngoài ra, trong quá trình chuyển đổi số, các cơ sở giáo dục cần phải xây dựng quy tắc ứng xử văn minh trong nhà trường và trên không gian mạng trên cơ sở Bộ Quy tắc ứng xử trên mạng xã hội và Cẩm nang chuyển đổi số của Bộ Thông tin và Truyền thông, Quy định về việc sử dụng trang thông tin điện tử cá nhân trên Internet, mạng xã hội của Bộ Chính trị. Từ đó, xây dựng văn hóa làm việc từ xa thay cho văn hóa làm việc trực tiếp như truyền thống; xây dựng văn hóa học tập suốt đời, thúc đẩy sự liên chính về học thuật khi mà các dữ liệu được khai thác dễ dàng qua Internet.

Hai là, cơ sở giáo dục cần tăng cường tuyên truyền, phổ biến pháp luật về an ninh mạng lồng ghép với công tác giáo dục chính trị, tư tưởng cho sinh viên

Trong thời kỳ chuyển đổi số, hoạt động thông tin tuyên truyền, giáo dục chính trị, tư tưởng phải hướng đến mục tiêu không ngừng nâng cao nhận thức, bồi dưỡng bản lĩnh chính trị, lập trường tư tưởng cách mạng, tinh thần cảnh giác, thái độ chuẩn mực, hành vi đúng đắn khi tham gia vào môi trường không gian mạng cho sinh viên. Sinh viên cần được hướng dẫn về việc bảo vệ thông tin cá nhân, nhận diện các email, tin nhắn hoặc trang web giả mạo và biết cách xử lý khi gặp các sự cố, tình huống nguy hiểm trong quá trình tham gia vào không gian mạng. Sinh viên nên sử dụng mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Đồng thời, khuyến khích sinh viên sử dụng các công cụ quản lý mật khẩu để tạo và lưu trữ mật khẩu an toàn. Sinh viên nên đảm bảo rằng các thiết bị của mình luôn được cập nhật mới nhất, sử dụng các phiên bản cập nhật bảo mật mới nhất có thể giúp ngăn chặn các lỗ hổng bảo mật và nguy cơ tấn công mạng. Trước khi sử dụng các ứng dụng hoặc trang web mới, sinh viên nên kiểm tra tính bảo mật, tính tin cậy của chúng. Muốn vậy, công tác tuyên truyền, phổ biến pháp luật về an ninh mạng cần được các cơ sở giáo dục triển khai thường xuyên, có kế hoạch cụ thể bám sát nội dung và nhiệm vụ trọng tâm trong chiến lược tuyên truyền, phổ biến, giáo dục pháp luật của Đảng, Nhà nước và Chính phủ. Đồng thời, cần phát huy vai trò xung kích của tổ chức Đoàn Thanh niên, Hội Phụ nữ trong việc huy

động đông đảo thanh niên, sinh viên tham gia tự học tập, bồi dưỡng, nâng cao trình độ pháp luật về an ninh mạng, giúp họ hiểu rằng kiến thức pháp luật sẽ đem lại cho bản thân hành trang quan trọng để phục vụ ngày càng tốt hơn cho thực tiễn công tác sau này. Bên cạnh đó, các cơ sở giáo dục cũng cần phối hợp với cơ quan An ninh để tăng cường tuyên truyền, giáo dục cho sinh viên nhận thức rõ âm mưu của các thế lực thù địch trong sử dụng mạng truyền thông để tác động tâm lý sinh viên; làm rõ các thủ đoạn đã, đang và sẽ được các thế lực thù địch sử dụng để lôi kéo, kích động sinh viên; khuyến cáo sinh viên cảnh giác trước thông tin xuyên tạc, dụ dỗ, kích động, lôi kéo trên các trang mạng xã hội, Internet. Lấy kết quả của công tác giáo dục chính trị, tư tưởng làm cơ sở cho việc nâng cao hiệu quả công tác giáo dục pháp luật và hình thành ý thức pháp luật tích cực, vững chắc cho sinh viên trước tác động đa chiều của chuyển đổi số.

Ba là, cơ sở giáo dục cần định hướng tiếp nhận và sử dụng thông tin từ các phương tiện truyền thông đại chúng cho sinh viên

Trong định hướng tiếp nhận và sử dụng thông tin, cơ sở giáo dục sẽ gặp và cần khắc phục cả hai chiều hướng: (i) tránh làm nhiều loạn thông tin, làm cho sinh viên mất định hướng và (ii) chủ quan, tạo ra khoảng trống thông tin, bỏ trống trận địa tư tưởng cho kẻ địch chiếm lĩnh từ đó gây mất ổn định về tư tưởng, mở đường cho mất ổn định về chính trị - xã hội. Để định hướng tiếp nhận và sử dụng thông tin từ các phương tiện truyền thông, cơ sở giáo dục cần tăng cường khả năng tự kiểm soát và sử dụng thông tin từ Internet, mạng xã hội cho sinh viên. Khi tham gia vào môi trường mạng, sinh viên cần được định hướng lan tỏa những thông tin, hình ảnh tốt đẹp về các hoạt động xã hội, hoạt động vì cộng đồng, phê phán những thói xấu, biểu hiện lệch lạc, hướng tới xây dựng văn hóa ứng xử văn minh trên mạng xã hội. Sinh viên không sử dụng ngôn từ tục tĩu, lai căng văn hóa, có tính bạo lực; không được đăng thông tin bịa đặt, tán phát thông tin không rõ nguồn gốc, chưa được kiểm chứng, thông tin vi phạm pháp luật; không lập và tham gia các hội, nhóm để nói xấu, bôi nhọ, xúc phạm người khác hoặc công kích lẫn nhau; không “a dua” theo đám đông khi chưa hiểu rõ về vụ việc hoặc không có căn cứ. Sinh viên cần nắm rõ và tuân thủ các quy định của Luật An ninh mạng, biến cuộc sống trên môi trường mạng thành một môi trường lành mạnh, thể hiện tinh thần trách nhiệm cộng đồng, kịp thời phát hiện, góp ý, phê bình, phản bác những thông tin xấu độc, chống Đảng, Nhà nước trên không gian mạng. Chủ động nâng cao “sức đề kháng”, trang bị hiểu biết về pháp luật, bộ lọc văn hóa tốt, ứng xử văn minh trên môi trường mạng, đánh giá được độ tin cậy của thông tin trên mạng xã hội.

Bốn là, cơ quan An ninh cần phối hợp, hướng dẫn các cơ sở giáo dục phòng ngừa, ngăn chặn, vô hiệu hóa các mối đe dọa an ninh mạng, an ninh thông tin.

Để đảm bảo an ninh sinh viên trong thời kỳ chuyển đổi số, bảo vệ an ninh quốc gia, cơ quan An ninh với chức năng, nhiệm vụ nòng cốt trong bảo vệ an ninh quốc gia

cần chủ động phối hợp, kiến nghị với các cơ sở giáo dục xây dựng các chính sách, quy định an ninh mạng trong nhà trường bao gồm: việc bảo vệ thông tin cá nhân, quản lý tài khoản và mật khẩu, kiểm soát truy cập, tập trung quản lý, nghiên cứu, kiểm tra, đảm bảo khả năng bảo mật cho hệ thống thông tin mạng và ứng dụng trong nhà trường... Phối hợp với cơ sở giáo dục tăng cường tuyên truyền, giáo dục, nâng cao nhận thức về an ninh mạng cho sinh viên, thông qua việc tổ chức hội thảo, tư vấn, phát động các cuộc thi tìm hiểu kiến thức. Xây dựng cơ chế phối hợp, trao đổi, chia sẻ thông tin với các cơ sở giáo dục về các mối đe dọa mới, các kỹ thuật tấn công mạng mới và biện pháp bảo vệ hiệu quả. Phối hợp với cơ sở giáo dục cung cấp chương trình đào tạo về an ninh mạng cho sinh viên để giúp họ nhận biết, phòng tránh và ứng phó với các mối đe dọa an ninh trực tuyến như lừa đảo, tấn công từ chối dịch vụ, tấn công malware... Ngoài ra, cơ quan An ninh cần thực hiện kiểm tra, đánh giá định kỳ các hệ thống mạng trong các cơ sở giáo dục để phát hiện và khắc phục lỗ hổng bảo mật, đồng thời đảm bảo các cơ sở giáo dục tuân thủ các tiêu chuẩn, quy trình về đảm bảo an ninh mạng. Đồng thời tăng cường giám sát hoạt động mạng để phát hiện, ngăn chặn các hoạt động đe dọa xâm phạm an ninh mạng; cảnh báo về các mối đe dọa an ninh mạng, phối hợp với cơ sở giáo dục để áp dụng các biện pháp xử lý khi sinh viên có hành vi cố ý xâm phạm an ninh trên không gian mạng và hệ thống thông tin của nhà trường.

H.Đ.N

TÀI LIỆU THAM KHẢO

- Bộ Thông tin và Truyền thông (2020). *Cẩm nang chuyển đổi số*. Hà Nội.
- Trường Đại học An ninh nhân dân. (2015). *Tìm hiểu ý thức bảo vệ an ninh quốc gia của sinh viên các trường đại học trên địa bàn Thành phố Hồ Chí Minh*. Thành phố Hồ Chí Minh.
- Tạp chí Thông tin & Truyền thông (2016), “*Quản lý các mối đe dọa an ninh thông tin trong các trường đại học, cao đẳng*”, từ website <https://ictvietnam.vn/quan-ly-cac-moi-de-doa-an-ninh-thong-tin-trong-cac-truong-dai-hoc-cao-dang-46353.html>
- Ban Thời sự (2022), “*Chống tin giả, sai sự thật: Hãy là người chia sẻ có trách nhiệm*”, từ website <https://vtv.vn/van-hoa-giai-tri/chong-tin-gia-sai-su-that-hay-la-nguoi-chia-se-co-trach-nhiem-20221130133541304.html>
- TPO (2023), “*Hơn 85% sinh viên được khảo sát lên mạng xã hội hàng ngày với mục đích gì*”, từ website https://doanthanhnien.vn/tin-tuc/hoi-sinh-vien-viet-nam/hon-85_-sinh-vien-duoc-khao-sat-len-mang-xa-hoi-hang-ngay-voi-muc-dich-gi

Bích Thủy (2021), “*Rò rỉ dữ liệu hồ sơ của 300.000 sinh viên Việt Nam*”, từ website <https://antoanthongtin.vn/hacker-malware/ro-ri-du-lieu-ho-so-cua-300000-sinh-vien-viet-nam-107437>

**NHẬN DIỆN TÁC ĐỘNG TIÊU CỰC CỦA NGƯỜI CÓ
ẢNH HƯỞNG TRÊN KHÔNG GIAN MẠNG (KOLs) ĐỐI VỚI
SINH VIÊN VIỆT NAM**

**IDENTIFYING THE NEGATIVE IMPACT OF KEY
OPINION LEADERS (KOLs) ON VIETNAMESE STUDENTS**

Tổng Quang Minh

Trường Đại học An ninh nhân dân

Tác giả liên hệ: quangminhtong538@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> <i>KOLs, Tác động tiêu cực, Sinh viên Việt Nam,</i>	Trên cơ sở nghiên cứu lý luận và thực tiễn, bài viết phân tích về những tác động tiêu cực của người có ảnh hưởng trên không gian mạng (KOLs) đối với sinh viên Việt Nam, xác định một số vấn đề đặt ra và đề xuất giải pháp nâng cao hiệu quả công tác phòng chống tác động tiêu cực do người có ảnh hưởng trên không gian mạng gây nên đối với sinh viên Việt Nam trong giai đoạn hiện nay
<i>Keyword:</i> <i>KOLs, Negative impact, Vietnamese university students</i>	ABSTRACT Based on theoretical and practical research, the article analyzes the negative impacts of Key opinion leaders (KOLs) on Vietnamese students, identifies a number of issues and proposing solutions to improve the effectiveness of preventing negative impacts caused by influential people in cyberspace on Vietnamese students in the current period

1. Người có ảnh hưởng trên không gian mạng KOLs (Key Opinion Leaders) để chỉ những người có khả năng tác động, định hướng dẫn dắt dư luận xã hội. Họ sở hữu, quản lý, chi phối, sử dụng hệ thống các tài khoản trực tuyến và có số lượng người theo dõi, tương tác lớn; có khả năng lan tỏa thông tin với tốc độ nhanh chóng. Ngoài ra, KOLs còn sở hữu năng lực kỹ thuật có khả năng ảnh hưởng gián tiếp đến

sự lan tỏa các luồng thông tin trên không gian mạng, qua đó có thể tác động đến quan điểm, hành vi của cộng đồng xã hội. Sự ảnh hưởng của KOLs chính là sự tác động đến cộng đồng bằng những nội dung được đăng tải lên trên trang thông tin hay trang mạng xã hội mà họ sở hữu.

Hiện nay, Việt Nam có khoảng 500 kênh Youtube có trên 01 triệu lượt theo dõi, trong đó khoảng 100 kênh Youtube trên 03 triệu lượt theo dõi, trung bình thu hút hơn 01 tỷ lượt xem/kênh. Những kênh có số lượng theo dõi lớn đều là kênh sở hữu cá nhân như: “NTN Vlogs” sở hữu 10,2 triệu lượt theo dõi; “Phú Lê” sở hữu 2,19 triệu lượt theo dõi;... Ngoài những kênh thuộc sở hữu cá nhân, còn có những hệ thống trang, kênh, nhóm với lượng thành viên, lượng theo dõi rất lớn như: “Thế Anh 28 Entertainment” với 11 triệu lượt theo dõi trên Facebook,....

Qua nghiên cứu thấy rằng có nhiều cách phân loại KOLs, có thể phân loại dựa theo số lượng người theo dõi, hoặc phân loại dựa trên các nền tảng mạng xã hội mà họ hoạt động như: Facebook, Google, Youtube, Tiktok,... Theo hướng tiếp cận nghiên cứu về tính chất, mức độ tác động, ảnh hưởng của KOLs, có thể phân chia KOLs thành các dạng sau:

Thứ nhất, những người có uy tín, ảnh hưởng trong cộng đồng xã hội, tham gia và tạo ảnh hưởng trên môi trường không gian mạng (KOLs có uy tín). Đây là những người có uy tín, địa vị trong xã hội như: chuyên gia, nhà báo, luật sư, bác sĩ, doanh nhân, chức sắc tôn giáo, diễn giả, văn nghệ sĩ... Họ sử dụng danh tiếng của mình để thu hút số lượng lớn người quan tâm theo dõi các kênh thông tin hay trang mạng xã hội trên nền tảng số và tạo ra những tác động nhất định đối với không gian mạng. Đa số KOLs có uy tín trên không gian mạng là những cá nhân tin tưởng vào đường lối, chủ trương, chính sách của Đảng và Nhà nước, tuyệt đối tuân thủ theo quy định của pháp luật. Trong đó, một số KOLs nổi tiếng còn sử dụng mức độ phủ sóng của mình để định hướng dư luận, kêu gọi mọi người tin tưởng tuyệt đối vào chủ trương của Đảng, chính sách, pháp luật của Nhà nước, tham gia đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng. Quảng bá những hình ảnh đẹp, giá trị tốt đẹp của con người Việt Nam đến với bạn bè quốc tế. Đóng góp nhiều trong công cuộc bảo vệ an ninh trật tự, an ninh quốc gia, xây dựng nhà nước xã hội chủ nghĩa Việt Nam. Tuy nhiên, đối ngược lại với các hoạt động tích cực, một số KOLs sa đà vào việc đưa thông tin giật gân, “câu like”, “câu view”, gây sự chú ý để kiếm tiền từ các trang, kênh của mình. Thậm chí họ sẵn sàng sử dụng lời lẽ thô tục, xúc phạm danh dự, nhân phẩm của người khác. Những sự việc này tác động ảnh hưởng tiêu cực đến cộng đồng xã hội tham gia không gian mạng, trong đó có sinh viên. Nổi lên trong thời gian qua là tình trạng những người tự xưng là nhà báo thiết lập tài khoản mạng xã hội để viết các bài viết nhằm gây xôn xao dư

lượn ngày càng diễn biến phức tạp. Trên danh nghĩa là phòng, chống tiêu cực, những trang mạng xã hội, tài khoản Facebook cá nhân của các “nhà báo tự xưng” dễ dàng thu hút lượng lớn quan tâm. Họ chủ động sản xuất những bài viết, thông tin nhạy cảm, ảnh hưởng nghiêm trọng đến uy tín, phẩm chất, danh dự của các đồng chí lãnh đạo cấp cao, các tổ chức, doanh nghiệp... gây bức xúc dư luận. Điển hình như đối tượng T.C.H.D, H.N với số lượng người theo dõi lớn đã gây ra những phức tạp trong đời sống xã hội.

Thứ hai, người tạo ra ảnh hưởng trên không gian mạng nhờ lượng theo dõi lớn (KOL mạng). Đây thường là những người hoạt động sáng tạo nội dung trên không gian mạng, thu hút được lượng lớn người quan tâm theo dõi nhờ vào ngoại hình, tài năng, bản sắc riêng cá nhân. Tuy nhiên một số đối tượng lại dựa vào sự “khác người”, “đị biệt” để làm “mồi câu” người theo dõi. Thời gian qua, xuất hiện nhiều “hiện tượng mạng” sở hữu các kênh, tài khoản mạng xã hội với hàng triệu lượt theo dõi. Các “hiện tượng mạng” này không phải là những người có địa vị, uy tín trong xã hội mà đa phần làm những công việc như nhân viên văn phòng, lao động phổ thông... Đặc biệt một số đối tượng còn là giang hồ, nghiện, hút, tù tha nhưng lại được tung hô trên không gian mạng như những người hùng, thần tượng, tạo ra tác động tiêu cực đến bộ phận người dùng mạng xã hội, đặc biệt là sinh viên. Lợi dụng sự “khác người” của mình, nhóm người này thường xuyên làm các video dạng thử thách, hài nhảm, nói “đạo lý”... Những đối tượng này luôn tìm cách “câu view” một cách bất chấp, nên đa phần các sản phẩm đăng tải lên mạng xã hội đều nhảm nhí, thiếu tính giáo dục. Nguy hiểm hơn nữa là các video này lại được thu hút bởi hàng triệu lượt xem, tác động mạnh mẽ đến đời sống xã hội, cổ xúy cho lối sống “giang hồ”, bạo lực, thiếu đi tình người. Chẳng hạn như “D.T”, “P.L”, “Đ.N”; những cái tên được tung hô như là thần tượng của giới trẻ đã lần lượt bị xử lý về pháp luật.

Thứ ba, những người có ảnh hưởng gián tiếp trên không gian mạng (KOLs ẩn). Khác với những người lộ diện thân phận, tạo ra ảnh hưởng trực tiếp trên không gian mạng mang tính chất cá nhân, những người có ảnh hưởng gián tiếp quản lý, điều hành, chi phối các tài khoản, trang, kênh, nhóm trên không gian mạng có số lượng thành viên đông, lượng theo dõi lớn; có khả năng ảnh hưởng đến mức độ lan tỏa thông tin hoặc tác động đến hoạt động của nhiều cá nhân khác trên không gian mạng. Các “KOLs ẩn” có khả năng huy động cộng đồng thông qua các nhóm, trang trên mạng xã hội cùng thực hiện một hành động nhằm phục vụ cho mục đích riêng. Từ đó tiềm ẩn những nguy cơ xâm phạm an ninh trật tự, an toàn xã hội, phá hoại hệ thống chính trị. Những người này còn liên kết giữa các diễn đàn, hội nhóm với nhau tạo thành một “thế lực” trên không gian mạng, có thể phát động những chiến

dịch nhằm tấn công vào cá nhân, tổ chức nhất định (cạnh tranh không lành mạnh, vu khống, làm nhục,...) như “Hội những người anti hoa hậu Yến Nhi”, ...

2. Ngày nay, đa phần sinh viên đều có cơ hội tiếp cận các thiết bị truy cập vào Internet. Họ có thể truy cập Internet, tham gia mạng xã hội tại nhà, nơi làm việc, quán cà phê, và nhiều nơi khác. Các phương tiện được sử dụng như: máy tính xách tay, máy tính gia đình, điện thoại,... Về thời gian truy cập Internet, sinh viên thường truy cập Internet trong khoảng 6h - 12h và 18h - 22h vào ngày thường. Và từ 7 - 12h và 17 - 23h vào ngày nghỉ cuối tuần. Mục đích sử dụng mạng xã hội: tìm kiếm, cập nhật thông tin, giải trí; liên lạc bạn bè, gia đình. Hiện nay, sinh viên tham gia nhiều mạng xã hội khác nhau như: Facebook, Zalo, Youtube, Tiktok, Instargram,...

Trong bối cảnh toàn cầu hóa và hội nhập quốc tế, với việc đẩy mạnh chuyển đổi số như hiện nay, các thế lực thù địch, phản động trong và ngoài nước triệt để sử dụng không gian mạng để chống phá nhà nước, các KOLs gia tăng hoạt động nhằm nhiều mục đích khác nhau. Hoạt động của KOLs bên cạnh những điều tích cực thì cũng nảy sinh nhiều tiêu cực, tác động ảnh hưởng xấu đến sinh viên Việt Nam.

Thứ nhất, tiêm nhiễm lối sống “ảo”, sai lệch chuẩn mực xã hội. Thông tin do KOLs đăng tải có tốc độ lan truyền nhanh chóng hơn nhiều lần so với các tin được đăng tải bởi những người sử dụng thông thường. Những thông tin này có khả năng tác động đến nhiều nhóm đối tượng, nhiều địa bàn, nhiều lĩnh vực trong đời sống xã hội. Thông tin giật gân, câu khách, chạy theo lối sống xa hoa, vô bổ đã tác động mạnh đến nhận thức của sinh viên. Thậm chí, KOLs chủ động đưa thông tin có tính chất ăn chơi đua đòi, hưởng thụ, các cách thức làm giàu nhanh,... dẫn tới lối sống thiếu chuẩn mực. Sinh viên bị sa đà vào mạng xã hội, chạy theo “hào nhoáng” thức thời mà không quan tâm đến nhiệm vụ chính của mình là rèn luyện và học tập, tham gia vào các hoạt động xã hội ý nghĩa.

Thứ hai, kích động bạo lực, thúc đẩy vi phạm về trật tự an toàn xã hội. Nhiều đối tượng “giang hồ mạng”, nghiện hút, tù tha, cho vay nặng lãi, bóc lột họ, đòi nợ thuê,.. như “P.L”, “K.B” nhưng vẫn thu hút được đông đảo sự quan tâm, theo dõi của sinh viên. Họ thường xuyên đăng tải lên kênh Youtube hoặc trang cá nhân Facebook những video clip, hình ảnh với lời lẽ thô tục, hành vi lệch chuẩn, nói đạo lý nhưng lại hành xử theo “luật giang hồ” thay vì theo quy định của pháp luật. Nhiều kênh còn đăng tải những trò chơi, thử thách vô bổ, nhằm cổ xúy mê tín dị đoan, khiến cho người xem tin vào ma quỷ, xúi giục thực hiện những hành vi gây nguy hiểm đến bản thân và những người xung quanh, và dẫn chứng là đã có một số

bộ phận sinh viên làm theo như thử thách “cá voi xanh”, những thử thách trên Tiktok nhằm trở nên nổi tiếng,...

Thứ ba, tác động ảnh hưởng xấu đến tư tưởng chính trị, lôi kéo tham gia hoạt động xâm phạm an ninh quốc gia. Vốn là tầng lớp nhạy cảm về vấn đề chính trị và thường xuyên tiếp cận với mạng Internet, tầng lớp sinh viên được các thế lực thù địch tăng cường tiến hành các hoạt động lôi kéo, móc nối, tạo thành một lực lượng đối lập trong nước, coi đây là lực lượng nòng cốt để tiến hành chiến lược “diễn biến hòa bình” và lật đổ chính quyền khi có thời cơ. Một số KOLs như Đ.N.Q, T.H.S, T.Q.H lợi dụng sự ảnh hưởng trên không gian mạng của mình để đưa quan điểm cá nhân, bình luận chỉ trích, phê phán chủ trương, chính sách hoặc lợi dụng các vấn đề nóng trong xã hội để công kích lãnh đạo, Đảng và Nhà nước. Tình hình ngày càng nghiêm trọng hơn khi các đối tượng này liên kết, móc nối với nhau tạo thành những chiến dịch biểu tình, kích động đám đông ra đường, hoặc ký tên qua mạng để yêu cầu các yêu sách vô lý, phản đối một số chủ trương mới của Đảng, Nhà nước.

3. Trước những tác động, ảnh hưởng tiêu cực nêu trên đối với sinh viên Việt Nam, các cơ quan chức năng đã chủ động tổ chức biện pháp công tác nhằm ngăn ngừa hậu quả xảy ra và thu được nhiều kết quả tích cực. Thời gian tới, để góp phần tạo môi trường thông tin trên không gian mạng lành mạnh hơn, giúp cho sinh viên được an toàn khi tham gia mạng xã hội, cần nghiên cứu thực hiện tốt một số nhiệm vụ sau:

Một là, nâng cao hơn nữa hiệu quả tuyên truyền, vận động sinh viên khi tham gia mạng xã hội. Đa dạng hóa các hình thức tuyên truyền, nội dung tuyên truyền sáng tạo và tươi mới để có thể đạt được hiệu quả và phù hợp với giới trẻ, tác động được nhiều hơn đến đời sống sinh viên. Trong thời đại chuyển đổi số hiện nay, công tác tuyên truyền có vai trò rất quan trọng, phải thường xuyên và liên tục nhằm giúp cho người dân nói chung và sinh viên nói riêng nhận diện được các thủ đoạn, nội dung chứa thông tin sai lệch, đầu là quan điểm sai trái, thù địch, nhận thức được tính chất nguy hiểm của nó đối với cá nhân và xã hội. Tránh thấy được tin “hot”, tin “sốt dẻo” là chia sẻ, bình luận mà không kiểm chứng được nguồn tin, vô tình tiếp tay cho các hoạt động chống phá và các hành vi tiêu cực, phản cảm, sai lệch đối với chuẩn mực đạo đức sống trên không gian mạng. Mỗi sinh viên sẽ trang bị cho mình những kiến thức cần thiết để có thể tự sàng lọc, tiếp nhận thông tin hữu ích, cũng như lên án, tẩy chay những KOLs sử dụng tin giả để “câu view”, “câu like”. Đa dạng hóa các hình thức tuyên truyền trên không gian mạng nhằm giúp thông tin chính thống đến tay của các bạn sinh viên một cách thú vị hơn. Xây dựng nội dung tuyên truyền với những từ khóa, gắn liền với những “hot trend”, xu hướng

hiện nay để nội dung trở nên hấp dẫn, lôi cuốn hơn, đồng thời đăng tải vào thời gian phù hợp để có thể tiếp cận nhiều nhóm đối tượng sinh viên.

Hai là, phát huy vai trò Đoàn thanh niên trong việc giảm thiểu tác động tiêu cực của KOLs. Với tư cách là “đội dự bị tin cậy của Đảng”, là “cánh tay đắc lực của Đảng”, Đoàn Thanh niên cộng sản Hồ Chí Minh cần chú trọng đẩy mạnh các hoạt động tuyên truyền, giáo dục lý tưởng cách mạng cho đoàn viên, thanh niên (mà ở đây phần lớn là sinh viên các trường đại học trên cả nước) thông qua các hình thức như: Hội nghị, tọa đàm, hội thi, hội diễn văn nghệ,... Qua đó, kịp thời nắm bắt tình hình tư tưởng, định hướng dư luận trong cộng đồng sinh viên trước những diễn biến phức tạp của KOLs. Mỗi sinh viên sẽ là những người tuyên truyền viên tích cực, không để các tác động, ảnh hưởng tiêu cực từ KOLs lôi kéo, kích động.

Ba là, thực hiện tốt công tác tham mưu, hoàn thiện pháp luật về phòng, chống tội phạm và những vi phạm pháp luật liên quan tới hành vi đăng tải những thông tin sai sự thật, gây hoang mang dư luận của các KOLs. Hoàn thiện pháp luật, cụ thể hơn là thống nhất định nghĩa KOLs và những thông tin mà KOLs được phép đăng tải. Đối với KOLs cần làm rõ những điều kiện xác định cụ thể để một người bình thường có thể trở thành một KOLs (về phẩm chất, đạo đức, số lượt theo dõi, số lượt yêu thích, số lượng thành viên trong một hội, nhóm do KOLs này điều hành, lượng tương tác...) Những thông tin mà KOLs có quyền được phép đăng tải và phát tán theo các quy định của pháp luật. Phải xử phạt nghiêm các trường hợp đăng tải thông tin giả mạo làm ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội.

Bốn là, triển khai đồng bộ các biện pháp nghiệp vụ và biện pháp kỹ thuật nhằm phục vụ cho việc phát hiện và gỡ bỏ những thông tin sai sự thật do KOLs đăng tải. Tổ chức, phân công chặt chẽ, bảo đảm đồng bộ, thống nhất giữa các lực lượng, công an đơn vị địa phương trong triển khai công tác công an với KOLs. Từ đó nhằm triển khai đồng bộ lực lượng, phương tiện, biện pháp đảm bảo yêu cầu kịp thời, thu thập đầy đủ về tài liệu, chứng cứ về hành vi vi phạm để phục vụ xử lý bằng pháp luật khi có yêu cầu. Trong trường hợp cần thiết, cần áp dụng đồng bộ biện pháp nghiệp vụ và biện pháp kỹ thuật nhằm vô hiệu hóa hoạt động của các KOLs trên không gian mạng. Phối hợp với Ban Tuyên Giáo Trung ương, Bộ thông tin và Truyền thông chỉ đạo, định hướng các cơ quan báo chí kịp thời lên án, phê phán, vạch mặt, hạ uy tín các KOLs cực đoan, quá khích, vi phạm pháp luật, vi phạm đạo đức lối sống; tuyên truyền, giáo dục, định hướng nhận thức, lối sống đúng đắn cho sinh viên, hạn chế tác động tác động của những trào lưu, hiện tượng tiêu cực trên không gian mạng.

TÀI LIỆU THAM KHẢO

- KOLs và những mặt trái, Báo Dân trí. Truy cập vào 3/9/2023, từ <https://dantri.com.vn/xa-hoi/kols-va-nhung-mat-trai-20220425093832356.htm>
- KOL - Quyền lực và mặt trái, Ban thời sự VTV. Truy cập vào 3/9/2023, từ <https://vtv.vn/trong-nuoc/kol-nhung-nguoi-co-tam-anh-huong-tren-mang-xa-hoi-20190620000137296.htm>
- Nhật Hạ. KOL sức mạng và truyền thông số, Báo Đồng Nai. Truy cập vào 4/9/2023, từ <https://baodongnai.com.vn/dong-nai-cuoi-tuan/202207/kol-va-suc-manh-truyen-thong-so-3125599/>
- Di Li. KOLs và trách nhiệm xã hội – Pháp lý trong quảng cáo, Tạp chí điện tử Kinh tế Môi Trường. Truy cập vào 4/9/2023, từ <https://kinhtemoitruong.vn/kols-va-trach-nhiem-xa-hoi-phap-ly-trong-quang-cao-56563.html>
- Xuân Mai. KOLs và những mặt trái, Báo Công an nhân dân. Truy cập vào 4/9/2023, từ <https://cand.com.vn/doi-song/bai-1-kols-va-nhung-mat-trai-i651386/>
- Phạm An. Nhận diện KOL, Báo Công an nhân dân. Truy cập vào 4/9/2023, từ <https://antgct.cand.com.vn/Chuyen-de/Nhan-dien-KOLs-i557251/>
- Hồng Ngọc. Mạng xã hội - thời của KOLs, Báo Công an nhân dân. Truy cập vào 4/9/2023, từ <https://antgct.cand.com.vn/Chuyen-de/Nhan-dien-KOLs-i557251/>
- Hà Quang Minh. Con chim bách thanh với cái đầu Medusa, Báo Công an nhân dân. Truy cập vào ngày 4/9/2023, từ <https://antgct.cand.com.vn/Chuyen-de/Nhan-dien-KOLs-i557251/>

**NHẬN THỨC CỦA SINH VIÊN CÁC TRƯỜNG CAO ĐẲNG,
ĐẠI HỌC THÀNH PHỐ HỒ CHÍ MINH VỀ VẤN ĐỀ BẢO VỆ
PHỤ NỮ VÀ TRẺ EM TRÊN KHÔNG GIAN MẠNG
PERCEPTION OF SOCIAL WORK STUDENT AT
COLLEGES AND UNIVERSITIES IN HO CHI MINH CITY ON
THE ISSUE OF PROTECTING WOMEN AND CHILDREN IN
CYBERSPACE**

Lê Thị Huỳnh Như, Huỳnh Lê Phụng Nhi, Lê Ngọc Anh

Học viện Cán bộ Thành phố Hồ Chí Minh

*Tác giả liên hệ: lethihuynhnhuca@gmail

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> nhận thức, bảo vệ phụ nữ và trẻ em, không gian mạng, sinh viên ngành Công tác xã hội, an ninh mạng. <i>Keywords:</i> awareness, protection of women and children, cyberspace, students majoring in social work, cyber security.	An ninh mạng là cụm từ được tìm hiểu, nghiên cứu từ khi cuộc cách mạng công nghiệp 4.0 diễn ra trên toàn cầu. Đối với sinh viên hiện nay thì cụm từ an ninh mạng trở nên phổ biến hơn hẳn vì đây chính là môi trường mở mà sinh viên có thể thoải mái mở rộng giao tiếp, học tập và làm việc một cách chủ động. Bên cạnh những thuận lợi là vô vàn những khó khăn, thách thức thì con người nói chung và sinh viên nói riêng cần chủ động học tập, rèn luyện trước những nguy cơ đang diễn ra trên không gian mạng là vô cùng cần thiết. Đặc biệt đối với sinh viên ngành CTXH thì đây là một trong những vấn đề quan tâm hàng đầu trong tiếp cận, hỗ trợ giải quyết những vấn đề của xã hội. ABSTRACT Cyber security is a phrase that has been studied and researched since the 4.0 industrial revolution took place globally. For students today, the phrase cyber security has become much more popular because this is an open environment where students can freely expand communication, study and work proactively. Besides the advantages, there are countless difficulties and challenges. It is extremely necessary for people in general and students in particular to proactively study and practice against the risks taking place in cyberspace. Especially for students majoring in social work, this is one of the top concerns in approaching and supporting the solution of social problems.

1. Giới thiệu

Hiện nay, Việt Nam là một trong số những nước có tốc độ phát triển nhanh về công nghệ thông tin, số người sử dụng Internet, mạng xã hội ngày càng tăng. Theo thống kê, đến tháng 1/2020 Việt Nam có số người sử dụng Internet lên đến 68,17 triệu người (chiếm tỷ lệ 70% số dân); số lượng người dùng mạng xã hội là 65 triệu người (chiếm tỷ lệ 67% số dân). Việt Nam là quốc gia đứng thứ 18 thế giới về tỷ lệ người dân sử dụng Internet và là 1 trong 10 nước có lượng người dùng Facebook, Zalo, YouTube,... cao nhất thế giới. Bên cạnh những thuận lợi của không gian mạng đó chính là tiết kiệm được thời gian, tiền bạc và sức lực của người tham gia, tuy nhiên có rất nhiều vấn đề nảy sinh trong quá trình sử dụng không gian mạng của con người. Trong đó, sinh viên là đối tượng tiếp cận với không gian mạng thường xuyên với các nhu cầu như học tập, giải trí, kết bạn... Đối với các sinh viên đang theo học ở chuyên ngành Công tác xã hội (CTXH) thì đây là vấn đề cần nhận được quan tâm, nghiên cứu và tìm ra biện pháp hỗ trợ, khắc phục, giải quyết các vấn đề đang diễn ra trên không gian mạng như an toàn thông tin, bảo vệ con người nói chung trước các vấn đề xâm hại, bắt nạt hoặc những thông tin xấu - độc gây ảnh hưởng trực tiếp đối với người sử dụng. Đã có rất nhiều nghiên cứu về vấn đề tiếp cận không gian mạng của con người nói chung, những khó khăn và các vấn đề bất cập. Tuy nhiên, chưa có nghiên cứu liên quan đến nhận thức của sinh viên ngành CTXH đối với các vấn đề liên quan đến không gian mạng. Do đó, nhóm nghiên cứu đã thực hiện nghiên cứu sâu đối với vấn đề nhận thức của sinh viên ngành CTXH các trường cao đẳng, đại học Thành phố Hồ Chí Minh về vấn đề bảo vệ phụ nữ và trẻ em trên không gian mạng. Đây là một trong số các đề tài có liên quan đến lĩnh vực nghiên cứu các vấn đề bảo vệ phụ nữ và trẻ em trước những nguy cơ khi tiếp cận không gian mạng. Việc thực hiện nghiên cứu về nhận thức của sinh viên ngành CTXH với mục đích là phân tích thực trạng của xã hội, nghiên cứu thực tiễn địa bàn từ đó phát hiện những khó khăn, vấn đề bất cập, gây cản trở trong quá trình nâng cao nhận thức của sinh viên ngành CTXH nói riêng và sinh viên ở khu vực TP. HCM nói chung. Trong quá trình thực hiện nghiên cứu, nhóm nghiên cứu thực hiện khảo sát và thu về 490 mẫu trong đó sinh viên ngành CTXH và sinh viên ngành khác.

2. Cơ sở lý thuyết

Đề tài được thực hiện dựa trên các thuyết:

Thuyết nhu cầu Maslow: Dựa trên cơ sở của thuyết về 05 nhu cầu của con người từ đó đề tài áp dụng vào quá trình nghiên cứu, xem xét dựa trên các mức nhu cầu đó để xem nhu cầu con người có được đảm bảo và lý thuyết được chứng minh vào thực tiễn hay không?

Thuyết hành động Max Weber cho rằng hành động xã hội là một hành vi mà chủ thể gắn cho ý nghĩa chủ quan nhất định, động cơ bên trong chủ thể là nguyên nhân của

hành động, do vậy có thể nghiên cứu được cái yếu tố chủ quan thúc đẩy hành động. Chỉ có những hành động nào có động cơ, mục đích thì mới được coi là hành động xã hội. Cho nên trong hành động xã hội bao giờ cũng có sự tham gia của yếu tố ý thức, dù mức độ có thể khác nhau. Đề tài nghiên cứu những hành động của sinh viên từ đó tìm ra nguyên nhân cho những hành động xã hội đó. Hành vi xã hội của sinh viên sẽ xuất phát từ nhận thức của họ, là quá trình quan sát, đúc kết kinh nghiệm mà có được từ đó sinh viên sẽ tự đưa ra hành động xã hội cho bản thân trước vấn đề bảo vệ phụ nữ và trẻ em trên KGM.

Max Weber cho rằng hành động xã hội là một hành vi mà chủ thể gắn cho ý nghĩa chủ quan nhất định, động cơ bên trong chủ thể là nguyên nhân của hành động, do vậy có thể nghiên cứu được cái yếu tố chủ quan thúc đẩy hành động. Chỉ có những hành động nào có động cơ, mục đích thì mới được coi là hành động xã hội. Cho nên trong hành động xã hội bao giờ cũng có sự tham gia của yếu tố ý thức, dù mức độ có thể khác nhau. Đề tài nghiên cứu những hành động của sinh viên từ đó tìm ra nguyên nhân cho những hành động xã hội đó. Hành vi xã hội của sinh viên sẽ xuất phát từ nhận thức của họ, là quá trình quan sát, đúc kết kinh nghiệm mà có được từ đó sinh viên sẽ tự đưa ra hành động xã hội cho bản thân trước vấn đề bảo vệ phụ nữ và trẻ em trên KGM.

Từ các lý thuyết trên, nhóm nghiên cứu đưa ra các giả thuyết như sau:

- Hiện nay nhận thức của sinh viên ngành CTXH về vấn đề bảo vệ phụ nữ và trẻ em trên KGM đang diễn ra đầy đủ, trong đó bao gồm nhận biết về các nguy cơ, yếu tố bảo vệ, các chính sách pháp luật cũng như là các dịch vụ CTXH.
- Quá trình nhận thức của sinh viên chịu sự tác động từ các yếu tố bản thân, thông tin truyền thông, giáo dục và các chuẩn mực giá trị.
- Việc điều chỉnh khung chương trình đào tạo, sắp xếp các thứ tự học phần, tăng cường các giải pháp truyền thông và vai trò của người làm CTXH, giúp sinh viên có cơ hội trải nghiệm để hiểu mình, hiểu nghề, xác định đúng mục tiêu học tập từ đó giúp nâng cao nhận thức của SV về các vấn đề xã hội.

3. Phương pháp nghiên cứu

3.1 Phương pháp luận

Đề tài chọn chủ nghĩa Mác - Lênin làm cơ sở lý luận. Ý nghĩa của luận là ở chỗ, trong công việc nghiên cứu của tác giả không dừng lại ở việc mô tả, mà cần tiếp tục đi sâu hơn vào bản chất của đối tượng và chỉ ra tính quy luật. Con đường nhận thức này đòi hỏi phải đặt đối tượng nghiên cứu của mình vào bối cảnh lịch sử cụ thể.

3.2 Phương pháp cụ thể

Để tiếp cận đối tượng nghiên cứu, chúng tôi sử dụng phương pháp định lượng kết hợp với định tính, cụ thể như sau:

- Nghiên cứu tài liệu:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Là việc phân tích và tổng hợp các khái niệm làm việc, các cách tiếp cận lý thuyết, các nội dung và phương pháp của các công trình có liên quan ở trong nước và nước ngoài, cũng như các nguồn số liệu thống kê mà địa phương cung cấp. Trong đó, bao gồm: (1). Các sách, báo in, báo mạng, tạp chí khoa học và công trình nghiên cứu tại các hội thảo quốc gia, quốc tế; (2). Các nghị định, đề án của Chính phủ, Bộ, ngành và các văn bản pháp luật có liên quan đến đối tượng nghiên cứu;

- Phỏng vấn trực tiếp bằng bảng hỏi:

Để xác định, quy mô của mẫu nghiên cứu của 10 trường cao đẳng, đại học, nhóm tác giả sử dụng công thức sau:

$$n = N / (1 + N \cdot e^2)$$

n: Quy mô (cỡ) mẫu

N: Quy mô dân số nghiên cứu

e: Mức sai lệch mà nhà nghiên cứu mong muốn
(tỷ lệ phần trăm sai lệch từ 1% đến 10% do việc sử dụng mẫu thay vì nghiên cứu toàn mẫu).

Trong nghiên cứu này với N = 2240

STT	Trường đại học/cao đẳng	Số lượng sinh viên
1	Đại Học Khoa học xã hội & nhân văn	290 sinh viên
2	Đại Học Tôn Đức Thắng	200 sinh viên
3	Đại Học Văn Lang	24 sinh viên
4	Học Viện Cán bộ TP.HCM	268 sinh viên
5	Phân Hiệu Học viện Phụ nữ Việt Nam TP.HCM	250 sinh viên
6	Đại Học Mở TP.HCM	292 sinh viên
7	Đại Học Lao động và Xã Hội II	446 sinh viên
8	Đại Học Sư Phạm TP.HCM	204 sinh viên
9	Cao Đẳng Kinh tế TP.HCM	250 sinh viên
10	Cao Đẳng Sư Phạm Trung ương TP.HCM	16 sinh viên

e = 4%, ta có: $n = 2240 / (1 + 2240 \times 0.042) = 488$ (đơn vị mẫu).

Để đảm bảo dung lượng mẫu nhóm nghiên cứu đã làm tròn lên 550 đơn vị mẫu. Tuy nhiên, sau khi kết thúc quá trình khảo sát nhóm nghiên cứu thu được 490 đơn vị mẫu. Các đơn vị mẫu là các khách thể sinh viên học tại các trường đại học, cao đẳng ở TP Hồ Chí Minh. Việc lựa chọn các đặc điểm của người được phỏng vấn là để phản ánh nhận thức của sinh viên ngành CTXH tại các trường đại học, cao đẳng TP Hồ Chí Minh về bảo vệ phụ nữ, trẻ em trên không gian mạng.

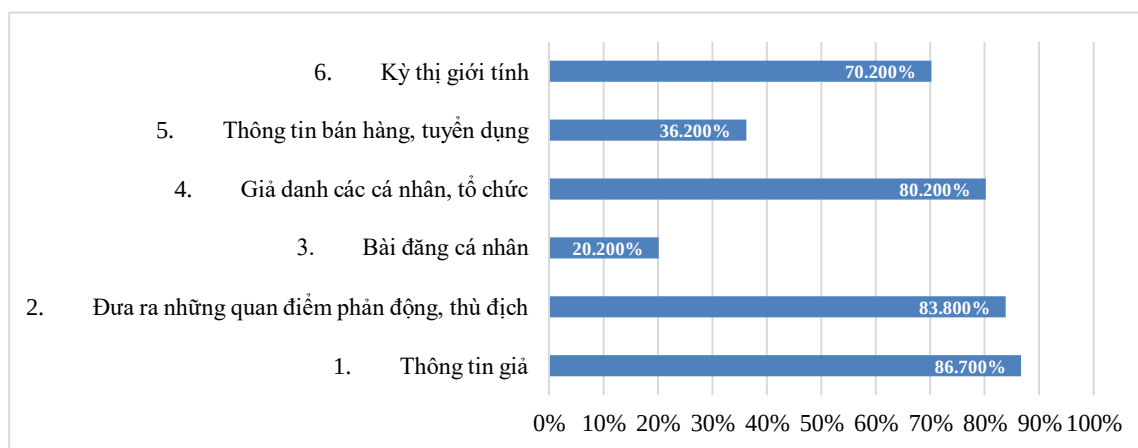
4. Kết quả nghiên cứu

4.1. Kết quả

Nhận thức về thông tin xấu độc

Hiện nay với sự phát triển của công nghệ 4.0, vô số thông tin được đăng tải trên trang mạng xã hội với nhiều nội dung khác nhau. Mạng xã hội đang là phương tiện nguy hiểm nhất, với đặc tính lan truyền nhanh, vượt qua những rào cản về ngôn ngữ, khoảng cách địa lý, gây ra những tác hại trên diện rộng hơn bất kì hình thức nào. Để tìm hiểu về nhận thức của sinh viên trước những thông tin xấu độc nhóm tác giả đã tiến hành cuộc khảo sát như sau:

Biểu đồ 1. Nhận biết về thông tin xấu độc



(Nguồn: Khảo sát của đề tài)

Biểu đồ 1 cho ta thấy nhận biết của sinh viên về thông tin xấu độc được thể hiện rõ ở 6 chỉ báo. Ở chỉ báo số 1/ Nhận biết thông tin giả chiếm tỷ lệ cao nhất 86.7% so với các chỉ báo còn lại: ở chỉ báo 2/ Đưa ra những quan điểm phản động, thù địch chiếm 83.8%, 4/ Giả danh các cá nhân, tổ chức là 80.2%, 6/ Kỳ thị giới tính là 70.2%. Thấp nhất là 3/ Bài đăng cá nhân chiếm 20.2% và 5/ Thông tin bán hàng, tuyển dụng là 36.2% hai chỉ số này chỉ dưới 50%. Các tỉ lệ này càng tăng cao và cho thấy sự hiểu biết của sinh viên trên địa bàn TP.HCM có nhận thức khá tốt về vấn đề. Và kết quả này cho thấy các Nghị định, Nghị Quyết của Đảng, Nhà nước đã đi vào từng ngõ ngách của đời sống xã hội, trong đó có các nhóm sinh viên trên địa bàn cả nước. Chẳng hạn như Nghị định 72/2013/NĐ-CP và trong Luật an ninh mạng 2018 đã được triển khai và đi vào đời sống của người dân, sinh viên, học sinh hiện nay. Tuy nhiên, đây chỉ dừng lại ở việc thống kê tần suất để đi sâu hơn nhóm tác giả xin được phân tích các nhóm xã hội để làm nổi bật lên vấn đề nghiên cứu hiện nay.

Bảng 1. Nhận biết thông tin xấu độc trên không gian mạng theo nhóm ngành học

Nhận biết thông tin xấu độc trên không gian mạng	Nhóm ngành học					
	CTXH		Ngành khác		Tổng	
	N	%	N	%	N	%
1. Thông tin giả	222	88,4	142	84,0	364	86,7
2. Đưa ra những quan điểm phản động, thù địch	224	89,2	128	75,7	352	83,8
3. Bài đăng cá nhân	47	18,7	38	22,5	85	20,2
4. Giả danh các cá nhân, tổ chức	206	82,1	131	77,5	337	80,2
5. Thông tin bán hàng, tuyển dụng	86	34,3	66	39,1	152	36,2
6. Kỳ thị giới tính	187	74,5	108	63,9	295	70,2
Tổng	251	100,0	169	100,0	420	100,0
Significant = 0.001						

(Nguồn: Khảo sát của đề tài)

Khi tìm hiểu giữa các xã hội với nhau, xét nhóm chuyên ngành, cũng ở bảng 1 với Significant = 0.001 cho ta thấy giữa các nhóm ngành có sự khác biệt với nhau về nhận biết thông tin xấu độc sinh viên. Tác giả xin lựa một số các chỉ báo để phân tích và làm rõ sự khác biệt này. Ở chỉ báo 2/ Đưa ra những quan điểm phản động, thù địch, ngành CTXH chiếm tỷ lệ cao nhất là 89.2% so với ngành khác tỷ lệ 75.7%. Ở chỉ báo 5/ Thông tin bán hàng, tuyển dụng nhóm sinh viên ngành khác lại chiếm tỷ lệ lại cao hơn là 39.1% so với nhóm sinh viên ngành CTXH là 34.3%. Từ những chỉ báo trên ta có thể thấy rằng việc nhận biết của sinh viên về thông tin xấu độc có sự khác biệt. Khi xét theo các nhóm xã hội ở nhóm ngành học, nhóm tác giả cũng tiến hành một cuộc phỏng vấn như sau: Một bạn sinh viên ngành CTXH cho hay “Sinh viên CTXH phải cập nhật tình hình xã hội nhiều nên vấn đề nhận biết về thông tin xấu độc cũng sẽ hiểu cao” (N.H.N.H-SV năm 3 CTXH). Bên cạnh đó bạn sinh viên khác ngành có ý kiến “Hiện nay các thông tin tràn lan trên mạng thật giả lẫn lộn khó phân biệt nào là thật nào là giả, ngoài ra mình cũng ít tiếp cận với các vấn đề khác ngành học” (T.M.A-SV ngành QTKD-ĐH Văn Lang). Ở chỉ báo 4/ Giả danh các cá nhân, tổ chức ở nhóm sinh viên năm 1 có tỷ lệ là 77.1% thấp hơn so với sinh viên năm 2 là 88.7%. Thông qua số liệu trên nhóm nghiên cứu đã có một cuộc khảo sát và thu được kết quả: một bạn sinh viên năm tư cho rằng “Việc sinh viên năm hai trở lên có nhận thức tốt về vấn đề là do trong quá trình học tập, làm bài và dưới sự giảng dạy của thầy cô thì nhận thức của các bạn sẽ cao hơn”. (SV CTXH- năm 4). Bên cạnh đó, một bạn sinh viên năm nhất cũng có ý kiến “Nhận thức xuất phát từ thái độ và trách nhiệm của người học, sinh viên năm nhất cũng có thể nhận biết cao” (SV CTXH – năm 1).

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thông qua khảo sát về nhận biết thông tin xấu độc nhìn chung sinh viên đều có thể nhận thức tốt về vấn đề. Đối với thông tin xấu độc có thể do môi trường học tập và tính chất của ngành nghề mà nhận biết của sinh viên ngành CTXH có sự nổi trội và thể hiện rõ ràng hơn so với ngành khác. Điều này là phù hợp với tình hình thực tế hiện nay, khi sinh viên yêu thích và đam mê một khía cạnh nào đó thì nhận biết sẽ ở mức độ cao hơn so với sinh viên bình thường. Tuy nhiên việc nhận biết thông tin xấu độc là một vấn đề quan trọng và cần được đẩy mạnh hơn nữa nên chúng ta cần thay đổi môi trường nhà trường để sinh viên dù là ngành CTXH hay là ngành khác thì khả năng tiếp cận, nhận biết thông tin xấu độc đều tốt.

Quan điểm về thông tin xấu độc

Bảng 2. Quan điểm của sinh viên về các nguy cơ trên không gian mạng theo nhóm ngành học

Quan điểm của sinh viên về các nguy cơ trên không gian mạng		Nhóm ngành học					
		CTXH		Ngành khác		Tổng	
		N	%	N	%	N	%
1. Các tin tức giả thường có tiêu đề hấp dẫn, bắt mắt lôi kéo người xem	Đồng ý	210	83,3	140	82,4	350	82,9
	Không đồng ý	42	16,7	30	17,6	72	17,1
	Significant = 0,793						
2. Giả danh một cá nhân hay tổ chức nào đó sẽ làm tổn hại danh dự, nhân phẩm	Đồng ý	236	93,7	156	91,8	392	92,9
	Không đồng ý	16	6,3	14	8,2	30	7,1
	Significant = 0,460						
3. Những đối tượng hay kì thị giới tính thường lấy hình ảnh, clip của người khác ra kèm theo những ngôn ngữ công kích điều này gây tổn hại về sức khỏe tinh thần	Đồng ý	230	91,3	156	91,8	386	91,5
	Không đồng ý	22	8,7	14	8,2	36	8,5
	Significant = 0,858						
4. Kỳ thị giới tính chính là hệ quả của quá trình chịu tác động từ văn hóa – xã hội như trọng nam khinh nữ	Đồng ý	217	86,1	142	83,5	359	85,1
	Không đồng ý	35	13,9	28	16,5	63	14,9
	Significant = 0,465						
5. Những đối tượng mạo danh cá nhân hay tổ chức họ thường sử dụng hình ảnh cắt ghép của người khác với mục đích xấu	Đồng ý	33	2,5	59	3,5	92	2,9
	Không đồng ý	9	,5	1	,5	0	,1

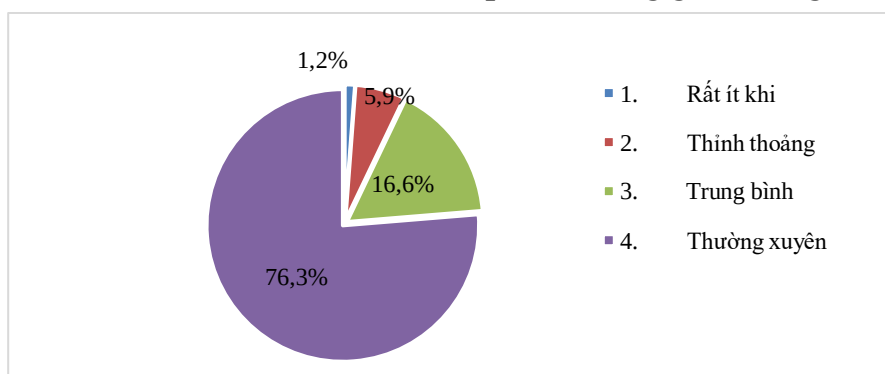
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

	Significant = 0,675						
6. Tin xấu - độc đang xuất hiện tràn lan trên các trang mạng xã hội là hệ quả của sự kiểm soát kém	Đồng ý	226	89,7	148	87,1	374	88,6
	Không đồng ý	26	10,3	22	12,9	48	11,4
	Significant = 0,405						
7. Nâng cao nhận thức về bình đẳng giới thì sẽ giảm đi sự kỳ thị giới	Đồng ý	239	94,8	153	90,0	392	92,9
	Không đồng ý	13	5,2	17	10,0	30	7,1
	Significant = 0,058						
	Tổng	252	100,0	170	100,0	422	100,0

(Nguồn: Khảo sát của đề tài)

Khi xem xét các nhóm xã hội, trong đó có ngành học thì nhóm tác giả đã khảo sát ở 7 chỉ báo. Nhìn chung bảng số liệu 2.2 Quan điểm của sinh viên về các nguy cơ trên không gian mạng theo nhóm ngành học đều không có căn cứ để chứng minh cho sự khác biệt, hầu như các chỉ báo đều có số significant lớn hơn 0.005. Điều này có thể chứng minh được rằng sinh viên có quan điểm tương đương với nhau đều theo một quy luật hiển nhiên, bởi với sự phát triển vượt trội như ngày nay, thời gian tiếp xúc với mạng xã hội ngày một nhiều. Điều này cũng tác động đến quan điểm của sinh viên, nó được thể hiện qua biểu đồ 2.2 về mức độ tiếp cận không gian mạng:

Biểu đồ 2. Mức độ tiếp cận không gian mạng



(Nguồn: Khảo sát của đề tài)

Hiện nay chỉ có 1.2% sinh viên rất ít khi sử dụng mạng xã hội, 5.9% là thỉnh thoảng và 16% chỉ ở mức trung bình. Số lượng còn lại là thường xuyên và chiếm mức độ cao nhất là 76.3%. Hầu như các nền tảng mạng xã hội đều được cập nhật các thông tin về các vấn đề xã hội ví dụ các nền tảng: youtube, facebook, zalo,...

Quay trở lại bảng 2.2 Quan điểm của sinh viên về các nguy cơ trên không gian mạng theo nhóm ngành học nhóm tác giả chọn ra 2 chỉ báo để phân tích sâu. Ở chỉ báo 1/ Các tin tức giả thường có tiêu đề hấp dẫn, bắt mắt lôi kéo người xem nhóm ngành học CTXH có 83.3% sinh viên đồng ý và nhiều hơn so với sinh viên trái ngành có tỷ lệ

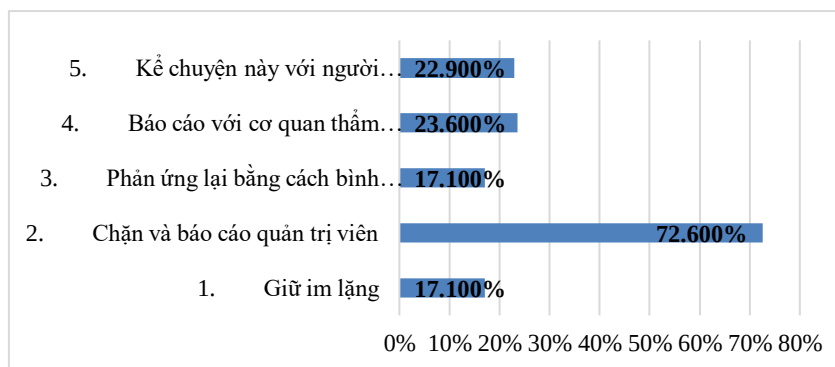
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

82.4%. Về số lượng không đồng ý sinh viên CTXH có 16.7% thấp hơn ngành khác là 17,6%. Theo như số significant của chỉ báo này thu được là bằng 0.793. Nhóm đã tiến hành phỏng vấn một bạn sinh viên ngành CTXH và có kết quả như sau: “Việc thường xuyên tiếp xúc với không gian mạng sẽ làm cho sinh viên nhận diện được các thông tin xấu độc và từ đó cũng có quan điểm giống nhau. Hầu như chỉ cần bạn tìm kiếm thông tin đó một lần thì mạng xã hội sẽ nhận diện và đưa ra các gợi ý giống với thông tin trước đó bạn tìm” (Sinh viên năm 3, ngành CTXH).

Nói về quan điểm không phải sinh viên nào nhận thức tốt thì sẽ đưa ra được những quan điểm về vấn đề ở mức độ cao. Từ nhận biết để đi đến đưa ra các quan điểm là một quá trình, và hiện nay quan điểm về thông tin xấu độc của sinh viên ngành CTXH không có sự khác biệt nhiều so với ngành khác. Nguyên nhân dẫn đến việc này có rất nhiều và nguyên nhân chủ yếu là do các bạn chưa nhận thức được ngành học, vai trò của ngành CTXH và hướng đến của CTXH từ đó còn hạn chế đưa ra các quan điểm đối với một vấn đề xã hội. Song chúng ta cần có những sự thay đổi về khuôn chương trình học để sinh viên có thể tiếp cận về hiểu được ngành mình học từ đó sẽ giúp sinh viên đưa ra những quan điểm rõ ràng và mang tính thuyết phục hơn.

Thái độ về thông tin xấu độc

Biểu đồ 1. Thái độ của sinh viên trước thông tin xấu độc xảy ra trên không gian mạng



(Nguồn: Khảo sát của đề tài)

Khi nhìn vào biểu đồ 2.3 chúng ta có thể nhận diện được rằng đa phần sinh viên sau khi biết được các thông tin xấu độc đều có thái độ 2/ Chặn và báo cáo quản trị viên chiếm 72.6%. Số còn lại thì 4/ Báo cáo với cơ quan thẩm quyền 23.6%, 5/ Kể chuyện này với người thân và nhờ sự giúp đỡ của người thân và bạn bè chiếm 22.9, 1/ Giữ im lặng 17.1% và cuối cùng là 3/ Phản ứng lại bằng cách bình luận cũng chỉ chiếm 17.1%. Thái độ chính là yếu tố quan trọng để quyết định được hành động sau đó của con người, tiếp theo chúng ta sẽ tìm hiểu sâu hơn các nhóm xã hội.

Bảng 2. Thái độ của sinh viên trước các tình huống đã xảy ra trên không gian mạng theo nhóm ngành học

Thái độ của sinh viên trước các tình huống xảy ra trên không gian mạng	Nhóm ngành học					
	CTXH		Ngành khác		Tổng	
	N	%	N	%	N	%
Giữ im lặng	45	17,9	27	16,0	72	17,1
Chặn và báo cáo quản trị viên	177	70,5	128	75,7	305	72,6
Phản ứng lại bằng cách bình luận	58	23,1	14	8,3	72	17,1
Báo cáo với cơ quan thẩm quyền	67	26,7	32	18,9	99	23,6
Kể chuyện này với người thân và nhờ sự giúp đỡ của người thân và bạn bè	53	21,1	43	25,4	96	22,9
Tổng	251	100,0	169	100,0	420	100,0
Significant = 0.001						

(Nguồn: Khảo sát của đề tài)

Thái độ là một trong những yếu tố quan trọng nhất giúp con người vượt qua những tình huống khó khăn của cuộc sống. Thái độ và cách hành xử của một số người có thể ảnh hưởng tiêu cực đến cuộc sống cá nhân của họ theo hướng ngày càng trầm trọng. Chính vì vậy, mỗi chúng ta phải có nhiệm vụ tự định hướng và tìm cách xây dựng cho bản thân phương pháp tư duy, nhân sinh quan và thái độ sống phù hợp. Nói một cách đơn giản, thái độ sống tích cực sẽ mang lại vô vàn những kết quả tốt đẹp, ngược lại tư duy và hành động tiêu cực là nguồn gốc của mọi trở ngại bạn sẽ gặp phải.

Khi xem xét về các nhóm xã hội, trong đó có nhóm ngành học, bảng 2.3 đã thu được kết quả Significant = 0.001 điều này đã chứng minh được thái độ của sinh viên khi đứng trước tình huống thông tin xấu độc luôn có những thái độ khác nhau. Ở chỉ báo 1/ Giữ im lặng ngành CTXH chiếm lên đến 17.9% thế nhưng ngành khác lại thấp hơn chỉ có 16.0%. Khi nhận được kết quả khảo sát này nhóm tác giả đã phỏng vấn 1 bạn sinh viên ngành CTXH để hiểu rõ hơn lý do có sự chênh lệch ở chỉ báo này. Bạn sinh viên đã cho hay “Giữ im lặng ở đây không phải là không hề quan tâm chỉ là thay vì thể hiện nói rõ trên mạng các bạn sẽ nhắn tin giúp đỡ phụ nữ và trẻ em. Không gian mạng vốn là con dao hai lưỡi nên thay vì tranh cãi trên không gian mạng hay chặn thì bạn muốn tìm hiểu rõ hơn bằng cách liên hệ giúp đỡ nạn nhân” (SV năm 3-CTXH). Có chăng đây là sự ảnh hưởng tích cực từ chương trình học ngành CTXH mang đến. Đó chính là thân chủ, phụ nữ và trẻ em những đối tượng cần giúp đỡ họ là trung tâm trong việc trợ giúp. Chính vì đó, mà thay vì có những hành động theo như 5 chỉ báo trong bảng hỏi các bạn chọn cách liên hệ trực tiếp với người cần hỗ trợ. Ở một chỉ báo khác, 2/ Chặn và báo cáo quản trị viên ở chỉ báo này sinh viên ngành khác chiếm tỷ lệ cao nhất là 75.7% so

với ngành CTXH là 70.5%. Để hình thành nên thái độ ở sinh viên thì trước đó quan điểm về vấn đề sẽ là một định hướng. Quan điểm đi đến thái độ là một khoảng cách. Ở chỉ báo này nhóm đã có hai cuộc phỏng vấn một bạn sinh viên ngành CTXH và một bạn khác ngành và có được các câu trả lời như sau: Sinh viên CTXH: “Chặn và báo cáo với quản trị viên sẽ giúp cho quản trị viên kiểm soát chặt hơn thông tin và xóa những bài không nên tồn tại” (SV CTXH-năm 3). Hay cũng một bạn CTXH cho rằng “Xem thông tin xấu, hay trải qua các vấn đề là để rút kinh nghiệm từ từ, với vị trí là sinh viên ngành CTXH tui nghĩ tui muốn gặp các trường hợp đó để phát triển kỹ năng bảo vệ bản thân và kỹ năng hỗ trợ người khác giải quyết vấn đề. tất nhiên là trong quá trình tham gia vào những môi trường như vậy thì tui cần tỉnh trước nó” (SV CTXH – năm 3). Còn đối với bạn sinh viên khác ngành lại cho rằng “Chặn và báo cáo là để tránh đi những tiêu cực xấu và bản thân cũng không muốn vướng vào rắc nên đây sẽ là biện pháp tốt” (ngành QTKD – năm 3).

Nhìn chung, tỷ lệ khác biệt hầu như không nhiều, các bạn dù là SV CTXH hay SV ngành khác đều có sự tương đồng trong nhận biết, quan điểm, thái độ như nhau. Nhưng nhận thức chỉ ở mức cơ bản để đi đến mức độ nâng cao thì sinh viên cần có cả một quá trình cải thiện và phát triển về nhận thức. Hiện nay tỷ lệ SV CTXH mặc dù đã nhận thức đầy đủ nhưng chỉ ở mức đầy đủ chưa thể nâng cao được, mặc dù là sinh viên học các môn chuyên ngành.

Hạn chế: Hiện nay các thông tin xấu độc ngày một lan truyền rộng rãi trên mạng xã hội và nó trở nên khó nhận diện hơn. Nhưng sinh viên hiện đã và đang có một nhận thức tốt đối với các thông tin xấu độc, hầu như sinh viên đều có thể nhận diện được thông tin xấu độc là những thông tin nào. Nhưng chúng ta không thể phủ rằng nhận thức tốt chưa hẳn sẽ hành động tốt nhưng nếu nhận thức sai là chắc chắn sẽ hành động sai. Và hiện nay mặc dù nhận thức của sinh viên đang ở mức tốt nhưng xét ở khía cạnh khác nhận thức này chưa đủ bởi khi đưa ra các quan điểm sinh viên vẫn còn ở mức độ chung, và mỗi sinh viên cần có sự rèn luyện nhiều hơn nữa. Cụ thể là sinh viên có thể nhận diện được các thông tin nhưng để dẫn đến thái độ, thì một bộ phận sinh viên vẫn còn tồn tại sự vô cảm. Sinh viên chưa nhận thức được rằng các thông tin xấu độc ấy sẽ là một quả bom gây hại cho xã hội hay cũng có thể sinh viên không có cảm thấy những thông tin ấy không liên quan đến bản thân mình. Để nâng cao nhận thức thì sinh viên ngành CTXH, cần phải có sự chủ động nắm bắt các tin tức về các vấn đề xã hội. Đây là điều sinh viên tăng cường tính tự lực và trách nhiệm đối với xã hội. Từ việc sinh viên chủ động, theo thời gian sẽ hình thành nên thói quen và sau đó là nhận thức được nâng cao.

4.1.2. Giải pháp

Đối với nhà trường

Đầu tiên là giải pháp về khung chương trình đào tạo: Theo Hiệp hội Quốc gia (NASW) thì: Công tác xã hội là một hoạt động nghề nghiệp giúp đỡ các cá nhân, nhóm hay cộng đồng để nhằm nâng cao hay khôi phục tiềm năng của họ để giúp họ thực hiện chức năng xã hội và tạo ra các điều kiện xã hội phù hợp với mục tiêu của họ. Công tác xã hội tồn tại để cung cấp các dịch vụ xã hội mang tính hiệu quả và nhân đạo cho cá nhân, gia đình, nhóm, cộng đồng và xã hội giúp họ tăng năng lực và cải thiện cuộc sống. Phụ nữ hay trẻ em muốn tiếp cận các dịch vụ công tác xã hội thì họ phải có sự hiểu biết, mà sự hiểu biết này bắt nguồn từ việc hỗ trợ của nhân viên CTXH. Thế nhưng với tình hình nhận thức của sinh viên hiện nay là một trở ngại lớn nhất, dựa trên số liệu mà nhóm nghiên cứu đã thu thập được, nhận thức của sinh viên CTXH hiện nay tại TP.HCM còn nhiều lỗ hổng. Khi nhóm nghiên cứu khảo sát về nhận thức các yếu tố nguy cơ mà phụ nữ và trẻ em có thể đối mặt trên không gian mạng đã thể hiện rõ được tình trạng của sinh viên hiện nay. Việc sửa đổi chương trình khung ở đại học là một vấn đề hết sức nan giải nhưng cần phải cải thiện càng sớm càng tốt. Vì theo như phân tích cho thấy rằng sinh viên CTXH từ những năm đầu tiên chưa thể nắm rõ các kiến thức do quá trình tiếp cận môn học còn nhiều khó khăn, cách phân bổ chương trình học còn hạn chế, chưa vào trọng tâm ngành học mà bắt đầu từ những môn lý luận chính trị. Và cũng có thể thấy sinh viên hiện nay chưa nắm vững và vận dụng được kiến thức tốt do các bạn chỉ học trên lý thuyết và chưa thực hành nhiều. Dựa theo đối sánh các môn học đại cương của của đại học Arizona State, Đại học Tôn Đức Thắng, Đại học Mở, Đại học KHXH & NV, Phân viện Học viện Phụ nữ TPHCM, Học viện cán bộ TP.HCM và Cao đẳng kinh tế TP.HCM, chúng ta có thể thấy có sự khác biệt trong phân bổ chương trình học. Đối với đại học Arizona State của Mỹ môn học đầu tiên mà sinh viên được học chính là môn học trải nghiệm, trải nghiệm ở đây chính là trải nghiệm về ngành học. Các bạn cần có định hướng cụ thể cho bản thân và ngành học của mình.

Đối với truyền thông

Ngày nay, truyền thông là một trong những lĩnh vực nhận được nhiều sự quan tâm của Đảng, Nhà nước, cá nhân và cộng đồng bởi sự tiện lợi, nhanh chóng và đa phương thức của chúng. Là một kiểu tương tác xã hội, truyền thông có vai trò quan trọng trong việc giúp các cá nhân, tổ chức thực hiện việc truyền tải thông tin, trao đổi cảm xúc, thể hiện thái độ đến với những đối tượng nhận thông tin.

Truyền thông ảnh hưởng rất lớn đến các vấn đề của xã hội, trong đó có vấn đề bảo vệ phụ nữ và trẻ em. Truyền thông tác động đến nhận thức của tất cả mọi người trong đó có sinh viên, nhận thức đúng chưa chắc hành vi đúng nhưng nhận thức sai thì chắc chắn hành vi sẽ sai. Nhận thức là gốc, là nền của mọi hành động. Khi có một cách

ứng xử tốt được lan truyền rộng rãi thông qua hình thức truyền thông sẽ có sức hút rất lớn đến cộng đồng, xã hội. Phương pháp hữu hiệu là truyền thông bằng hình thức trực tiếp thông qua các Hội nghị, Hội thảo, báo cáo, chuyên đề. Cần phối hợp với các cơ quan, đơn vị tổ chức nhiều chuyên đề liên quan đến các vấn đề xã hội để cho sinh viên tiếp cận và đưa ra phương án giải quyết giúp sinh viên có nhiều trải nghiệm, tăng trách nhiệm và năng lực tự chủ trong quá trình học tập và làm việc. Và nên tổ chức các chuyên đề từ năm thứ nhất để sinh viên có hướng đi và cách tiếp cận phù hợp với các vấn đề. Thông qua kết quả khảo sát, số lượng sinh viên tham gia vào mạng xã hội là chiếm đến 76,3%. Số liệu đó cho thấy được sinh viên tham gia vào môi trường mạng là rất nhiều nhưng chỉ với mục đích lướt dạo và xem những trang mà mình thích. Vì thế, để tránh phải bị trôi thông tin truyền thông tin một cách nhạt nhòa thì một thiết kế đầy màu sắc, mang đầy đủ nội dung tuyên truyền như thiết kế Poster, Infographic, Canva,...rất đa dạng và phù hợp với thời công nghệ số như hiện nay.

Đối với cá nhân

Đầu tiên, về phía sinh viên. Theo khảo sát từ Đề tài nghiên cứu “Nhận thức của sinh viên ngành CTXH tại các trường cao đẳng, đại học TP.HCM về vấn đề bảo vệ phụ nữ và trẻ em trên KGM” cho thấy được sinh viên nói chung và sinh viên ngành CTXH nói riêng đều có nhận thức tốt về vấn đề bảo vệ phụ nữ và trẻ em trên KGM. Từ nhiều khía cạnh khác nhau dẫn đến cách nhìn nhận của bản thân mỗi sinh viên sẽ khác nhau. Song đó, còn thấy được sinh viên các ngành khác lại có mối quan tâm các vấn đề xã hội nhiều hơn sinh viên ngành CTXH. Phải chăng đó là do bản thân của sinh viên ngành Công tác xã hội chưa tâm huyết với ngành học và việc làm sau này? Để khắc phục tình trạng trên thì trước hết bản thân sinh viên phải là người chủ động trong quá trình học tập và trau dồi tri thức, ngoài tiếp thu các kiến thức được đào tạo trong trường lớp thì sinh viên phải có thêm nhiều mối liên kết với các Chương trình, Hội thảo trong và ngoài khu vực để có cái nhìn thực tế hơn để từ đó nhận diện các vấn đề xảy ra, trước hết là để bảo vệ cho chính bản thân mình và sau đó là bảo vệ cho thân chủ của mình. Sinh viên cần phải chủ động trong quá trình tiếp cận và xử lý các tình huống, qua đó còn giúp cho họ tự bảo vệ mình trước nhiều nguy cơ tiềm ẩn.

Dựa trên kết quả khảo sát của nhóm nghiên cứu, mức độ quan tâm đến các vấn đề xã hội của sinh viên hiện nay đang ở mức cơ bản. Trong tình hình này cần có sự thay đổi ở cá nhân sinh viên, cụ thể sinh viên cần có sự chủ động cập nhật tin tức thời sự về các vấn đề xã hội. Hiện nay tỷ lệ sinh viên tham gia mạng xã hội với số lượng lớn, dựa trên điều này sinh viên có thể dễ dàng cập nhật tin tức một cách nhanh chóng. Sinh viên ngành CTXH là nguồn nhân lực sẽ đóng góp cho xã hội trong tương lai, vì vậy cần tăng cường sự chủ động tiếp cận tin tức, điều này cũng thể hiện được trách nhiệm của sinh

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

viên đối với xã hội. Ngày nay với sự phát triển hiện đại của đất nước, sự tiến bộ của công nghệ số.

4.2. Thuật ngữ viết tắt

STT	Cụm từ đầy đủ	Viết tắt
1.	Thành phố Hồ Chí Minh	TP. HCM
2.	Không gian mạng	KGM
3.	Công tác xã hội	CTXH

5. Kết luận & Khuyến nghị

An ninh mạng trong sinh viên là vấn đề cần được quan tâm trong giai đoạn hiện nay - thời kỳ chuyển đổi số ngày càng được ứng dụng vào mọi hoạt động đời sống của con người.

Qua các kết quả được phân tích, đánh giá cũng như những thực trạng trên cho thấy, nhận thức của sinh viên ngành CTXH hiện nay chỉ đạt mức nhận biết đầy đủ và cũng có sự chênh lệch giữa các năm học và ngành học. Cùng với sự phát triển mạnh mẽ và diễn ra trên nhiều lĩnh vực như công nghệ, kinh tế, xã hội, con người càng ngày càng khẳng định được vị thế và vai trò của mình. Song cùng với sự phát triển này cũng tồn tại những mối nguy hại cụ thể ở đây là trên không gian mạng, các nguy hại mà con người đã và đang đối mặt là xâm hại tình dục, xâm phạm đời tư, bắt nạt, thông tin xấu độc... Có thể nói, nghề CTXH đang trực tiếp tham gia giải quyết những vấn đề xã hội nảy sinh, bức xúc, giải quyết mối quan hệ giữa con người với con người, giảm bất bình đẳng và mâu thuẫn trong xã hội, mang lại niềm vui, hạnh phúc, góp phần thúc đẩy phát triển kinh tế, công bằng tiến bộ xã hội. Việt Nam là nước có số lượng đối tượng cần trợ giúp của các dịch vụ công tác xã hội (CTXH) lớn và để trợ giúp đối tượng yếu thế, Đảng, Nhà nước đã ban hành nhiều chủ trương, chính sách từng bước ổn định và nâng cao đời sống cho đối tượng, bảo đảm an sinh xã hội và phát triển kinh tế - xã hội của đất nước. Đặc biệt, ngày 25 tháng 3 năm 2010, Thủ tướng Chính phủ đã ban hành Quyết định số 32/2010/QĐ-TTg phê duyệt Đề án phát triển nghề CTXH giai đoạn 2010-2020.

Chính vì vậy nghiên cứu nhận thức của sinh viên ngành CTXH về vấn đề bảo vệ phụ nữ và trẻ em trên không gian mạng là một việc rất quan trọng sau khi tìm hiểu về thực trạng nhóm nghiên cứu mạnh dạn nêu ra một số khuyến nghị sau:

Một là, về phía nhà trường. Nhà trường là một trong những môi trường có sự tác động đến sinh viên tương đối nhiều và có thể thay đổi dần nhận thức của sinh viên. Tuy nhiên, hiện nay ở môi trường nhà trường vẫn còn tồn tại những hạn chế, điều này làm trở ngại cho quá trình nâng cao nhận thức của sinh viên. Vì vậy cần có sự thay đổi, điều chỉnh trong khung chương trình học, tăng cường thời gian thực hành, thực tập dành cho sinh viên. Tạo điều kiện cho sinh viên cọ xát với thực tế, Nhà trường luôn quan tâm sâu

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

xát nắm bắt tâm tư nguyện vọng và lắng nghe những ý kiến đóng góp cho ngành trong quá trình học tập và rèn luyện.

Hai là, về từ phía cơ sở thực hành, thực tập. Tạo điều kiện cho sinh viên hiểu sâu hơn về các kỹ năng thực hành xã hội. Cơ sở thực hành, thực tập cần có thêm nhiều liên kết với các cơ sở khác trong và ngoài khu vực để tổ chức nhiều các hoạt động xã hội, chương trình ý nghĩa thu hút sự tham gia đông đảo của sinh viên đồng thời mang đến giá trị to lớn cho xã hội. Không chỉ dành cho sinh viên của ngành CTXH mà còn có cả sinh viên của những ngành khác, với mục đích cùng chung tay nhân cao nhận thức, hiểu biết và những ứng phó trước những nguy cơ tiềm ẩn mà không gian mạng đang gặp phải.

Ba là, các cơ quan chức năng có thẩm quyền cần đẩy mạnh công tác kiểm tra, thanh tra nắm bắt tình hình dư luận xã hội. Mạng xã hội nói riêng và không gian mạng nói chung là môi trường chứa rất nhiều nội dung tiêu cực và tích cực đan xen. Khi đó con người rất khó để phân biệt nếu như họ chưa có những kỹ năng, kiến thức về nhận diện các thông tin chính xác trên KGM. Ngoài ra, thực hiện nghiêm chỉnh các chính sách, quy định, pháp luật nhằm răn đe những hành vi gây nguy hiểm, nguy hại đến danh dự và tính mạng của người khác. Đem lại một môi trường sạch hơn cho KGM, giúp KGM phát huy đúng chức năng và nhiệm vụ của chúng là kết nối, nhanh chóng, thuận lợi và tiết kiệm trong thời kỳ xã hội ngày càng văn minh và tiến bộ như hiện nay.

LỜI CẢM ƠN

Nhóm nghiên cứu xin chân thành cảm ơn những đóng góp, hỗ trợ từ phía Ban Giám đốc, Cô hướng dẫn khoa học, Thầy Cô ở khoa Xây dựng Đảng Học viện Cán bộ Thành phố đã tạo mọi điều kiện thuận lợi để nghiên cứu được thực hiện một cách hoàn chỉnh nhất. Đồng thời, xin chân thành cảm ơn Thầy Cô, các đơn vị, các bạn sinh viên của các trường cao đẳng, đại học tại Thành phố Hồ Chí Minh đã hỗ trợ thực hiện khảo sát, phỏng vấn sâu, tạo điều kiện thuận lợi giúp đề tài được hoàn thiện nhanh chóng, đảm bảo tính khoa học.

Tài liệu tham khảo

Quốc Hội. (2018). Luật An ninh mạng

T.N.V (K8). (2021). Thông tin xấu, độc trên mạng xã hội và trách nhiệm công dân.

Trang điện tử Trường Đại học An ninh nhân dân. Truy cập ngày 28/4/2022 tại: <https://huonghoa.tinhuyquangtri.vn/thong-tin-xau-doc-tren-mang-xa-hoi-va-trach-nhiem-cong-dan>

Trang thông tin điện tử về gia đình (2021). Thực trạng tác động của Internet, thiết bị công nghệ đối với thanh, thiếu, nhi ở Việt Nam hiện nay. Truy cập ngày 21/3/2022 tại: <http://giadinh.bvhttdl.gov.vn/thuc-trang-tac-dong-cua-internet-thiet-bi-cong-nghe-doi-voi-thanh-thieu-nhi-o-viet-nam-hien-nay/>

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Trần Thị Vân Anh. (2006). Quyền con người và quyền của phụ nữ. Tạp chí Nghiên cứu Gia đình và Giới.
- Trung tâm nghiên cứu quyền con người - quyền công dân và Trung tâm nghiên cứu tội phạm học và tư pháp hình sự thuộc Khoa Luật - Đại học Quốc gia Hà Nội (2011). Sách chuyên khảo: “Bảo vệ các nhóm dễ bị tổn thương trong tổ tụng hình sự”. Nxb Đại học Quốc Gia Hà Nội.
- UBND Thành phố Hồ Chí Minh. (2021). Kế hoạch triển khai đề án “Giáo dục thông minh và học tập suốt đời tại Thành phố Hồ Chí Minh giai đoạn 2021-2030” năm 2021 và giai đoạn 2021-2025.

NHẬN THỨC CỦA SINH VIÊN TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN VỀ VẤN ĐỀ AN NINH THÔNG TIN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

Nguyễn Phúc Văn, Nguyễn Thị Diễm My

Trường Đại học An ninh nhân dân

Tác giả liên hệ: nguyenphucvan15@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> An ninh sinh viên, thông tin dữ liệu, đánh cắp thông tin, chuyển đổi số, an ninh thông tin.	Cách mạng công nghiệp lần thứ tư (CMCN 4.0) với sự giao thoa, hòa quyện của các công nghệ số - vật lý - sinh học có tác động cực lớn và phát triển theo cấp số nhân, có thể làm thay đổi hoàn toàn cách thức con người sống, làm việc, điều hành xã hội và đang tác động mạnh mẽ tới an ninh sinh viên của một quốc gia nói chung và an ninh sinh viên trường Đại học An ninh nhân dân nói riêng. Cùng với những lợi ích mà thời kỳ chuyển đổi số mang lại là những rủi ro đang tiềm ẩn như an toàn thông tin, dữ liệu của sinh viên có thể bị đe dọa. Vì vậy, mục đích của bài nhằm tạo ra sự hiểu biết về các mối đe dọa an ninh của sinh viên trong môi trường số, tạo ra sự hiểu biết chung về tầm quan trọng của việc bảo vệ thông tin cá nhân, an toàn trực tuyến cũng như đưa ra các giải pháp giảm thiểu tệ nạn liên quan đến an toàn thông tin trong sinh viên nói chung và sinh viên Trường đại học An ninh nhân dân nói riêng. Trong quá trình nghiên cứu, nhóm tác giả sử dụng phương pháp luận nghiên cứu của Chủ nghĩa duy vật biện chứng và Chủ nghĩa duy vật lịch sử. Đồng thời còn sử dụng một số phương pháp như điều tra khảo sát bằng bảng hỏi, nghiên cứu tài liệu. Bài viết đã lấy khảo sát từ 50 học viên Trường Đại học An ninh nhân dân. Thông qua việc nghiên cứu bài bài viết đã chỉ ra được thực trạng cũng như những thuận lợi, thách thức của sinh viên trong thời kỳ chuyển đổi số và đưa ra những giải pháp để giảm thiểu mất an toàn thông tin, dữ liệu trong thời kỳ chuyển đổi số trong sinh viên Trường đại học An ninh nhân dân hiện nay.

1. Giới thiệu

Trong thời kỳ chuyển đổi số, sinh viên là những người tiếp xúc rất nhiều với Internet. Cùng với sự phát triển vượt bậc của chuyển đổi số đem lại những thuận lợi cho sinh viên nhưng cũng đặt ra những thách thức không nhỏ đối với việc bảo mật thông tin cá nhân. Việc đa số sinh viên các trường đại học hiện nay đều không được trang bị kiến thức đầy đủ về an ninh mạng mang đến những lo ngại khi mà tốc độ chia sẻ lan rộng thông tin ngày càng nhanh chóng.

Đây là cơ hội cho tội phạm mạng tấn công và lấy cắp dữ liệu cá nhân của sinh viên. Vì vậy, làm sao để giảm thiểu nạn đánh cắp thông tin cá nhân trong thời kỳ chuyển đổi số là vấn đề nan giải. Bài viết này sẽ đưa ra khái quát một số vấn đề liên quan đến an ninh mạng trong cách mạng 4.0 và chuyển đổi số, các mối đe dọa an ninh mà sinh viên đang phải đối mặt, những thách thức đặt ra cho sinh viên trong tương lai đồng thời đưa ra một số giải pháp để khắc phục đến mức thấp nhất vấn đề trên.

2. Cơ sở lý thuyết

An ninh mạng và vấn đề an ninh mạng trong thời kỳ chuyển đổi số là một vấn đề không lạ. Tuy nhiên, việc nghiên cứu sâu vấn đề này trong sinh viên nói riêng vẫn còn khá mới mẻ và hầu như chưa được khai thác đúng cách. Điều đó làm cho tình hình mất an toàn thông tin trong sinh viên diễn ra khá thường xuyên và rất phức tạp.

Một số công trình nghiên cứu có liên quan đến đề tài như “Những điểm nhấn về an toàn, an ninh mạng Việt Nam năm 2020” của tác giả Minh Vân; “Nhận biết và ngăn chặn hành vi đánh cắp dữ liệu” của tác giả Nguyễn Công Minh được in trên Chuyên Đề Công nghệ và ngân hàng số 1 tháng 1 năm 2021, “Đảm bảo an ninh thông tin trong chuyển đổi số” của TS. Mai Diệu Anh được in trên tạp chí Tuyên giáo Trung ương ngày 1/5/2023.

Trên cơ sở tham khảo các công trình nghiên cứu trên và các nguồn tài liệu khác nhóm nghiên cứu đã đi sâu tìm hiểu vấn đề an ninh trong chính môi trường giáo dục cụ thể là tình hình an ninh trong sinh viên Trường Đại học An ninh nhân dân trong thời kỳ chuyển đổi số.

3. Phương pháp nghiên cứu

Trong quá trình nghiên cứu, nhóm tác giả sử dụng phương pháp luận nghiên cứu của Chủ nghĩa duy vật biện chứng và Chủ nghĩa duy vật lịch sử; đồng thời còn sử dụng một số phương pháp như điều tra khảo sát bằng bảng hỏi, nghiên cứu tài liệu.

4. Kết quả nghiên cứu

4.1. Vấn đề an ninh mạng trong cách mạng 4.0 và chuyển đổi số

4.1.1. Thực trạng an toàn thông tin mạng trên thế giới

Trong cuộc CMCN 4.0, thông tin là một dạng tài nguyên. Chính vì thế, đảm bảo an ninh, an toàn thông tin là nhiệm vụ quan trọng và cấp thiết. Tuy nhiên, hiện nay các

mối đe dọa từ không gian mạng không ngừng tăng lên và thay đổi nhanh chóng. Ví dụ như các vụ tấn công vào hệ thống thư điện tử của Bộ Ngoại giao Mỹ, hệ thống máy tính của Nhà trắng, Hạ viện Đức, Bộ Ngoại giao Australia,... Các loại tội phạm mạng hiện nay không chỉ tấn công vào thông tin của các cơ quan tổ chức mà còn tấn công vào hệ thống dữ liệu sinh viên của các trường Đại học. Việc bị đánh cắp thông tin của chính sinh viên gây ra những hậu quả cả về kinh tế lẫn tệ nạn xã hội.

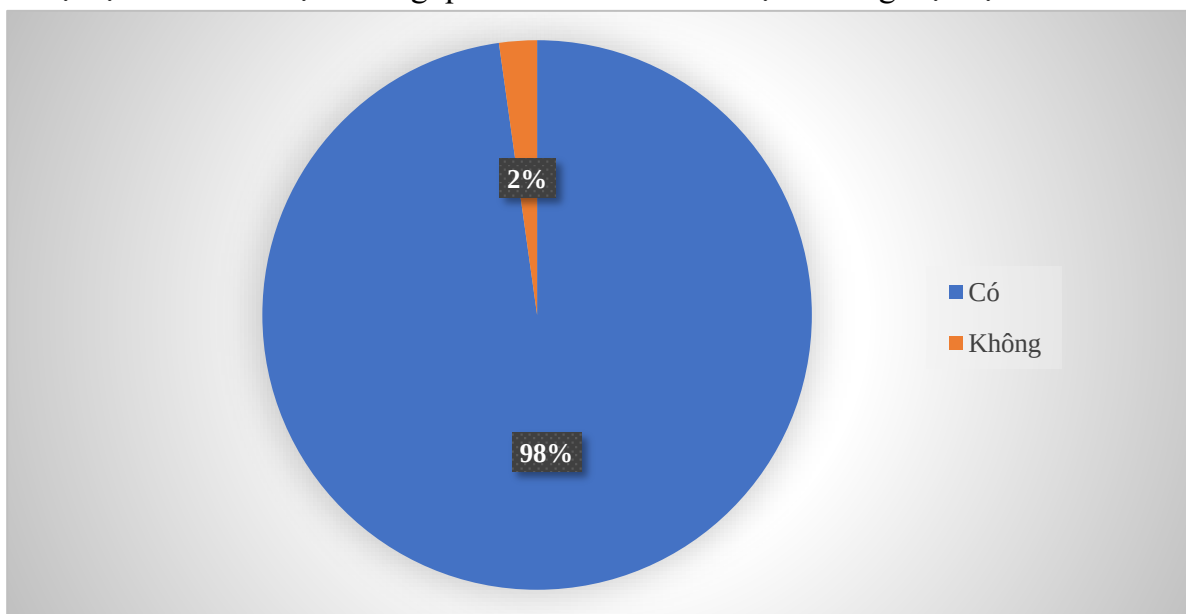
Tình hình an toàn thông tin mạng nhất là việc đánh cắp dữ liệu các nhân diện biến phức tạp, liên tục xảy ra các vụ tấn công, xâm nhập, đánh cắp dữ liệu trên hệ thống mạng của các cơ quan tổ chức giáo dục để lấy thông tin, dữ liệu của sinh viên của nhiều quốc gia.

Tài chính là mục tiêu lớn nhất để các tội phạm thực hiện việc đánh cắp thông tin dữ liệu.²

4.1.2. Thực trạng an toàn thông tin ở Việt Nam

Thực tế chuyển đổi số cũng đặt ra nhiều thách thức bởi lẽ khi toàn bộ hoạt động của con người được chuyển lên môi trường mạng thì chỉ cần một sự cố an ninh thông tin nghiêm trọng có thể làm cản trở chương trình chuyển đổi số của cả một ngành, một địa phương hay một doanh nghiệp cũng như đe dọa gây ra hậu quả khó lường.

Ở Việt Nam, trung bình mỗi người hoạt động trực tuyến khoảng 7-8 tiếng. Thời gian này càng gia tăng thì nguy cơ mất an ninh thông tin mạng lại càng cao. Nhất là trong bối cảnh tình hình an ninh thông tin ở Việt Nam đã và đang có những diễn biến phức tạp, tiềm ẩn nhiều rủi ro và nguy cơ đối với an ninh con người, an ninh quốc gia và trật tự an toàn xã hội. Thông qua khảo sát sinh viên tại Trường Đại học An ninh nhân



² ThS. Lâm Đông Hồ - ThS. Nguyễn Xuân Hoàng (2022), “Thực trạng an toàn thông tin mạng hiện nay ở Việt Nam và giải pháp phòng chống vi phạm pháp luật trên không gian mạng”, Tạp chí Công Thương - Các kết quả nghiên cứu khoa học và ứng dụng công nghệ, Số 23.

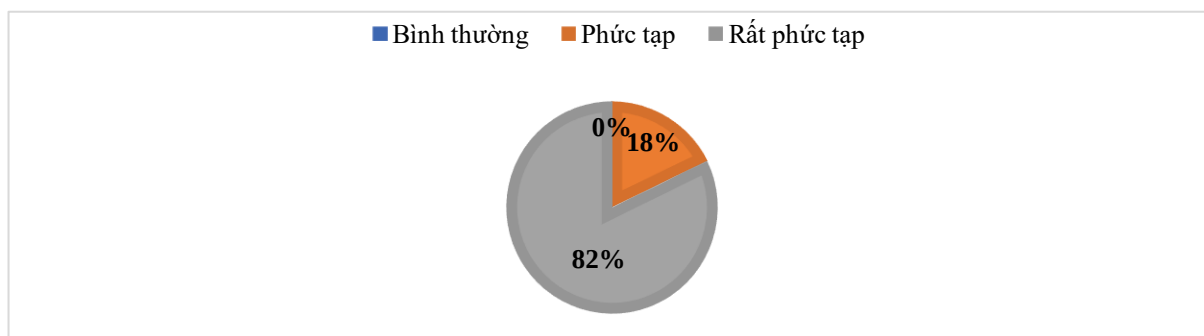
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

dân thì có đến 98% sinh viên cho rằng vấn đề an ninh sinh viên trong thời kỳ chuyển đổi số là thật sự cần thiết “xem hình 1”.

Hình 1: Vấn đề an ninh sinh viên có thật sự cần thiết không?

Sinh viên là nguồn nhân lực có vị trí, vai trò to lớn, là người chủ tương lai của đất nước, là nhân tố quan trọng quyết định vận mệnh của dân tộc. Trong suốt quá trình lãnh đạo cách mạng Việt Nam Chủ tịch Hồ Chí Minh luôn dành sự quan tâm đặc biệt đến việc giáo dục thế hệ trẻ, phát huy được sức mạnh to lớn của sinh viên làm động lực phát triển kinh tế xã hội đảm bảo an ninh, quốc phòng cho đất nước. Tuy nhiên, việc chuyển đổi số quá nhanh trong bối cảnh hiện nay bên cạnh những thuận lợi cũng gây ra không ít những thách thức nhất là về vấn đề an ninh thông tin trong sinh viên nói chung và sinh viên Trường Đại học An ninh nhân dân nói riêng.

Thật vậy, theo khảo sát của nhóm chúng tôi có đến 62,2% sinh viên Trường Đại học An ninh nhân dân tham gia khảo sát đã từng bị đánh cắp thông tin cá nhân. Trong số các sinh viên Trường Đại học An ninh nhân dân được khảo sát có tới 18% cho rằng việc đánh cắp thông tin, dữ liệu trong thời kỳ chuyển đổi số đang diễn ra phức tạp, trong



khi đó số cho rằng rất phức tạp chiếm tới 82% “xem hình 2”.

Hình 2: Việc đánh cắp thông tin dữ liệu trong thời kỳ chuyển đổi số đang diễn ra như thế nào?

Trung tuần tháng 8/2021, trên diễn đàn Raidforums, tài khoản có tên xiaolin1983 đã đăng bán dữ liệu của hơn 300.000 sinh viên được cho là của 10 trường đại học tại Việt Nam. Những hồ sơ này bao gồm rất nhiều dữ liệu nhạy cảm như họ tên, địa chỉ, số điện thoại, tài khoản ngân hàng, hình ảnh chứng minh nhân dân của nạn nhân.

Việc tài khoản rao bán này đã chia sẻ các dữ liệu bao gồm các thông tin cụ thể như họ tên, địa chỉ, số điện thoại, tài khoản ngân hàng, hình ảnh chứng minh nhân dân, hộ chiếu, khóa học, lớp học, thậm chí là tên của cha mẹ nạn nhân và công việc của họ. Điều đó đã gây ra tâm lý bất an cho nạn nhân và gia đình của họ.

Theo thống kê của Bộ Công an, đã có rất nhiều vụ để lộ lộ thông tin cá nhân thời gian qua. Điển hình như các vụ:

+ Công ty VNG để lộ hơn 163 triệu tài khoản khách hàng;

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

+ Tin tặc đã tấn công vào hệ thống máy chủ của một hãng hàng không, đăng tải lên Internet 411.000 tài khoản khách hàng thành viên;

+ Vụ gần 10.000 chứng minh nhân dân, căn cước công dân bị rao bán trên một diễn đàn tin tặc;

+ Dữ liệu khách hàng của Công ty FPT Shop bị đăng tải công khai trên mạng;

Và rất nhiều các vụ thông tin khách hàng bị lộ, lọt do các công ty môi giới dịch vụ taxi sử dụng để mời chào khách hàng.³

Các chuyên gia bảo mật cũng khuyến cáo người dùng hết sức cẩn thận với thông tin cá nhân, tuyệt đối không chia sẻ, cung cấp thông tin cá nhân xác định danh tính cho những đơn vị chưa rõ uy tín hoặc đáng ngờ, mỗi cá nhân cần trang bị kiến thức tốt để phòng tránh các tình huống lừa đảo có thể xảy ra.⁴

Theo Cục An toàn thông tin (Bộ Thông tin và Truyền thông), chỉ có khoảng 20% nguyên nhân để lọt, lộ thông tin cá nhân thuộc về nhà cung cấp dịch vụ nhưng có tới 80% nguyên nhân lộ lọt thông tin cá nhân là xuất phát từ chính sự bất cẩn của người dùng chiếm phần lớn trong số đó là sinh viên. Hầu hết các nhà cung cấp dịch vụ đều đòi hỏi cung cấp dữ liệu cá nhân, như tên tuổi, địa chỉ nhà, số điện thoại, nhà mạng. Trong nhiều trường hợp, sinh viên chấp nhận đánh đổi việc cung cấp dữ liệu cá nhân để sử dụng các nền tảng dịch vụ.⁵

Thực tế, trong nhiều trường hợp, sinh viên còn thờ ơ với việc bảo vệ thông tin cá nhân, tình trạng vô tình để lộ lọt thông tin cá nhân vẫn còn phổ biến có thể gây tác hại khôn lường, như những clip ngắn đăng trên TikTok, cung cấp số điện thoại, thậm chí địa chỉ nhà, số tài khoản cá nhân... trên những trang web bán hàng online.

Cục An Ninh mạng và phòng chống tội phạm sử dụng Công nghệ cao, Bộ Công an cũng đưa ra nhận định, cùng với sự phát triển của công nghệ thông tin, việc kết nối, chia sẻ thông tin ngày càng trở nên dễ dàng hơn. Đây chính là kẽ hở để nhiều đối tượng lợi dụng để đánh cắp thông tin cá nhân.

Bộ Công an cho biết, thẻ Căn cước công dân (CCCD) gắn chip điện tử được thiết kế với độ bảo mật cao. Tuy nhiên trường hợp người dân tự ý đăng tải, chia sẻ hình ảnh CCCD;

³ <https://vtv.vn/xa-hoi/nhan-dien-thu-doan-danh-cap-thong-tin-ca-nhan-20220402165440152.htm>, Tham khảo ngày 26/8/2023

⁴ <https://antoanthongtin.vn/hacker-malware/ro-ri-du-lieu-ho-so-cua-300000-sinh-vien-viet-nam-107437>, Tham khảo ngày 26/8/2023

⁵ <https://special.nhandan.vn/bao-ve-du-lieu-ca-nhan-trong-moi-truong-so/index.html>, Tham khảo ngày 26/8/2023

cung cấp thông tin CCCD cho những dịch vụ không thiết yếu, các dịch vụ không có cam kết bảo đảm an toàn thông tin cá nhân hay cho người khác mượn CCCD nếu không có mục đích chính đáng sẽ dẫn tới nhiều hệ lụy nghiêm trọng.⁶

Bên cạnh đó, nguyên nhân chính để lọt thông tin cá nhân của sinh viên là do nhóm đối tượng này thường xuyên đăng tải hình ảnh thông tin cá nhân của họ lên mạng xã hội, hay nhấp vào các đường link lạ được các đối tượng xấu gửi đến cũng như họ không sử dụng mật khẩu đủ mạnh để tham gia mạng xã hội nên dễ dàng bị hacker chiếm dụng tài khoản.

4.2. Các mối đe dọa an ninh mà sinh viên Đại học An ninh nhân dân đang phải đối mặt trong thời kỳ chuyển đổi số

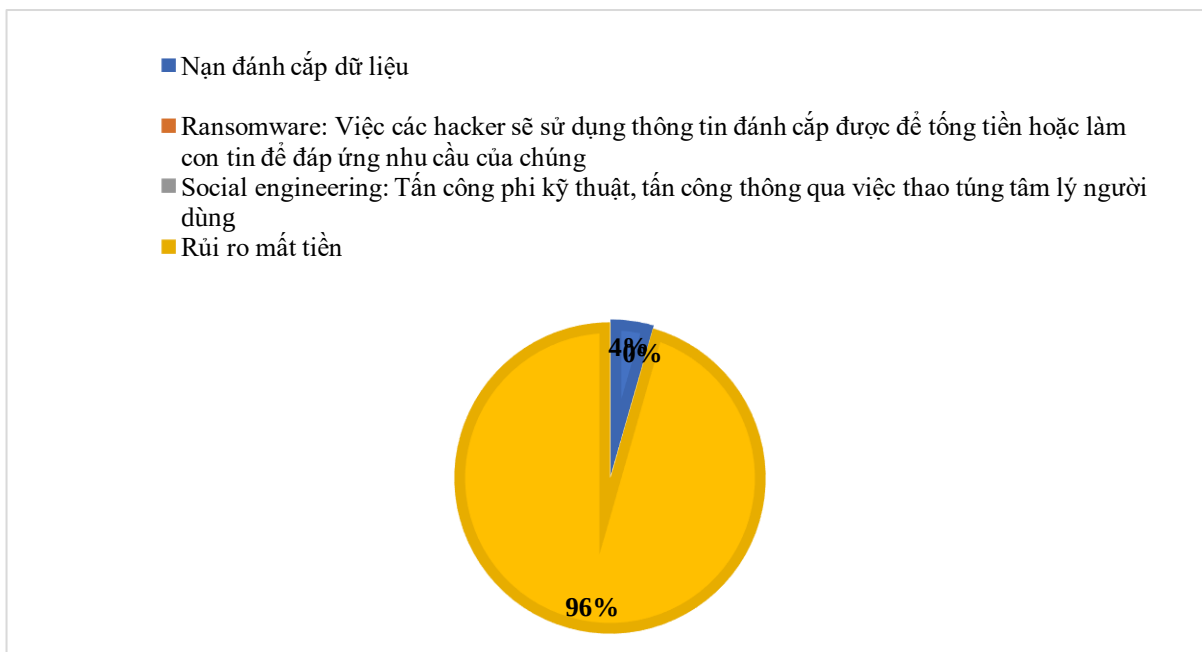
Bên cạnh những thuận lợi mà chuyển đổi số mang lại cho sinh viên như sinh viên được tiếp cận thông tin một cách nhanh chóng, dữ liệu thông tin cá nhân được lưu trữ một cách dễ dàng thì cũng xuất hiện các mối đe dọa đã và đang xảy ra đe dọa đến an ninh của sinh viên Đại học An ninh nhân dân.

Thứ nhất, đánh cắp dữ liệu. Thông tin cá nhân của sinh viên Trường Đại học An ninh nhân dân rất có giá trị với tin tặc. Chúng có thể dùng thông tin này rao bán kiếm lợi nhuận hay dùng nó để thực hiện các hành vi phi pháp ảnh hưởng đến hình ảnh và uy tín của học viên.

Vụ việc tin tặc rao bán dữ liệu của 30 triệu học sinh, giáo viên Việt Nam trên một diễn đàn gây ra hoang mang trong dư luận nói chung và cộng đồng sinh viên nói chung. Những thông tin này bị lộ ảnh hưởng nghiêm trọng đến tâm lý, cuộc sống của sinh viên. Phần lớn các cơ sở giáo dục đều lưu giữ thông tin của người dùng nên đây là nơi tin tặc thường xuyên muốn tấn công.

Thứ hai, nạn tống tiền. Thông qua khảo sát khi sinh viên được hỏi đâu là mối đe dọa đến an ninh sinh viên trong chuyển đổi số thì vấn đề rủi ro mất tiền được đến 96% sinh viên cho rằng đây là mối đe dọa lớn nhất “xem hình 3”.

⁶ <https://vtv.vn/xa-hoi/nhan-dien-thu-doan-danh-cap-thong-tin-ca-nhan-20220402165440152.htm>, Tham khảo ngày 26/8/2023



Hình 3: Đây là mối đe dọa đến an ninh sinh viên trong chuyển đổi số hiện nay?

Nạn tống tiền này là việc các hacker sẽ sử dụng thông tin đánh cắp được để tống tiền hoặc làm cho con tin mà chúng nắm giữ bí mật phải làm theo để đáp ứng các yêu cầu của chúng. Những thông tin được đánh cắp thường là thông tin cá nhân quan trọng của người dùng như tên, địa chỉ, số điện thoại, hình ảnh nhạy cảm... Ngoài ra, ở các sở giáo dục còn là trung tâm lưu trữ và nắm giữ thông tin, dữ liệu có trí tuệ cao nên tội phạm mạng rất muốn đánh cắp những thông tin này.

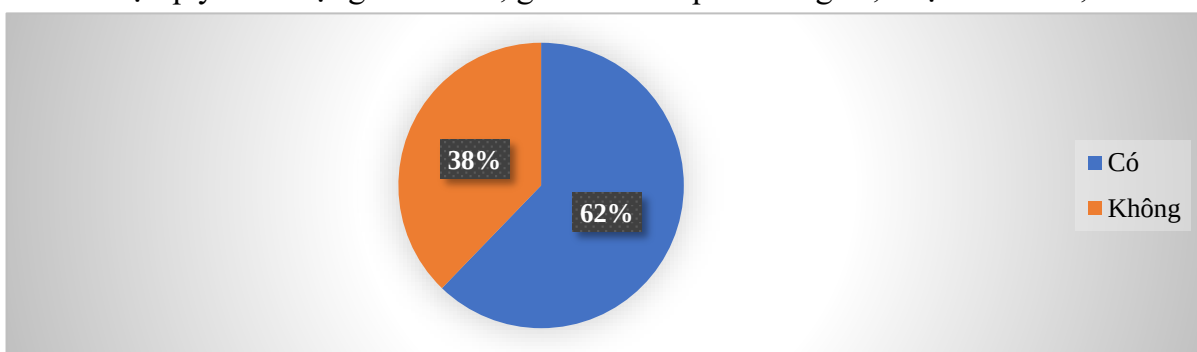
Thứ ba, social engineering (tấn công phi kỹ thuật). Các vụ tấn công mạng thông qua việc thao túng tâm lý người dùng là mối đe dọa an ninh mạng hàng đầu mà ngành giáo dục và sinh viên phải đối mặt. Các tin tặc sẽ khai thác những thói quen và sự tò mò khiến người dùng tiết lộ những thông tin bí mật và quan trọng. Sinh viên là đối tượng mà hacker nhắm đến do những thói quen như thường xuyên lướt mạng xã hội, web chơi game. Đây là những nơi lý tưởng để chúng chèn vào những đường link độc hại.

Cuối cùng, về rủi ro mất tiền. Hacker cũng có thể tấn công vào tài khoản ngân hàng của sinh viên khi đánh cắp được những thông tin này. Chúng thường sẽ gửi những link lạ - mà mã nguồn là tên các ngân hàng để khiến sinh viên truy cập vào đổi mật khẩu sau đó chúng sẽ chiếm được tài khoản ngân hàng và đương nhiên tiền trong tài khoản sẽ không cánh mà bay. Việc các mật khẩu tài khoản ngân hàng, mật khẩu điện thoại quá dễ đoán như ngày tháng năm sinh cũng rất dễ để các đối tượng xấu lợi dụng để chiếm đoạt tiền.

4.3. Các giải pháp giảm thiểu tệ nạn xã hội của sinh viên trong thời kỳ chuyển đổi số

Tệ nạn xã hội hiện nay được xác định là các hiện tượng trong xã hội mang tính chất phổ biến trong đời sống xã hội có giai cấp, tệ nạn xã hội được biểu hiện ở những hành vi sai lệch so với chuẩn mực xã hội, những hành vi vi phạm đạo đức và vi phạm pháp luật mà hậu quả của những hành vi này là gây tác động xấu về mọi mặt đối với đời sống xã hội, làm cản trở tiến bộ xã hội của nền văn hóa lành mạnh.

Nước ta hiện nay có rất nhiều tệ nạn xã hội, trong đó có một số tệ nạn xã hội phổ biến thường xảy ra hiện nay như: ma túy, cờ bạc, mại dâm, mê tín dị đoan, rượu bia, trộm cắp, tham ô, xâm hại tình dục,... Dưới góc độ nghiên cứu của bài tham luận, nhóm tác giả chỉ đề cập đến vấn đề tệ nạn xã hội của sinh viên trong thời kỳ chuyển đổi số có thể là: lừa đảo nhận quà từ nước ngoài, lừa đảo tuyển cộng tác viên bán hàng trên các sàn thương mại điện tử (shopee, lazada, tiktok shop,...), lừa đảo kêu gọi đầu tư tài chính, tiền ảo, lừa đảo trúng thưởng (thông qua các trang mạng xã hội như: zalo, facebook, telegram,...) mạo danh thông báo của ngân hàng, tổ chức tín dụng,... để chiếm đoạt quyền sử dụng tài khoản, giả danh cơ quan Công an, Viện kiểm sát, Tòa án.



Trên kết quả nghiên cứu khảo sát của sinh viên trường Đại học An ninh nhân dân từ 50 người, khi được hỏi sinh viên đã từng bị đánh cắp thông tin chưa thì có đến 62% trả lời là có và 38% trả lời là chưa từng “xem hình 4”.

Hình 4: Đồng chí đã từng bị đe dọa thông tin của chính mình chưa?

Qua đó có thể nhận thấy rằng vấn đề đánh cắp thông tin đang là vấn đề nhức nhối đối với bất kỳ cá nhân nào.

Thứ nhất, các đối tượng sẽ giả danh cán bộ Công an, Viện Kiểm sát, Tòa án gọi điện cho sinh viên để thực hiện hành vi lừa đảo, gây sức ép, yêu cầu khác nhau như: Phục vụ điều tra, làm sinh viên hoang mang... Từ đó, phải chuyển một số tiền lớn vào một tài khoản do các đối tượng này cung cấp.

Thứ hai, lừa đảo qua mạng xã hội, cụ thể như sau: Chiếm quyền điều khiển tài khoản mạng xã hội của người bị hại, tiếp tục tạo ra các kịch bản nhấn tin lừa đảo đến danh sách bạn bè của người bị hại; kết bạn qua mạng xã hội và hứa hẹn gửi quà có giá trị... Sau đó, yêu cầu nạn nhân chuyển tiền nộp thuế hoặc lệ phí hải quan nhằm chiếm

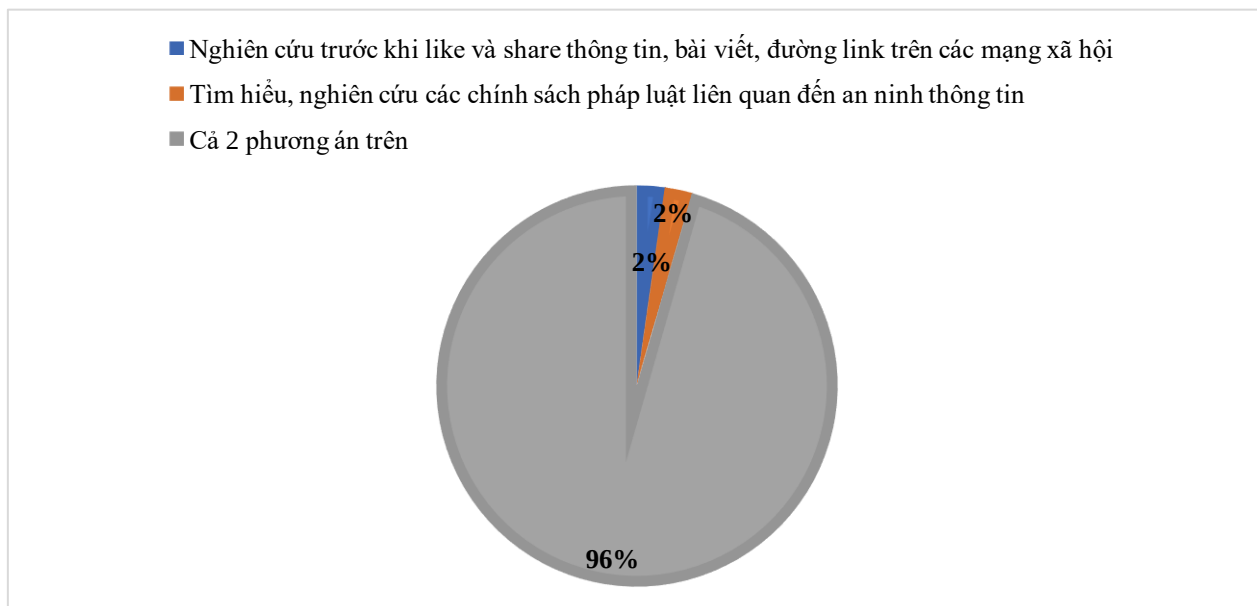
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

đoạt tiền; hoặc gửi tin nhắn qua Facebook, Zalo... thông báo trúng thưởng và đề nghị nộp phí để nhận thưởng.

Thứ ba, tội phạm lừa đảo chiếm đoạt tài sản thông qua hoạt động thương mại điện tử như: Các đối tượng mở các trang cá nhân bán hàng online, đặt hàng, sau đó quảng cáo, rao bán các mặt hàng, yêu cầu bị hại chuyển khoản đặt cọc. Sau khi nhận cọc hay được chuyển khoản trước để đặt mua hàng, đối tượng không giao hàng hoặc giao hàng giả, hàng kém chất lượng, chúng thường khóa trang mạng của mình hoặc xóa hẳn để xóa dấu vết, bỏ số điện thoại và chiếm đoạt tài sản của bị hại.

Khi các tội phạm công nghệ cao đánh vào tâm lý của sinh viên là đang rất cần tiền để sử dụng vào mục đích sinh hoạt học tập, do đó chúng đưa ra những việc làm có mức thu nhập hấp dẫn dễ dàng thực hiện ở bất cứ lúc nào và bất cứ nơi đâu. Nhiều sinh viên tham gia vào để kiếm thêm thu nhập, nhưng thật chất đã rơi vào cái bẫy do bọn tội phạm đặt ra, nhiều sinh viên bị mất tiền, bị mất tài khoản và còn bị lợi dụng tài khoản của cá nhân để mượn tiền người thân gia đình bạn bè. Trước những thiệt hại nặng nề đó đối với mỗi người sinh viên nói chung đặc biệt là sinh viên Trường Đại học An ninh nhân dân nói riêng phải hết sức cảnh giác, tỉnh táo và thận trọng trước những âm mưu và thủ đoạn lừa gạt của tội phạm công nghệ cao.

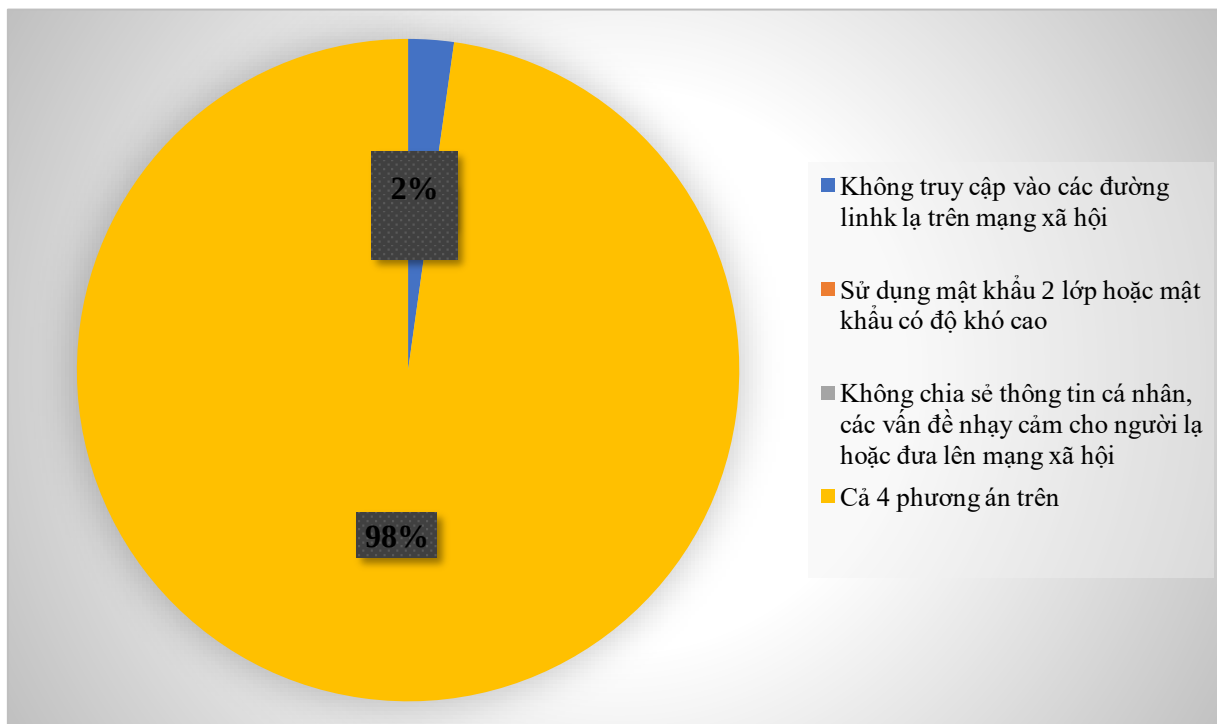
Qua kết quả khảo sát khi được hỏi cần làm gì để bảo đảm an ninh thông tin của sinh viên trong quá trình chuyển đổi số thì có đến 96% cho rằng cần phải nghiên cứu kỹ lưỡng trước khi like và share thông tin trên các trang mạng xã hội, tìm hiểu nghiên cứu các chính sách pháp luật liên quan đến vấn đề an ninh thông tin “xem hình 5”.



Hình 5: Cần làm gì để đảm bảo an ninh thông tin của sinh viên An ninh trong thời kỳ chuyển đổi số?

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Bên cạnh đó, sinh viên còn phải thường xuyên học tập nâng cao nhận thức về phòng chống tệ nạn xã hội. Tham gia tuyên truyền phòng chống tội phạm sử dụng công nghệ cao. Thông qua khảo sát thì có đến 98% sinh viên lựa chọn những cách để bảo vệ thông tin cá nhân như: Không truy cập vào các đường link lạ trên mạng xã hội, sử dụng mật khẩu 2 lớp hoặc mật khẩu có độ khó cao, không chia sẻ thông tin cá nhân các vấn đề nhạy cảm cho người lạ hoặc đưa lên mạng xã hội



đề nhạy cảm lên mạng xã hội “xem hình 6”.

Hình 6: Đây là cách để bảo vệ thông tin cá nhân trong thời kỳ chuyển đổi số?

4.4. Những thách thức đặt ra cho an ninh sinh viên trong tương lai

Với sự phát triển của chuyển đổi số, sinh viên sẽ phải đối mặt với những vấn đề vượt khỏi tầm kiểm soát của bản thân.

Thứ nhất, đó là vấn đề nghiện game online và các mạng xã hội.

Mạng xã hội đã trở thành một không gian tuyên truyền, phổ biến tư tưởng, là kênh thông tin phổ biến trong đời sống xã hội, có tác động mạnh mẽ đến suy nghĩ, nhận thức và hành động của mỗi người. Theo Điều tra quốc gia về vị thành niên và thanh niên Việt Nam năm 2013, tỷ lệ thanh niên sử dụng internet đạt 73%. Hơn 60% thanh, thiếu niên truy cập mạng để tán gẫu và chơi game. Trong số đó, một bộ phận thanh, thiếu niên say mê với game online, mạng internet đến mức nghiện. Việc nghiện game online, mạng internet khiến sức khỏe bị suy nhược, như dễ rối loạn giấc ngủ, não bộ, cột sống bị tổn thương, thị lực kém, trí nhớ suy giảm, thậm chí đe dọa đến tính mạng. Tình trạng nghiện game online, mạng internet được so sánh như nghiện ma túy, không thể tập trung vào công việc và học tập dẫn đến kết quả xấu, thậm chí bị đuổi việc, thôi học. Người nghiện thường chìm đắm trong thế giới ảo, xa rời thực tế và gia đình. Bên cạnh đó, việc nghiện game cũng dẫn đến những tệ nạn xã hội như trộm cắp, cướp của. Trong những năm gần

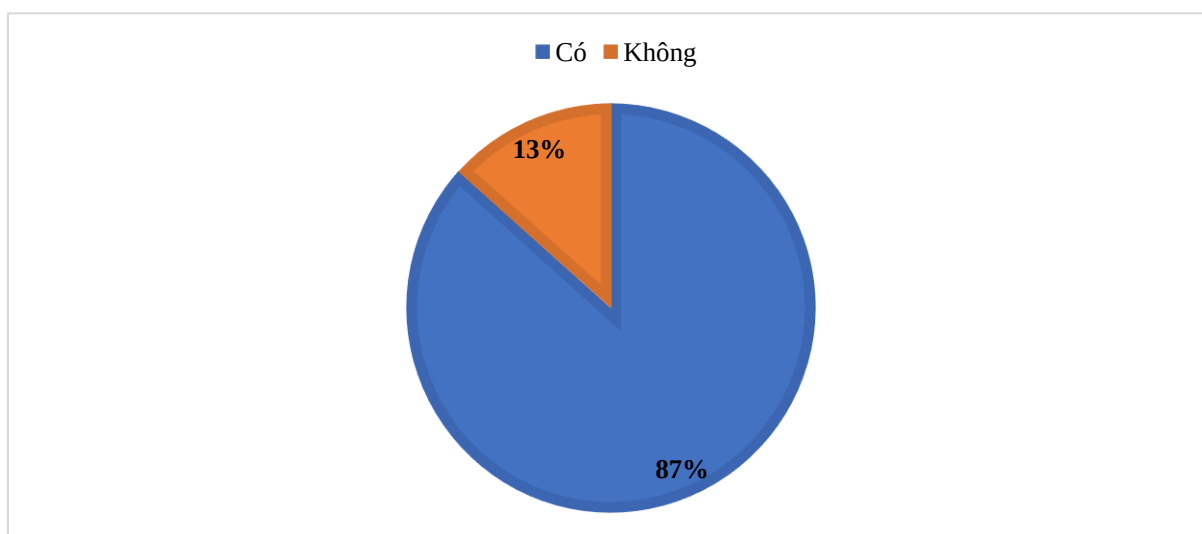
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

đây đã xuất hiện những vụ án mạng, giết người cướp của do con nghiện game, cần tiền để chơi.

Hệ quả là những người nghiện đánh mất an ninh cho bản thân, làm suy giảm hay đánh mất vai trò chủ thể đối với không ít quyền của mình, từ quyền cá nhân (ăn, uống, ở, mặc, đi lại, vui chơi, giới tính) đến quyền xã hội (dân sự, chính trị, kinh tế, xã hội, văn hóa). Đồng thời, tạo thêm gánh nặng cho Nhà nước và các tổ chức xã hội trong việc thực hiện nghĩa vụ bảo đảm an ninh con người. Người nghiện là người tự làm hại hay tàn phá bản thân họ, đồng thời tạo ra mối nguy hại đối với xã hội. Việc nghiện game online, mạng xã hội, góp phần làm gia tăng các tội phạm hình sự như trộm cắp, cướp của, giết người.

Thứ hai, những thách thức từ thông tin mạng xã hội. Thông tin xã hội (các mạng xã hội, các trang web,...) hấp dẫn người dùng ở việc trên các trang đó người dùng nhất là sinh viên với tuổi đời còn khá trẻ dễ dàng phát ngôn ra những từ, đăng những clip để mua vui hay thậm chí có nhiều sinh viên được mệnh danh là “anh hùng bàn phím”, sẵn sàng bày tỏ một ý kiến cá nhân đối với một sự việc nào đó mà không quan tâm tới hậu quả như thế nào. Hiện nay, việc đăng thông tin cá nhân hoặc thông tin của người khác có thể là người thân, bạn bè hay đồng nghiệp,... diễn ra phổ biến và là một phần không thể thiếu của thông tin xã hội. Hệ quả là hồ sơ của các cá nhân bị chia sẻ công khai và có thể trở thành đề tài đàm tiếu có tính xúc phạm trong đời sống thường nhật. Bất luận hậu quả tâm lý là tốt hay xấu, việc đăng tải thông tin cá nhân là hoàn toàn vi phạm quyền riêng tư của họ, đặc biệt đối với trẻ em, học sinh, sinh viên, người khuyết tật,...

Qua khảo sát, sinh viên khi được hỏi hiện nay đã có chính sách pháp luật để bảo vệ an ninh thông tin chưa thì 87% sinh viên trả lời là có và 13% sinh viên cho rằng chưa “xem hình 7”.



Hình 7: Hiện nay đã có chính sách pháp luật để bảo vệ an ninh thông tin chưa?

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Qua đó, có thể thấy hầu hết sinh viên đều tự tìm tòi và trang bị cho mình một nền tảng kiến thức pháp luật vững chắc để bảo vệ mình, gia đình và bạn bè trước sự diễn biến phức tạp của thời kỳ chuyển đổi số. Theo Bộ luật Dân sự (sửa đổi) năm 2015 và Luật An ninh Thông tin Mạng (tháng 7-2016), nếu bí mật đời tư của công dân bị xâm phạm thì cá nhân có quyền trình báo cơ quan công an để ngăn chặn hành vi này, đồng thời ngăn chặn việc phát tán những thông tin đó hoặc có quyền yêu cầu Tòa án ra quyết định buộc người vi phạm, cơ quan, tổ chức, cá nhân có liên quan phải thu hồi, tiêu hủy, chấm dứt việc sử dụng hình ảnh, bồi thường thiệt hại và áp dụng các biện pháp xử lý khác theo quy định của pháp luật. Người thực hiện hành vi quay lén có thể bị xem xét xử lý hình sự về tội “Làm nhục người khác” hoặc “Truyền bá văn hóa phẩm đồi trụy” nếu cố tình chia sẻ, phát tán hình ảnh có nội dung nhạy cảm của người bị quay. Người vi phạm có thể bị phạt cải tạo không giam giữ đến 3 năm hoặc phạt tù từ 6 tháng đến 20 năm tùy theo mức độ vi phạm.

Cuối cùng, là một sinh viên của nhà trường, một chiến sĩ Công an nhân dân trong tương lai thì mỗi sinh viên phải cảnh giác trước những âm mưu lợi dụng các trang mạng xã hội để chống phá Đảng và Nhà nước của các thế lực thù địch và phản động. Ở Việt Nam, thời gian qua, lợi dụng tính chất rộng mở, tự do của mạng xã hội, các thế lực thù địch dưới sự hậu thuẫn của các tổ chức, phần tử phản động từ nước ngoài luôn tìm cách thay đổi hệ tư tưởng và chế độ chính trị ở nước ta. Nhiều lực lượng thù địch, phản động đã lập ra các trang web, các kênh trên nền tảng mạng xã hội trực tuyến như Facebook, Instagram, Youtube... tuyên truyền sai sự thật, xúi giục, kích động hằn thù, gây chia rẽ nội bộ trong nước; kêu gọi người dân trong nước đi theo họ và tiến hành các hành vi gây rối, làm mất trật tự trị an; thậm chí còn kết nối, tập hợp lực lượng qua mạng xã hội nhằm chuẩn bị cho các cuộc bạo loạn, lật đổ, chống đối Đảng, Nhà nước ta.

Các thế lực thù địch, phản động, các phần tử cơ hội, chống đối cũng xác định mạng xã hội là mặt trận chính để thực hiện các hoạt động thông tin, tuyên truyền xuyên tạc nhằm chống phá hệ tư tưởng của đất nước ta với những hình thức rất đa dạng, tinh vi, như: dùng các bài viết, các tài liệu sai sự thật; các sản phẩm sách nói audio đánh tráo khái niệm, các video được cắt ghép bối cảnh, hoặc các bài nghiên cứu với việc sử dụng nhiều quan niệm, khái niệm không phù hợp với nhận thức và điều kiện lịch sử - văn hóa của dân tộc ta...

Bằng luận điệu “du nhập ngoại lai”, “nhập khẩu lý luận”, đánh tráo, thay thế các khái niệm, thổi phồng cái gọi là “chủ thuyết phát triển mới”; chúng trích dẫn cắt xén, nửa vời những quan điểm của chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh; xuyên tạc, làm méo mó các quan điểm của Đảng và hệ tư tưởng mácxít ở nước ta, hòng làm cho cán bộ, đảng viên và nhân dân hoang mang, dao động, suy giảm niềm tin vào sự lãnh đạo của Đảng, vào chủ nghĩa xã hội và con đường đi lên chủ nghĩa xã hội ở nước ta, làm

cho người đọc mất phương hướng, lẫn lộn, không phân biệt được đúng - sai; bôi nhọ, phủ nhận chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh⁷.

Đây chính là mảnh “đất màu mỡ” để các thế lực thù địch, chống đối gieo rắc tư tưởng sùng bái quyền dân sự, quyền chính trị theo mô hình của phương Tây, phớt lờ các thành tựu của nước ta về dân chủ, về quyền con người đã được Liên hợp quốc và các tổ chức quốc tế khác công nhận.

5. Kết luận

Qua những nghiên cứu trên đây, chúng ta thấy rằng vấn đề an ninh mạng trong thời kỳ chuyển đổi số là một vấn đề hết sức phức tạp và vô cùng quan trọng nhất là đối với sinh viên thế hệ trẻ của đất nước. Thông qua việc nghiên cứu tài liệu và thực hiện khảo sát nhóm chúng tôi đã làm sáng tỏ nhận thức của sinh viên đối với vấn đề an ninh thông tin, từ đó đưa ra những giải pháp để hạn chế đến mức thấp nhất những thách thức mà sinh viên phải đối mặt như tuyên truyền, nâng cao ý thức pháp luật trong sinh viên nói chung và sinh viên Trường Đại học An ninh nhân dân nói riêng, thường xuyên kiểm tra cài đặt quyền riêng tư, không truy cập vào những đường link lạ, không chia sẻ những thông tin cá nhân của bản thân, gia đình và bạn bè lên mạng xã hội để tránh bị kẻ xấu lợi dụng và gây ra những hậu quả nặng nề.

LỜI CẢM ƠN

Để thực hiện và hoàn thành bài tham luận này, chúng tôi đã nhận được sự hỗ trợ, giúp đỡ cũng như là quan tâm, động viên tạo điều kiện từ chủ nhiệm trung đội và chi đoàn. Bài tham luận cũng được hoàn thành dựa trên sự khảo sát, tham khảo từ các nguồn tài liệu khác nhau như sách chuyên khảo, báo chuyên ngành của nhiều tác giả ở các trường Đại học, các tổ chức nghiên cứu, tổ chức chính trị có liên quan đến đề tài tham luận.

Tuy có nhiều cố gắng nhưng trong đề tài tham luận này không thể tránh khỏi những thiếu sót. Chúng tôi kính mong Quý thầy cô, cùng các chuyên gia và những người quan tâm đến đề tài này tiếp tục có những ý kiến đóng góp để giúp cho đề tài hoàn chỉnh hơn.

Một lần nữa chúng tôi xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO

1. Sách

Nguyễn, X. T (2020). *Tư tưởng, lý luận với đổi mới và phát triển đất nước*. Nxb Chính trị quốc gia Sự thật.

2. Tạp chí

Lâm, Đ. H - Nguyễn, X. H (2022). “*Thực trạng an toàn thông tin mạng hiện nay ở Việt Nam và giải pháp phòng chống vi phạm pháp luật trên không gian mạng*”, Tạp

⁷ GS, TS Nguyễn Xuân Thắng (2020): *Tư tưởng, lý luận với đổi mới và phát triển đất nước*, Nxb. Chính trị quốc gia Sự thật, H., tr.471-472, 472.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

chí Công Thương - Các kết quả nghiên cứu khoa học và ứng dụng công nghệ, Số 23.

Nguyễn, C. M (2021). “*Nhận biết và ngăn chặn hành vi đánh cắp dữ liệu*”, Chuyên Đề Công nghệ và ngân hàng số 1.

Mai, D. A (2023). “*Đảm bảo an ninh thông tin trong chuyển đổi số*”, tạp chí Tuyên giáo Trung ương.

3. Tài liệu tham khảo khác

<https://vtv.vn/xa-hoi/nhan-dien-thu-doan-danh-cap-thong-tin-ca-nhan-20220402165440152.htm>, Tham khảo ngày 26/8/2023

<https://antoanthongtin.vn/hacker-malware/ro-ri-du-lieu-ho-so-cua-300000-sinh-vien-viet-nam-107437>, Tham khảo ngày 26/8/2023

<https://special.nhandan.vn/bao-ve-du-lieu-ca-nhan-trong-moi-truong-so/index.html>, Tham khảo ngày 26/8/2023

**NHẬN THỨC VÀ THÁI ĐỘ CỦA SINH VIÊN CÁC
TRƯỜNG ĐẠI HỌC CÔNG AN NHÂN DÂN PHÍA NAM VỀ
BẢO VỆ CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG
AWARENESS AND ATTITUDE OF SOUTHERN
PEOPLE'S PUBLIC SECURITY UNIVERSITIES STUDENTS
ABOUT PROTECTING NATIONAL SOVEREIGNTY IN
CYBERSPACE**

ThS. Dương Văn Quế, Bùi Thị Thanh Quyên

Trường Đại học An ninh nhân dân

*Tác giả liên hệ: duongvanque2087@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Bảo vệ chủ quyền quốc gia, không gian mạng, nhận thức, thái độ, sinh viên các Trường Đại học Công an nhân dân phía Nam	Bài viết làm rõ cơ sở lý luận và thực trạng nhận thức, thái độ của sinh viên các Trường Đại học Công an nhân dân phía Nam về bảo vệ chủ quyền quốc gia trên không gian mạng. Kết quả khảo sát trên 400 sinh viên cho thấy: Nhận thức của sinh viên về bảo vệ chủ quyền quốc gia trên không gian mạng ở mức khá tốt nhưng mặt thái độ chỉ ở mức trung bình. Ngoài ra, sinh viên chưa tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên không gian mạng. Vì vậy, để nâng cao nhận thức và thái độ đúng đắn cho sinh viên các Trường Đại học Công an nhân dân phía Nam về bảo vệ chủ quyền quốc gia trên không gian mạng cần có những biện pháp tác động tích cực và đồng bộ từ phía Nhà trường, các đơn vị chức năng và sinh viên.
<i>Keywords:</i> Protecting national sovereignty, cyberspace, awareness, attitudes, Southern People's Public Security Universities students	ABSTRACT The research article clarifies the basis for discussion and implementation of awareness and attitudes of Southern People's Public Security Universities students regarding protecting national sovereignty in cyberspace. Survey results of over 400 students show that: Students' awareness of protecting national sovereignty in cyberspace is quite good, but their attitudes are only on an

average level. In addition, students have not actively participated in activities to protect national sovereignty in cyberspace. Therefore, to raise awareness and the right attitude for students of Southern People's Public Security Universities about protecting national sovereignty in cyberspace, it is necessary to have positive and synchronous impact measures from the University, functional units and students.

1. Giới thiệu

Hiện nay, với sự phát triển mạnh mẽ của khoa học kỹ thuật và công nghệ, đặc biệt là cuộc cách mạng công nghiệp lần thứ tư đã tạo ra một không gian chiến lược mới - “Không gian mạng” (KGM) và có tác động mạnh mẽ và sâu sắc trên mọi phương diện của đời sống kinh tế, xã hội. Đồng thời, KGM cũng là môi trường mà các thế lực thù địch (TLTD) triệt để lợi dụng để chống phá Đảng và Nhà nước ta. Tình hình mất an toàn thông tin, an ninh trên KGM diễn biến rất phức tạp, xuất hiện ngày càng nhiều cuộc tấn công mạng với quy mô lớn với tính chất rất nghiêm trọng, mức độ nguy hiểm cao đe dọa trực tiếp đến An ninh quốc gia (ANQG) và trật tự, an toàn xã hội. Theo đó, vấn đề bảo đảm an ninh mạng và bảo vệ chủ quyền quốc gia trên KGM có ý nghĩa đặc biệt quan trọng trong giai đoạn hiện nay. Để bảo vệ tốt chủ quyền quốc gia trên KGM cần phải tăng cường giáo dục, phổ biến pháp luật nhằm nâng cao nhận thức và thái độ cho người dân nhất là học sinh, sinh viên về vấn đề này. Sinh viên các Trường Công an nhân dân (CAND) phía Nam là những cán bộ công an tương lai, có vai trò quan trọng trong công tác bảo vệ an ninh, trật tự nói chung và chủ quyền quốc gia trên KGM nói riêng. Bên cạnh những sinh viên có nhận thức tốt, thái độ tích cực với hoạt động bảo vệ chủ quyền quốc gia trên KGM, vẫn còn một bộ phận sinh viên nhận thức chưa đúng đắn, thiếu tích cực trong hoạt động này. Chính vì vậy, việc làm rõ thực trạng nhận thức và thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên không gian mạng, trên cơ sở đó đưa ra một số đề xuất góp phần nâng cao nhận thức, thái độ tích cực cho sinh viên là rất cần thiết. Bên cạnh đó, hiện nay, có một số công trình nghiên cứu về vấn đề chủ quyền quốc gia trên KGM nhưng chưa có công trình nào nghiên cứu nhận thức và thái độ của sinh viên về bảo vệ chủ quyền quốc gia trên KGM. Trong phạm vi bài viết, tác giả nghiên cứu làm rõ một số khái niệm công cụ như: chủ quyền quốc gia trên KGM, bảo vệ chủ quyền quốc gia trên KGM và nhận thức, thái độ của sinh viên về bảo vệ chủ quyền quốc gia trên không gian mạng; làm rõ thực trạng nhận thức và thái độ của sinh viên hệ chính quy các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM và đưa ra một số đề xuất.

2. Cơ sở lý thuyết

Trên cơ sở nghiên cứu, tổng hợp tài liệu, tác giả làm rõ một số khái niệm công cụ như sau:

- Chủ quyền quốc gia trên KGM

Theo Điều 2, Luật An ninh mạng khẳng định: “KGM là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian” (Quốc hội, 2018). Theo đó, KGM có bản chất vật lý và bản chất xã hội.

“KGM quốc gia là KGM do Chính phủ xác lập, quản lý và kiểm soát” (Quốc hội, 2018). Bên cạnh không gian truyền thống như vùng đất, vùng trời, vùng biển và không gian vũ trụ, KGM trở thành không gian thứ năm, miền thứ năm của các quốc gia. Chính vì vậy, việc xác lập chủ quyền trên KGM là nhu cầu tất yếu của các quốc gia để bảo vệ lợi ích quốc gia, dân tộc.

Chủ quyền quốc gia trên KGM là quyền làm chủ một cách độc lập, toàn vẹn và đầy đủ về lập pháp, hành pháp và tư pháp của một quốc gia trong phạm vi lãnh thổ mạng của quốc gia đó, phù hợp với luật pháp quốc tế và bản chất của KGM (Tô Lâm, 2021). Theo đó, chủ quyền quốc gia trên KGM bao gồm một số nội dung sau: Chủ quyền lãnh thổ mạng; Quyền kiểm soát hoạt động mạng trên lãnh thổ mạng quốc gia; Quyền tài phán trên KGM; Quyền pháp lý theo quốc kỳ và hồ sơ đăng ký tại quốc gia; Quyền miễn trừ quốc gia (Tô Lâm, 2021).

Cũng giống như chủ quyền lãnh thổ, chủ quyền quốc gia trên KGM là quyền tối cao, tuyệt đối, hoàn toàn và riêng biệt của quốc gia đối với phạm vi KGM và các vùng thông tin do Nhà nước quản lý, kiểm soát bằng chính sách, pháp luật và năng lực công nghệ phù hợp với luật quốc tế.

- Bảo vệ chủ quyền quốc gia trên KGM

Chủ quyền quốc gia là quyền thiêng liêng, bất khả xâm phạm của một quốc gia dân tộc. Việt Nam là một nước độc lập, có chủ quyền, thống nhất và toàn vẹn lãnh thổ, bao gồm đất liền, hải đảo, vùng biển và vùng trời. Do vậy, yêu cầu bảo vệ chủ quyền quốc gia là yếu tố sống còn của dân tộc. Trong thời đại của cuộc cách mạng công nghiệp lần thứ tư đã tạo ra một không gian mới có chủ quyền đó là KGM. Do đó, bảo vệ chủ quyền quốc gia trên KGM cũng là một bộ phận của bảo vệ chủ quyền quốc gia. Ngoài ra, Nghị quyết số 51-NQ/TW, ngày 5/9/2019 của Bộ Chính trị về Chiến lược bảo vệ an ninh quốc gia xác định, cũng đặt ra yêu cầu cần phải “Tăng cường bảo vệ an toàn, an ninh mạng các hệ thống thông tin quan trọng quốc gia và các hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, phát hiện và đấu tranh ngăn chặn các hoạt động xâm phạm ANQG trên KGM, khắc phục điểm yếu, lỗ hổng bảo mật, nguy cơ mất an toàn, an ninh mạng, an ninh thông

tin” (Ban Chấp hành trung ương Đảng Cộng sản Việt Nam, 2019). Điều đó cho thấy, quan điểm chỉ đạo của Đảng và Nhà nước ta về bảo vệ chủ quyền quốc gia trên KGM.

Bên cạnh đó, Theo Điều 6, Luật An ninh mạng quy định về bảo vệ KGM quốc gia: “Nhà nước áp dụng các biện pháp để bảo vệ KGM quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân trên KGM” (Quốc hội, 2018).

Theo đó, bảo vệ chủ quyền quốc gia trên KGM là hoạt động phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại âm mưu và hoạt động xâm phạm chủ quyền quốc gia, ANQG trên KGM, đảm bảo an toàn, an ninh mạng, an ninh thông tin.

Bảo vệ chủ quyền quốc gia trên KGM đó là cuộc đấu tranh toàn diện trên tất cả các lĩnh vực, trong đó có bảo vệ chủ quyền biên giới mạng, bảo vệ an ninh quốc gia, trật tự, an toàn xã hội trên KGM, việc chấp hành pháp luật, lựa chọn và duy trì thể chế chính trị, văn hóa, quyền tự quyết, tự do, độc lập, thống nhất, toàn vẹn của quốc gia trên KGM...

Bảo vệ chủ quyền quốc gia trên KGM là trách nhiệm của toàn Đảng, toàn dân, toàn quân ta, trong đó lực lượng chuyên trách bảo vệ an ninh mạng của Bộ Quốc phòng, Bộ Công an làm nòng cốt. Do đó, để triển khai công tác này, phải phát huy sức mạnh dân tộc kết hợp với sức mạnh thời đại; đồng thời, xác định đây là cuộc đấu tranh của toàn dân, dưới sự lãnh đạo của Đảng, là nhiệm vụ trọng yếu của cuộc đấu tranh bảo vệ ANQG, giữ gìn trật tự, an toàn xã hội, là trách nhiệm của cả hệ thống chính trị, trong đó, lực lượng công an giữ vai trò nòng cốt, lực lượng an ninh mạng và cảnh sát phòng, chống tội phạm công nghệ cao có trách nhiệm trực tiếp thực hiện nhiệm vụ bảo vệ chủ quyền, lợi ích quốc gia trên KGM. Ngoài ra, lực lượng chuyên trách bảo vệ An ninh mạng của Bộ Quốc phòng, lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về ANQG cũng có nhiệm vụ bảo vệ an ninh mạng (Quốc hội, 2018).

- Nhận thức của sinh viên các trường CAND phía Nam về bảo vệ chủ quyền quốc gia trên không gian mạng

Nhận thức của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM là quá trình tâm lý phản ánh hiểu biết của sinh viên về vấn đề bảo vệ chủ quyền quốc gia trên KGM và được biểu hiện cụ thể ở những tiêu chí sau:

- + Nhận thức về nội dung chủ quyền quốc gia trên KGM;
- + Nhận thức về mức độ cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM;
- + Nhận thức về tầm quan trọng của hoạt động bảo vệ chủ quyền quốc gia trên KGM;
- + Nhận thức về chủ thể bảo vệ chủ quyền quốc gia trên KGM;
- + Nhận thức về trách nhiệm của bản thân trong bảo vệ chủ quyền quốc gia trên KGM;
- + Nhận thức về nguy cơ đe dọa đến An ninh quốc gia trên KGM hiện nay;
- + Nhận thức về âm mưu, phương thức, thủ đoạn hoạt động của các TLTD trên KGM;

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Thái độ của sinh viên các Trường Đại học Công an nhân dân phía Nam về bảo vệ chủ quyền quốc gia trên không gian mạng

Thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM là trạng thái tâm lý tích cực hay tiêu cực của sinh viên về bảo vệ chủ quyền quốc gia trên KGM thể hiện thông qua hành vi của sinh viên đối với hoạt động trên. Thái độ của sinh viên về bảo vệ chủ quyền quốc gia trên KGM được nghiên cứu trên các tiêu chí sau:

+ Mức độ đồng tình, ủng hộ đối với những hành vi tích cực trong bảo vệ chủ quyền quốc gia trên KGM;

+ Mức độ lên án, phê phán đối với những hành vi tiêu cực trong bảo vệ chủ quyền quốc gia trên KGM;

+ Mức độ tích cực tuyên truyền, vận động người khác tham gia hoạt động bảo vệ chủ quyền quốc gia trên KGM;

+ Mức độ chủ động trong nghiên cứu, tìm hiểu về âm mưu, phương thức, thủ đoạn hoạt động của các TLTĐ lợi dụng KGM để xâm phạm ANQG, an ninh mạng;

+ Mức độ hứng thú khi tham gia các tập huấn các kỹ năng và đấu tranh phản bác các quan điểm sai trái, thù địch trên KGM;

+ Mức độ sẵn sàng tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM;

+ Mức độ tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM;

Nhận thức và thái độ có mối quan hệ biện chứng với nhau. Nhận thức đúng đắn sẽ giúp cho sinh viên có thái độ tích cực khi tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM và ngược lại. Bên cạnh đó, thái độ đúng đắn, tích cực sẽ giúp cho nhận thức thêm sâu sắc.

3. Phương pháp nghiên cứu

Để nghiên cứu, làm rõ thực trạng nhận thức và thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM, tác giả sử dụng một số phương pháp cơ bản sau:

- Phương pháp nghiên cứu tài liệu: Tác giả tiến hành nghiên cứu tài liệu từ sách, tạp chí, các công trình nghiên cứu... có liên quan về chủ quyền quốc gia, bảo vệ chủ quyền quốc gia trên KGM. Thông qua đó, hệ thống hóa tài liệu, xác định và xây dựng cơ sở lý luận, làm rõ các khái niệm công cụ về nhận thức và thái độ của SV về bảo vệ chủ quyền quốc gia trên KGM.

- Phương pháp điều tra bằng bảng hỏi: Đây là phương pháp quan trọng nhất được tác giả sử dụng để khảo sát về nhận thức và thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM, cụ thể:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

+ Xây dựng bảng hỏi: Căn cứ vào lý luận cơ bản, các khái niệm công cụ, tiêu chí và lĩnh vực đánh giá để thiết kế bảng hỏi. Đồng thời tiến hành khảo sát thử và chỉnh sửa, hoàn chỉnh bảng hỏi.

+ Chọn mẫu:

Xác định cỡ mẫu: Cỡ mẫu được tính theo công thức sau:

$$n = \frac{N}{1 + N \cdot (e)^2}$$

Trong đó:

n: Cỡ mẫu

N: Dân số

e: sai số tiêu chuẩn (+/-5%)

Các Trường Đại học Công an nhân dân phía Nam bao gồm: Trường Đại học An ninh nhân dân và Trường Đại học Cảnh sát nhân dân là với khoảng 8000 sinh viên. Theo đó, số lượng mẫu khảo sát là 381 sinh viên.

+ Phương pháp chọn mẫu: chọn mẫu ngẫu nhiên, mang tính đại diện.

+ Tiến hành điều tra chính thức: Tác giả sử dụng ứng dụng Google Form để khảo sát trên 400 sinh viên (200 sinh viên Trường Đại học An ninh nhân dân và 200 sinh viên Trường Đại học Cảnh sát nhân dân).

- *Phương pháp phỏng vấn*: Tác giả tiến hành phỏng vấn 04 sinh viên hệ chính quy để tìm hiểu sâu hơn một số nội dung nhận thức, thái độ của sinh viên về bảo vệ chủ quyền quốc gia trên KGM.

- *Phương pháp thống kê toán học*

Tác giả sử dụng phần mềm SPSS 24.0 để xử lý số liệu bằng cách tính tỉ lệ phần trăm (%), tính điểm trung bình. Những câu hỏi khảo sát mức độ sẽ được tính điểm từ 1 điểm tới 5 điểm tương ứng với các mức từ 1 đến 5 trong đó: mức 1 là mức tiêu cực nhất và mức 5 là mức tích cực nhất. Theo đó, tác giả chia thành năm mức độ như sau:

Từ 1.00 điểm đến 1.80 điểm là mức rất yếu (Mức 1);

Từ 1.81 điểm đến 2.60 điểm là mức yếu (Mức 2);

Từ 2.61 điểm đến 3.40 điểm là mức trung bình (Mức 3);

Từ 3.41 điểm đến 4.20 điểm là mức khá tốt (Mức 4);

Từ 4.21 điểm đến 5.00 điểm là mức rất tốt (Mức 5).

4. Kết quả nghiên cứu, thảo luận

4.1. Nhận thức của sinh viên về bảo vệ chủ quyền quốc gia trên KGM

Để làm rõ nhận thức của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM, tác giả tiến hành khảo trên trên 07 phương diện và thu được kết quả như sau:

Một là, nhận thức về nội dung chủ quyền quốc gia trên KGM

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Khảo sát nhận thức của sinh viên về nội dung chủ quyền quốc gia trên KGM, tác giả thu được kết quả ở Bảng 1, cụ thể: Nhận thức của sinh viên về nội dung chủ quyền quốc gia trên KGM ở mức trung bình với ĐTB chung là 3.16, trong đó có 02 nội dung nhận thức ở mức khá tốt (Quyền kiểm soát hoạt động mạng trên lãnh thổ mạng quốc gia với ĐTB là 4.0; Chủ quyền lãnh thổ mạng với ĐTB là 3.80), 02 nội dung nhận thức ở mức trung bình (Quyền tài phán đối với lãnh thổ mạng; Quyền pháp lý theo quốc kỳ và hồ sơ đăng ký tại quốc gia với điểm trung bình lần lượt là 2.80 và 2.62) và 01 nội dung nhận thức ở mức yếu nhưng tiệm cận mức trung bình (Quyền miễn trừ quốc gia với ĐTB là 2.58). Điều đó cho thấy, một số biểu hiện nhận thức của sinh viên các Trường Đại học CAND phía Nam về chủ quyền quốc gia trên KGM còn hạn chế (xem Bảng 1).

Bảng 1

Nhận thức của sinh viên về nội dung chủ quyền quốc gia trên KGM

TT	Nội dung	Điểm trung bình	Thứ bậc
1	Chủ quyền lãnh thổ mạng	3.80	2
2	Quyền kiểm soát hoạt động mạng trên lãnh thổ mạng quốc gia	4.0	1
3	Quyền tài phán đối với lãnh thổ mạng	2.80	3
4	Quyền pháp lý theo quốc kỳ và hồ sơ đăng ký tại quốc gia	2.62	4
5	Quyền miễn trừ quốc gia	2.58	5
ĐTB chung		3.16	

Hai là, nhận thức về sự cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM

Khảo sát nhận thức của sinh viên về sự cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM, tác giả thu được kết quả ở Bảng 2 như sau: Nhận thức của sinh viên về sự cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM ở mức rất tốt với ĐTB là 4.58, trong đó: có 92% sinh viên lựa chọn ở mức “*Khá cần thiết*” và “*Rất cần thiết*”, 8% lựa chọn mức bình thường. Điều này cho thấy, đa số sinh viên có nhận thức đúng đắn và đánh giá cao mức độ cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM.

Bảng 2

Nhận thức về sự cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM

TT	Mức độ	Tỷ lệ %	ĐTB
1	Không cần thiết	0%	4.58
2	Ít cần thiết	0 %	
3	Bình thường	8%	
4	Khá cần thiết	26%	

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

5 Rất cần thiết 66%

Ba là, nhận thức về tầm quan trọng của việc bảo vệ chủ quyền quốc gia trên KGM

Nhận thức của sinh viên về tầm quan trọng của việc bảo vệ chủ quyền quốc gia trên KGM ở mức rất tốt với ĐTB là 4.27. Đa số sinh viên đánh giá cao tầm quan trọng của việc bảo vệ chủ quyền quốc gia trên KGM, cụ thể có 81.5% sinh viên lựa chọn ở mức “*Rất quan trọng*” và “*khá quan trọng*” trở lên. Tuy nhiên, vẫn còn 5% sinh viên lựa chọn việc bảo vệ chủ quyền quốc gia trên KGM là “*Ít quan trọng*” (xem Bảng 3). Điều này cho thấy, vẫn còn một bộ phận sinh viên nhận thức chưa đúng đắn về vấn đề này.

Bảng 3

Nhận thức về tầm quan trọng của việc bảo vệ chủ quyền quốc gia trên KGM

TT	Mức độ	Tỷ lệ %	ĐTB
1	Không quan trọng	0%	
2	Ít quan trọng	5%	
3	Bình thường	13.5%	4.27
4	Khá quan trọng	31.5 %	
5	Rất quan trọng	50%	

Ngoài ra kết quả phỏng vấn cho thấy, 04/04 sinh viên cho rằng hoạt động bảo vệ chủ quyền quốc gia trên KGM là rất cần thiết và có tầm quan trọng đặc biệt đối với quốc gia. Sinh viên N.T chia sẻ rằng: “Bảo vệ chủ quyền quốc gia trên KGM rất quan trọng vì chủ quyền trên KGM là một bộ phận quan trọng của chủ quyền quốc gia và bảo đảm chủ quyền quốc gia trên KGM chính là bảo vệ chủ quyền quốc gia, dân tộc”; Còn sinh viên L.N.N chia sẻ rằng: “Việc bảo vệ chủ quyền quốc gia trên KGM trong thời kỳ hội nhập, thời kỳ chuyển đổi số như hiện nay thật sự rất cần thiết khi mà các TLTĐ hoạt động với phương thức và thủ đoạn ngày càng tinh vi, xảo quyệt

Bốn là, nhận thức về chủ thể bảo vệ chủ quyền quốc gia trên KGM

Nhận thức của sinh viên về chủ thể bảo vệ chủ quyền quốc gia trên KGM ở mức trung bình với ĐTB là 3.31, trong đó chủ thể được sinh viên đồng ý cao nhất đó là “*Toàn Đảng, toàn quân và toàn dân trong đó lực lượng chuyên trách bảo vệ an ninh mạng của công an, quân đội làm nòng cốt*” với ĐTB là 3.98 ở mức khá tốt; tiếp đến là “*Lực lượng bảo vệ an ninh mạng trong các cơ quan nhà nước, tổ chức*” với ĐTB là 3.87; Hai chủ thể được sinh viên ít lựa chọn nhất đó là “*Lực lượng Công an nhân dân*” và “*Lực lượng quân đội nhân dân*” với ĐTB lần lượt là 2.87 và 2.71 (xem Bảng 4).

Bảng 4

Nhận thức về chủ thể bảo vệ chủ quyền quốc gia trên KGM

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

TT	Nhận thức	Điểm trung bình	Thứ bậc
1	Lực lượng Công an nhân dân	2.87	5
2	Lực lượng Quân đội nhân dân	2.71	4
3	Lực lượng bảo vệ an ninh mạng trong các cơ quan nhà nước, tổ chức	3.87	2
4	Các cơ quan, ban ngành	3.13	3
5	Toàn Đảng, toàn quân và toàn dân trong đó lực lượng chuyên trách bảo vệ an ninh mạng của công an, quân đội làm nòng cốt	3.98	1
ĐTB chung		3.31	

Đa số sinh viên các Trường Đại học CAND phía Nam đều có nhận thức đúng đắn về chủ thể bảo vệ chủ quyền quốc gia trên KGM và cho rằng đó là trách nhiệm của “*Toàn Đảng, toàn quân và toàn dân trong đó lực lượng chuyên trách bảo vệ an ninh mạng của công an, quân đội làm nòng cốt*” và đồng thời là trách nhiệm của “*Lực lượng bảo vệ an ninh mạng trong các cơ quan nhà nước, tổ chức*”. Tuy nhiên, vẫn còn một bộ phận sinh viên nhận thức chưa đầy đủ về chủ thể bảo vệ chủ quyền quốc gia trên KGM (một bộ phận sinh viên vẫn lựa chọn phương án “*Lực lượng Công an nhân dân*”, “*Lực lượng Quân đội nhân dân*” và “*Các cơ quan ban ngành*”).

Năm là, nhận thức về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM

Khảo sát nhận thức về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM, tác giả thu được kết quả ở Bảng 5, như sau: Nhận thức của sinh viên về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM ở mức trung bình với ĐTB là 3.17, trong đó có 35% sinh viên lựa chọn mức biết khá rõ và biết rất rõ, 40% lựa chọn mức bình thường, 25% lựa chọn mức biết ít và không biết. Điều đó cho thấy, một bộ phận sinh viên nhận thức hạn chế về trách nhiệm của bản thân đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Bảng 5

Nhận thức về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM

TT	Mức độ	Tỷ lệ %	ĐTB
1	Không biết	5%	3.17
2	Biết ít	20%	
3	Bình thường	40%	
4	Biết khá rõ	23%	

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

5 Biết rất rõ 12%

Bên cạnh, kết quả phỏng vấn cho thấy: 02/04 sinh viên có nhận thức chưa đầy đủ về trách nhiệm của bản thân đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM, cụ thể như sinh viên M.H chia sẻ: *“Mặc dù biết về Luật An ninh mạng nhưng em chưa nghiên cứu kỹ nên không biết rõ bản thân có trách nhiệm gì, và chưa nắm vững những hành vi bị nghiêm cấm”*.

Sáu là, nhận thức về nguy cơ đe dọa đến An ninh quốc gia trên KGM

Khảo sát nhận thức của sinh viên về nguy cơ đe dọa đến an ninh quốc gia trên KGM, tác giả thu được kết quả ở Bảng 6, cụ thể:

Bảng 6

Nhận thức về nguy cơ đe dọa đến An ninh quốc gia trên KGM

TT	Nguy cơ	Điểm trung bình	Thứ bậc
1	Chiến tranh mạng	3.06	6
2	Gián điệp mạng	3.66	4
3	Hoạt động tấn công mạng nhằm vào hệ thống thông tin Việt Nam	3.23	6
4	Tội phạm sử dụng mạng máy tính, công nghệ cao	3.75	2
5	Tình trạng mất an ninh, an toàn thông tin mạng	3.39	5
6	Thông qua KGM thực hiện âm mưu “diễn biến hòa bình”	4.30	1
7	Tuyên truyền các quan điểm sai trái, thù địch của các thế lực thù địch trên KGM nhằm chia rẽ khối đại đoàn kết dân tộc, suy giảm niềm tin của nhân dân	3.73	3
ĐTB chung		3.59	

Kết quả ở Bảng 6 cho thấy: Nhận thức của sinh viên về nguy cơ đe dọa đến an ninh quốc gia trên KGM ở mức khá tốt với ĐTB chung là 3.59. Trong 07 nguy cơ được đề xuất, nhận thức của sinh viên đối với 01 nguy cơ ở mức rất tốt (Thông qua KGM thực hiện âm mưu “diễn biến hòa bình” với ĐTB là 4.30) 03 nguy cơ ở mức khá tốt (Tội phạm sử dụng mạng máy tính, công nghệ cao với ĐTB là 3.75; Tuyên truyền các quan điểm sai trái, thù địch của các thế lực thù địch trên KGM nhằm chia rẽ khối đại đoàn kết dân tộc, suy giảm niềm tin của nhân dân với ĐTB là 3,73 và Gián điệp mạng với ĐTB là 3.66); 03 nguy cơ ở mức trung bình (Chiến tranh mạng, Hoạt động tấn công mạng nhằm vào hệ thống thông tin Việt Nam, tình trạng mất an ninh, an toàn thông tin mạng với ĐTB lần lượt là 3.06, 3.23, 3.39).

Bảy là, nhận thức về phương thức, thủ đoạn hoạt động của các thế lực thù địch trên KGM

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Khảo sát nhận thức của sinh viên về phương thức, thủ đoạn hoạt động của các thế lực thù địch trên KGM, thu được kết quả ở Bảng 7 như sau:

Bảng 7

Nhận thức về phương thức, thủ đoạn hoạt động của các TLTĐ trên KGM

TT	Mức độ	Tỷ lệ %	ĐTB
1	Không tinh vi, xảo quyệt	0%	4.26
2	Ít tinh vi, xảo quyệt	5%	
3	Bình thường	7.5%	
4	Khá tinh vi, xảo quyệt	44%	
5	Rất tinh vi, xảo quyệt	43,5%	

Kết quả khảo sát ở Bảng 7 cho thấy nhận thức của sinh viên các trường Đại học CAND phía Nam về âm mưu và phương thức thủ đoạn hoạt động của các TLTĐ ở mức rất tốt với ĐTB là 4.26, cụ thể 87,5 % sinh viên lựa chọn mức độ "*Khá tinh vi, xảo quyệt*" và "*Rất tinh vi xảo quyệt*". Tuy nhiên, vẫn còn một bộ phận sinh viên có nhận thức hạn chế về phương thức, thủ đoạn hoạt động của các thế lực thù địch trên KGM với 7,5 % sinh viên lựa chọn mức "*Bình thường*" và có 5% sinh viên lựa chọn mức ít "*Tinh vi, xảo quyệt*". Ngoài ra, kết quả phỏng vấn cũng thể hiện rõ vấn đề này: 04/04 sinh viên đều cho rằng các thế lực thù địch luôn tìm mọi cách để lợi dụng KGM xâm phạm ANQG và phương thức, thủ đoạn hoạt động của chúng rất tinh vi, nguy hiểm.

Tổng hợp kết quả khảo sát về nhận thức của sinh viên cho thấy: Nhận thức của sinh viên về bảo vệ chủ quyền quốc gia trên KGM ở mức khá tốt với ĐTB chung là 3.76. Trong 07 biểu hiện của nhận thức có 03 biểu hiện ở mức rất tốt; 01 biểu hiện ở mức khá tốt và 03 biểu hiện ở mức trung bình, cụ thể: Ở vị trí thứ nhất là nhận thức về sự cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM với ĐTB là 4.58; tiếp đến là nhận thức về tầm quan trọng hoạt động chủ quyền quốc gia trên KGM với ĐTB là 4.27. Ngược lại, 02 mức độ nhận thức hạn chế nhất đó là nhận thức về nội dung chủ quyền quốc gia trên KGM và nhận thức về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM với ĐTB lần lượt là 3.16 và 3.17 (xem Bảng 8). Do vậy, cần có những biện pháp tác động nhằm nâng cao nhận thức cho sinh viên về vấn đề này.

Bảng 8

Tổng hợp nhận thức của sinh viên về bảo vệ chủ quyền quốc gia trên KGM

TT	Biểu hiện mặt nhận thức	Điểm trung bình	Thứ bậc
1	Nhận thức về nội dung chủ quyền quốc gia trên KGM	3.16	7
2	Nhận thức về sự cần thiết của việc bảo vệ chủ quyền quốc gia trên KGM	4.58	1
3	Nhận thức về tầm quan trọng của việc bảo vệ chủ quyền quốc gia trên KGM	4.27	2
4	Nhận thức về chủ thể bảo vệ chủ quyền quốc gia trên KGM	3.31	5
5	Nhận thức về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM	3.17	6
6	Nhận thức về nguy cơ đe dọa An ninh quốc gia trên KGM	3.59	4
7	Nhận thức về phương thức, thủ đoạn hoạt động của các thế lực thù địch trên KGM	4.26	3
DTB chung		3.76	

4.2. Thái độ của sinh viên đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM

Tiến hành khảo sát thái độ của sinh viên đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM trên 07 phương diện, tác giả thu được kết quả ở Bảng 9 như sau:

Bảng 9

Thái độ của sinh viên về bảo vệ chủ quyền quốc gia trên KGM

TT	Biểu hiện mặt thái độ	Điểm trung bình	Thứ bậc
1	Mức độ lên án, phê phán đối với những hành vi tiêu cực trong bảo vệ chủ quyền quốc gia trên KGM	3.6	2
2	Mức độ đồng tình, ủng hộ đối với những hành vi tích cực trong bảo vệ chủ quyền quốc gia trên KGM	3.9	1
3	Mức độ tích cực tuyên truyền, vận động người khác tham gia hoạt động bảo vệ chủ quyền quốc gia trên KGM	3.33	3
4	Mức độ chủ động trong nghiên cứu, tìm hiểu về âm mưu, phương thức, thủ đoạn hoạt động của các TLTD lợi dụng KGM xâm phạm ANQG	3.16	7

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

5	Mức độ hứng thú khi tham gia các tập huấn các kỹ năng bảo mật thông tin, bảo đảm an toàn thông tin mạng và đấu tranh phản bác các quan điểm sai trái, thù địch trên KGM	3.28	5
6	Mức độ sẵn sàng tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM	3.32	4
7	Mức độ tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM	3.23	6
ĐTB chung		3.40	

Kết quả ở Bảng 9 cho thấy: Thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM ở mức trung bình nhưng tiệm cận mức khá tốt với ĐTB chung là 3.40, cụ thể có 02 biểu hiện ở mức khá tốt, 05 biểu hiện ở mức trung bình. Trong đó, mức độ đồng tình, ủng hộ đối với những hành vi tích cực trong bảo vệ chủ quyền quốc gia trên KGM là tốt nhất với ĐTB là 3.90; Ở vị trí thứ 2 là mức độ lên án, phê phán đối với những hành vi tiêu cực trong bảo vệ chủ quyền quốc gia trên KGM với ĐTB là 3.60; Ở vị trí thứ 3 đó là mức độ tích cực tuyên truyền, vận động người khác tham gia hoạt động bảo vệ chủ quyền quốc gia trên KGM (ĐTB là 3.33). Ngược lại, 03 biểu hiện của mặt thái độ hạn chế nhất đó là: Mức độ chủ động trong nghiên cứu, tìm hiểu về âm mưu, phương thức, thủ đoạn hoạt động của các TLTĐ lợi dụng KGM xâm phạm ANQG; Mức độ tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM và mức độ sẵn sàng tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM với ĐTB lần lượt là 3.16, 3.23 và 3.28. Điều đó cho thấy, mặc dù sinh viên có thái độ đúng đắn với những hành vi tích cực và hành vi tiêu cực trong hoạt động bảo vệ chủ quyền quốc gia trên KGM nhưng sinh viên chưa thật sự chủ động trong nghiên cứu, tìm hiểu về âm mưu, phương thức, thủ đoạn hoạt động của các TLTĐ lợi dụng KGM để xâm phạm ANQG; chưa sẵn sàng và tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM. Ngoài ra, kết quả phỏng vấn cho thấy: 03/04 sinh viên cho rằng: mặc dù lên án phê phán những hành vi tiêu cực và ủng hộ những hành vi tích cực nhưng do kiến thức và kinh nghiệm của bản thân còn hạn chế cho nên chưa sẵn sàng và tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Bên cạnh đó, để tìm hiểu sâu hơn về mức độ tích cực của sinh viên khi tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM, tác giả tiến hành khảo sát ở 10 hoạt động, thu được kết quả ở Bảng 10 như sau:

Bảng 10

Mức độ tích cực của sinh viên khi tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

TT	Hoạt động	Điểm trung bình	Thứ bậc
1	Bảo vệ nền tảng tư tưởng của Đảng và đấu tranh phản bác các quan điểm sai trái, thù địch trên KGM	2.40	9
2	Thực hiện đúng quy định của Luật An ninh mạng khi sử dụng Internet và mạng xã hội	3.80	2
3	Bảo vệ bí mật nhà nước, bảo mật thông tin khi sử dụng Internet và mạng xã hội	4.10	1
4	Tham gia các hội, nhóm, fanpage về bảo vệ chủ quyền quốc gia trên KGM	3.40	4
5	Tuyên truyền, vận động người thân, bạn bè tuân thủ quy định của pháp luật khi sử dụng Internet và mạng xã hội	3.15	8
6	Tích cực tìm hiểu về Luật An ninh mạng, về bảo vệ chủ quyền quốc gia trên KGM	3.42	3
7	Tương tác, chia sẻ với các bài viết về bảo vệ chủ quyền quốc gia trên KGM, các bài viết đấu tranh phản bác các quan điểm sai trái, thù địch	3.30	5
8	Tham gia các buổi tập huấn về kỹ năng bảo mật thông tin và sử dụng mạng xã hội an toàn	3.29	6
9	Theo dõi các websites, fanpage của các đối tượng phản động, để tìm hiểu về âm mưu và phương thức thủ đoạn lợi dụng KGM xâm phạm ANQG của các thế lực thù địch	3.18	7
10	Tham gia các cuộc vận động, các cuộc thi tìm hiểu về bảo vệ chủ quyền quốc gia trên KGM	2.30	10
ĐTB chung		3.23	

Kết quả khảo sát ở Bảng 10 cho thấy: Mức độ tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM của sinh viên chỉ ở mức trung bình, trong 10 hoạt động được đề xuất có 03 hoạt động mức độ tích cực của sinh viên ở mức khá tốt, 05 hoạt động ở mức trung bình và 02 hoạt động ở mức yếu. Trong đó, 03 hoạt động sinh viên tích cực thực hiện nhất đó là: Bảo vệ bí mật nhà nước, bảo mật thông tin khi sử dụng Internet và mạng xã hội với ĐTB là 4.10; Thực hiện đúng quy định của Luật An ninh mạng khi sử dụng Internet và mạng xã hội với ĐTB là 3.80 và Tích cực tìm hiểu về Luật An ninh mạng, về bảo vệ chủ quyền quốc gia trên KGM với ĐTB 3.42. Ngược lại, 03 hoạt động sinh viên ít tích cực thực hiện nhất là: Tham gia các cuộc vận động, các cuộc thi tìm hiểu về bảo vệ chủ quyền quốc gia trên KGM (ĐTB 2.30); Bảo vệ nền

tăng tư tưởng của Đảng và đấu tranh phản bác các quan điểm sai trái, thù địch trên KGM (ĐTB 2.40) và Tuyên truyền, vận động người thân, bạn bè tuân thủ quy định của pháp luật khi sử dụng Internet và mạng xã hội (ĐTB 3.15). Kết quả phỏng vấn cho thấy: 04/04 sinh viên đều cho rằng do kiến thức và kỹ năng hạn chế cho nên bản thân chưa tích cực và tự giác tham gia các hoạt động như: viết bài bảo vệ nền tảng tư tưởng của Đảng và đấu tranh phản bác các quan điểm sai trái, thù địch trên KGM; Tham gia các cuộc thi tìm hiểu kiến thức về bảo vệ chủ quyền quốc gia trên KGM.

5. Kết luận và đề xuất

5.1. Kết luận: Tóm lại, mặc dù nhận thức của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM ở mức khá tốt với ĐTB là 3.76 tuy nhiên thái độ của sinh viên với hoạt động bảo vệ chủ quyền quốc gia trên KGM chỉ ở mức trung bình nhưng gần tiệm cận mức khá tốt với ĐTB là 3.40. Ngoài ra, có 03 biểu hiện mặt nhận thức và 05 biểu hiện mặt thái độ của sinh viên về bảo vệ chủ quyền quốc gia trên KGM ở mức trung bình. Đặc biệt, sinh viên chưa tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM (có 05 hoạt động mức độ tích cực thực hiện của sinh viên chủ ở mức trung bình và 02 hoạt động ở mức yếu). Điều này cho thấy, một bộ phận sinh viên vẫn còn nhận thức hạn chế và chưa có thái độ đúng đắn đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM. Vì thế, cần có những biện pháp tác động trên cả hai phương diện này nhằm nâng cao nhận thức và thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM.

5.2. Đề xuất: Trên cơ sở nghiên cứu thực trạng nhận thức và thái độ của sinh viên các Trường Đại học CAND phía Nam về bảo vệ chủ quyền quốc gia trên KGM, để nâng cao nhận thức và thái độ tích cực của sinh viên về vấn đề này, tác giả đưa ra một số đề xuất sau:

- Về phía các Trường Đại học CAND phía Nam và các đơn vị chức năng trong Nhà trường

Thứ nhất, tăng cường hơn nữa công tác tuyên truyền nhằm nâng cao nhận thức của sinh viên về bảo vệ chủ quyền quốc gia trên KGM nhất là các nội dung về chủ quyền quốc gia trên KGM về trách nhiệm của bản thân trong hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Thứ hai, lồng ghép nội dung giáo dục về chủ quyền quốc gia và bảo vệ chủ quyền quốc gia trên KGM vào trong chương trình giảng dạy góp phần nâng cao nhận thức và thái độ tích cực cho sinh viên về vấn đề này.

Thứ ba, tổ chức các buổi tọa đàm, tập huấn nhằm trang bị kiến thức và kỹ năng cần thiết cho sinh viên như: Kỹ năng sử dụng mạng xã hội an toàn, kỹ năng bảo mật thông tin, kỹ năng nhận diện, đấu tranh, phản bác các quan điểm sai trái, thù địch trên KGM...

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thứ tư, tổ chức các cuộc thi, hoạt động nhằm vận động, phong trào lôi cuốn sinh viên tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM. Đồng thời, đổi mới nội dung, hình thức sinh hoạt ngoại khóa, hoạt động của các câu lạc bộ nhằm thu hút sinh viên tham gia, khuyến khích sinh viên tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Thứ năm, mời báo cáo viên báo cáo chuyên đề, cập nhật kiến thức thực tế cho sinh viên về chủ quyền quốc gia trên KGM, kỹ năng bảo mật thông tin, tình hình an ninh mạng, an ninh thông tin.

Thứ sáu, xây dựng các kênh truyền thông như: Câu lạc bộ, hội nhóm, fanpage trên mạng xã hội, fanpage để tuyên truyền về âm mưu, phương thức thủ đoạn hoạt động lợi dụng KGM chống Đảng và Nhà nước ta của các thế lực thù địch, hướng dẫn cách thức phòng tránh cho sinh viên.

- Về phía sinh viên

Một là, sinh viên cần tích cực nghiên cứu tìm hiểu, nâng cao nhận thức của bản thân về Luật An ninh mạng, các hoạt động bảo vệ chủ quyền quốc gia trên KGM, ý thức trách nhiệm của bản thân trong bảo vệ chủ quyền quốc gia trên KGM. Khi sinh viên có nhận thức đúng đắn và đầy đủ sẽ có thái độ và hành động tích cực.

Hai là, nhận thức rõ và nêu cao tinh thần trách nhiệm của bản thân đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM; đề cao cảnh giác trước các âm mưu, phương thức hoạt động của các thế lực thù địch; ý thức bảo mật thông tin, bảo vệ bí mật Nhà nước khi tham gia các hoạt động trên KGM nhất là mạng xã hội.

Ba là, tuyên truyền, vận động người thân, bạn bè... tìm hiểu về Luật An ninh mạng, tuân thủ quy định của pháp luật khi sử dụng Internet và mạng xã hội và trách nhiệm của cá nhân đối với hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Bốn là, tích cực tham gia các câu lạc bộ, các buổi tập huấn, báo cáo chuyên đề do Nhà trường, các đơn vị chức năng tổ chức nhằm cải thiện kiến thức, kỹ năng về vấn đề bảo mật thông tin, kỹ sử dụng mạng xã hội an toàn, kỹ năng đấu tranh phản bác các quan điểm sai trái, thù địch... Qua đó, cập nhật kiến thức, cải thiện kỹ năng để sinh viên có thể tự tin và tích cực tham gia các hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Năm là, tham gia các hội, nhóm, fanpage tích cực trên mạng xã hội để tìm hiểu về âm mưu, hoạt động của các thế lực thù địch, được hướng dẫn cách thức phòng ngừa, học hỏi kinh nghiệm, thực hành các hoạt động bảo vệ chủ quyền quốc gia trên KGM.

Bảo vệ chủ quyền quốc gia trên không gian mạng là nội dung mới, cần phải tăng cường giáo dục, phổ biến pháp luật nhằm nâng cao nhận thức và thái độ và về bảo vệ chủ quyền quốc gia trên không gian mạng cho sinh viên các Trường Đại học CAND phía Nam nói riêng – những cán bộ công an tương lai, góp phần đảm bảo an ninh mạng, an ninh quốc gia và trật tự an toàn xã hội.

LỜI CẢM ƠN

Tác giả xin gửi lời cảm ơn chân thành và sâu sắc đến sự hỗ trợ nhiệt tình của sinh viên Trường Đại học An ninh nhân dân và Trường Đại học Cảnh sát nhân dân đã giúp tác giả hoàn thành phiếu khảo sát và phỏng vấn phục vụ bài tham luận. Đồng thời, xin gửi lời cảm ơn đến lãnh đạo Khoa Tâm lý – Trường Đại học An ninh nhân dân đã tạo điều kiện cho tác giả hoàn thành tham luận một cách thuận lợi.

TÀI LIỆU THAM KHẢO

1. Ban chấp hành trung ương Đảng Cộng sản Việt Nam. (2019). ***Nghị quyết của Bộ Chính trị về Chiến lược bảo vệ An ninh quốc gia***. Hà Nội.
2. Bộ Công an. (2022), ***Bình luận khoa học sách “Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia***. Tập 1. Thành phố Hồ Chí Minh.
3. Quốc hội. (2018). ***Luật an ninh mạng***. Hà Nội.
4. Tô, L. (2021), ***Chủ quyền không gian mạng: Yêu cầu thời đại và nghĩa vụ quốc gia***. Hà Nội: Công an nhân dân.

NHẬN THỨC VỀ MỐI ĐE DỌA AN NINH MẠNG VÀ CÁCH BẢO VỆ THANH THIẾU NIÊN

Nguyễn Thị Mỹ Hạnh

Đại học Kinh tế TP. Hồ Chí Minh

Email: hanhnguyen.31211027446@st.ueh.edu.vn

Phone number: 0943972527

THÔNG TIN	TÓM TẮT
Từ khóa: An ninh mạng; tội phạm mạng; mối đe dọa, thông tin, bảo mật	Nghiên cứu này nhằm tìm hiểu nhận thức về mối đe dọa an ninh mạng và hiểu biết về các biện pháp phòng ngừa nhằm bảo vệ giới trẻ khỏi các rủi ro trực tuyến. Để làm được điều này, một phương pháp định lượng đã được áp dụng và bảng câu hỏi khảo sát được thiết lập để thu thập dữ liệu ngẫu nhiên từ những thanh niên đang học từ lớp 11 trở lên. Tổng cộng có 264 thanh niên, 147 nữ và 117 nam đã trả lời bảng khảo sát này. Dữ liệu được tổ chức và phân tích bằng gói công cụ phân tích dữ liệu Excel, được diễn giải và biểu diễn dưới dạng biểu đồ kèm theo một số giải thích. Nhận thức về mối đe dọa bảo mật trực tuyến được đánh giá là tốt với 20% hoàn toàn nhận thức được nó. Kiến thức về xác thực hai yếu tố được cho là khá thấp. Việc sử dụng mã hóa đám mây, bảo vệ và bảo mật bằng tường lửa chưa quá quen thuộc với giới trẻ. Tuy nhiên, việc sử dụng mật khẩu mạnh cho các tài khoản và nền tảng khác hầu hết được giới trẻ áp dụng. Thanh niên cũng được cho là có mối quan tâm đến phần mềm và hệ thống trên điện thoại di động cũng như các thiết bị khác của họ khi họ trả lời rằng họ cập nhật phần mềm thường xuyên.

1. Giới thiệu

Mối đe dọa an ninh mạng đã trở thành vấn đề cấp bách và nổi cộm trên toàn cầu. Với sự phát triển nhanh chóng trong việc sử dụng công nghệ thông tin, mối đe dọa an ninh mạng ngày càng gia tăng. Có lừa đảo trực tuyến, hack các trang web, hack tài khoản email cá nhân và các tài khoản mạng xã hội khác. Những điều này đã gây ra sự gián đoạn lớn cho một số cá nhân, văn phòng, tổ chức, cơ quan, công ty, Chính phủ và thậm chí là cả quốc gia. Tuy nhiên, đối với tất cả các mối đe dọa này, đều có các biện pháp phòng ngừa để chống lại nhằm giảm thiểu rủi ro từ các mối đe dọa bảo mật trực tuyến.

Nhưng điều này chỉ có thể thực hiện được nếu có kiến thức và nhận thức đầy đủ về các mối đe dọa, hậu quả của nó và cách giải quyết vấn đề.

Việt Nam cũng không ngoại lệ trước mối đe dọa an ninh mạng. Sau khi dịch vụ Internet được cung cấp vào năm 1997, số lượng người Việt Nam sử dụng điện thoại di động, máy tính, máy tính xách tay và mạng xã hội không ngừng tăng lên. Do đó, mối đe dọa an ninh mạng tăng lên tương ứng. Điều này đã khiến người dân và Chính phủ cảnh giác vì tính phức tạp của nó và khả năng gây ra thiệt hại ở mức độ lớn hơn. Có một số là nạn nhân của lừa đảo trực tuyến, bị lừa bởi cả bạn bè và người lạ, bắt nạt trên mạng xảy ra tràn lan và nhiều người tham gia vào những hoạt động bất hợp pháp thông qua mạng xã hội dẫn đến bị truy cứu trách nhiệm hình sự. Quan trọng nhất là có một lượng lớn thanh thiếu niên sử dụng điện thoại di động, máy tính, máy tính xách tay và Internet. Nguy cơ bị đe dọa an ninh mạng là rất cao đối với giới trẻ vì họ sử dụng Internet nhiều hơn hẳn so với người lớn.

2. Phạm vi nghiên cứu

Nghiên cứu này tìm hiểu mức độ nhận thức và kiến thức của thanh thiếu niên ở Việt Nam về các mối đe dọa an ninh mạng và các biện pháp phòng ngừa. Nghiên cứu này không phải một nghiên cứu chuyên sâu. Vì vậy, những phát hiện từ nghiên cứu này chỉ giới hạn ở nhận thức về mối đe dọa an ninh mạng và kiến thức về một số biện pháp phòng ngừa cơ bản. Các phát hiện sẽ dựa trên phản hồi định lượng do những người tham gia cung cấp.

3. Ý nghĩa của nghiên cứu

Nghiên cứu này tìm hiểu nhận thức, kiến thức của giới trẻ về mối đe dọa an ninh mạng và một số biện pháp phòng ngừa. Điều này giúp thiết lập một số mức độ hiểu biết về nhận thức và kiến thức của giới trẻ liên quan đến mối đe dọa an ninh mạng và các biện pháp phòng ngừa. Từ kết quả nghiên cứu, các cơ quan, tổ chức có liên quan sẽ có thể tiến hành một chương trình hoặc thực hiện chương trình vận động để giáo dục thanh thiếu niên. Nghiên cứu này cũng sẽ chỉ ra sự cần thiết phải nghiên cứu sâu hơn về các lĩnh vực tương tự để có được kiến thức và hiểu biết chuyên sâu.

4. Mục tiêu nghiên cứu

- Tìm hiểu nhận thức của giới trẻ về mối đe dọa an ninh mạng.
- Tìm hiểu kiến thức của giới trẻ về mối đe dọa an ninh mạng.
- Tìm hiểu những biện pháp được giới trẻ áp dụng để ngăn chặn các mối đe dọa an ninh mạng.

5. Phương pháp nghiên cứu

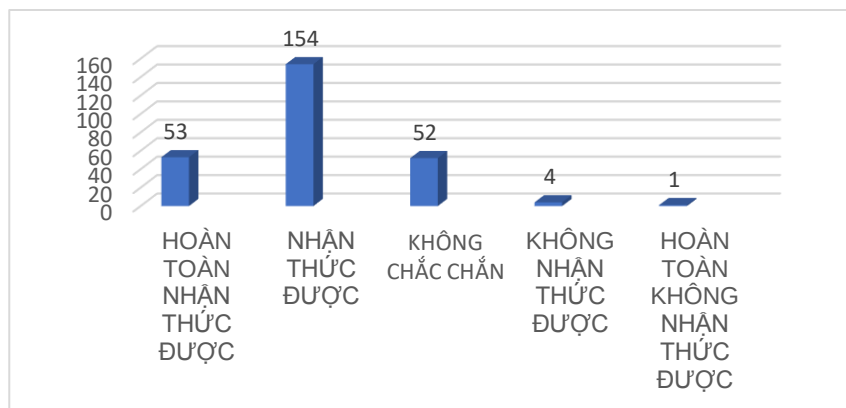
Nghiên cứu này sử dụng phương pháp định lượng để tiếp cận với nhiều thanh thiếu niên hơn, đồng thời thu được kiến thức và hiểu biết đầy đủ về giới trẻ cũng như nhận thức của họ về an ninh mạng và những mối đe dọa trực tuyến. Hơn nữa, dữ liệu

khách quan được tạo ra và được truyền đạt bằng số liệu thống kê. Dữ liệu được thu thập định lượng bằng cách sử dụng các câu hỏi khảo sát vì những người tham gia được chọn ngẫu nhiên từ những nơi khác nhau. Bảng câu hỏi được thiết kế gồm 15 mục sử dụng thang đo Likert 5 mức độ. Cuộc khảo sát được thực hiện thông qua việc sử dụng Google Form trực tuyến. Việc lấy mẫu kết quả được sử dụng để chọn những người tham gia nghiên cứu: 117 nam và 147 nữ, tổng cộng 264 thanh niên đang theo học ở các lớp khác nhau, từ lớp 11 đến sinh viên đại học đã trả lời các câu hỏi khảo sát này.

6. Phân tích dữ liệu

Dữ liệu được thu thập trong Google Form đã được chuyển đổi sang bảng Excel và phân tích sâu hơn được thực hiện bằng gói công cụ phân tích dữ liệu trong Excel. Một phân tích mô tả đã được thực hiện để phân tích dữ liệu, biểu đồ cột và các biểu đồ khác được sử dụng để trình bày các phát hiện và diễn giải.

6.1. *Bạn có nhận thức được sự nguy hiểm của mỗi đe dọa an ninh mạng khi sử dụng điện thoại di động, máy tính xách tay, mạng xã hội và Internet?*



Hình 1: Nhận thức về sự nguy hiểm của mỗi đe dọa an ninh mạng

Có 20% (53) và 58,3% (154) thanh niên hoàn toàn nhận thức và nhận thức được sự nguy hiểm của mỗi đe dọa an ninh mạng khi sử dụng điện thoại di động, máy tính xách tay, mạng xã hội và Internet. Ngoài ra còn có 19,6% (52) thanh niên chưa chắc chắn về điều này.

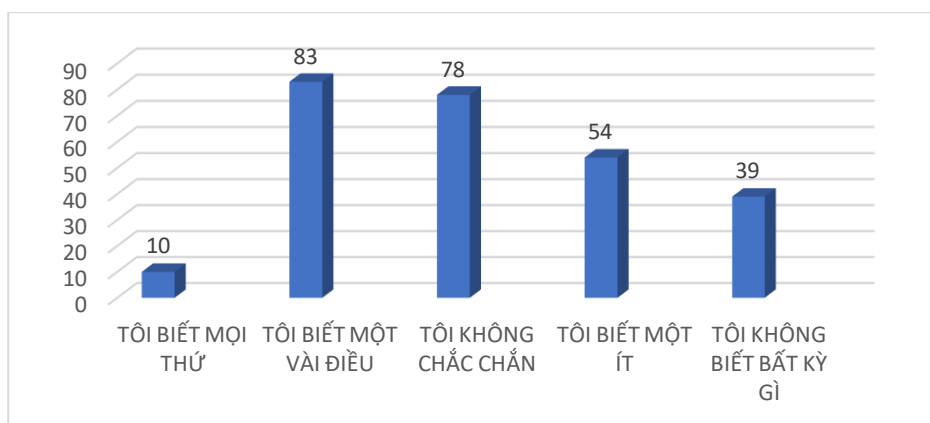
Bảng 1: Nhận thức về sự nguy hiểm của mỗi đe dọa an ninh mạng

Giá trị trung bình	3.96
Sai số chuẩn	0.04
Độ lệch chuẩn	0.70
Độ tin cậy	0.08

Giá trị trung bình là 3,96 với độ lệch chuẩn là 0,70 cho thấy giới trẻ nhận thức được sự nguy hiểm của mỗi đe dọa an ninh mạng khi sử dụng điện thoại di động, máy tính xách tay, mạng xã hội và Internet. Tuy nhiên, còn thiếu nhận thức đầy đủ về sự nguy hiểm của mỗi đe dọa an ninh mạng.

6.2. *Bạn biết bao nhiêu về xác thực hai yếu tố?*

Kỹ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”



Hình 2: Xác thực hai yếu tố

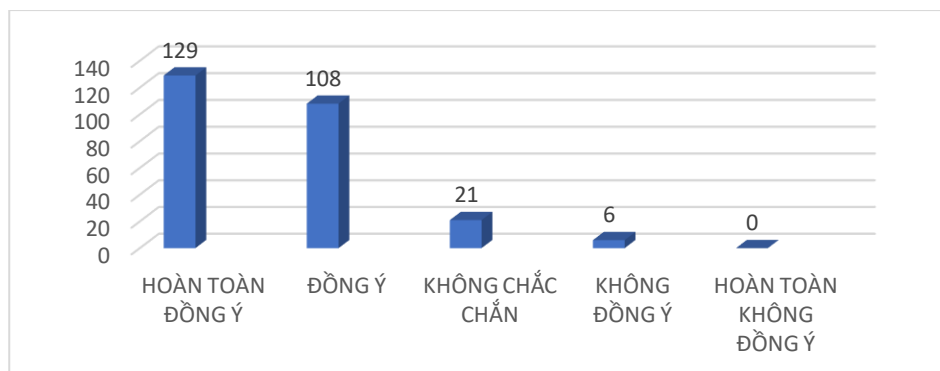
Chỉ có 3,8% (10) biết mọi thứ, 31,4% (83) biết một vài điều, 20,4% (54) biết một ít và 14,7% (39) không biết gì và 29,5% (78) không chắc chắn về xác thực hai yếu tố

Bảng 2: Kiến thức về xác thực 2 yếu tố

Giá trị trung bình	2.89
Sai số chuẩn	0.07
Độ lệch chuẩn	1.12
Độ tin cậy	0.14

Giá trị trung bình là 2,89 và độ lệch chuẩn là 1,12 cho thấy giới trẻ chỉ biết rất ít về xác thực hai yếu tố được áp dụng để bảo mật và bảo vệ trực tuyến khỏi các mối đe dọa.

6.3. *Tất cả mật khẩu mà tôi đã tạo cho email, tài khoản mạng xã hội và những mật khẩu khác có 8 hoặc nhiều hơn 8 ký tự?*



Hình 3: Mật khẩu có từ 8 ký tự trở lên

48,8% (129) hoàn toàn đồng ý và 40,9% (108) đồng ý rằng trong tất cả mật khẩu họ đã tạo cho email, tài khoản mạng xã hội và những mật khẩu khác đều có 8 ký tự trở lên. Ngoài ra, có 7,9% (21) thanh niên trả lời rằng họ không chắc chắn về điều đó.

Bảng 3: Sử dụng mật khẩu có từ 8 ký tự trở lên

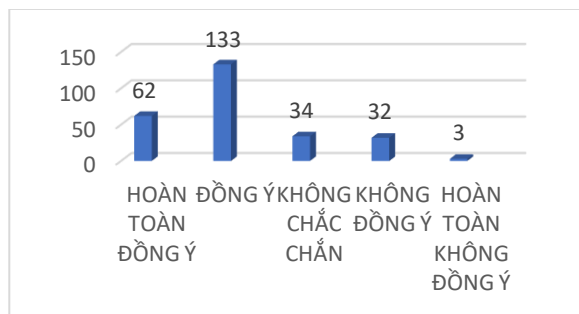
Giá trị trung bình	4.36
Sai số chuẩn	0.04
Độ lệch chuẩn	0.73

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Độ tin cậy	0.09

Giá trị trung bình là 4,36 và độ lệch chuẩn là 0,04 cho thấy giới trẻ hoàn toàn đồng ý rằng mật khẩu mà các bạn đã tạo có từ 8 ký tự trở lên. Điều này cho thấy mật khẩu họ sử dụng mạnh và an toàn theo yêu cầu tiêu chuẩn về an toàn và bảo mật.

6.4. Trong tất cả mật khẩu tôi sử dụng đều có hơn 3 loại ký tự khác nhau (bảng chữ cái, số, ký hiệu).



Hình 4: Mật khẩu có nhiều hơn 3 loại ký tự khác nhau

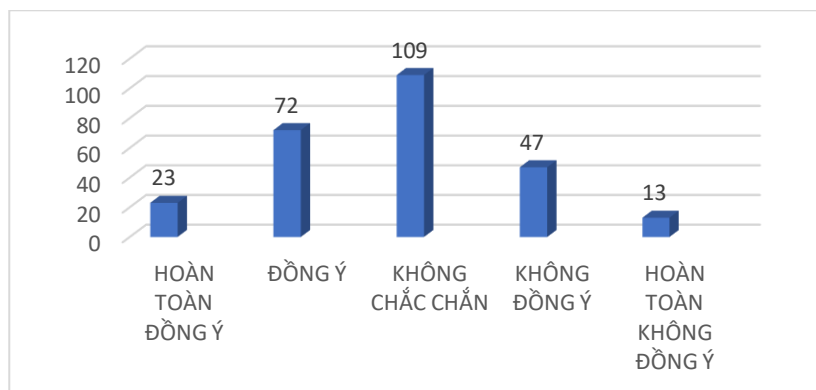
23,5% (62) hoàn toàn đồng ý, 50,4% (133) đồng ý, 12,9% (34) không chắc chắn và 12,1% (32) không đồng ý ở tất cả các mật khẩu mà họ sử dụng có hơn 3 loại ký tự khác nhau (bảng chữ cái, số và ký hiệu).

Bảng 4: Mật khẩu có nhiều hơn 3 loại ký tự khác nhau

Giá trị trung bình	3.82
Sai số chuẩn	0.05
Độ lệch chuẩn	0.96
Độ tin cậy	0.11

Các bạn trẻ đồng ý rằng mật khẩu của họ chứa 3 hoặc nhiều loại ký tự khác nhau với độ lệch chuẩn trung bình là 3,82 và 0,96. Độ lệch chuẩn cao hơn cho thấy có sự khác biệt lớn trong phản hồi của giới trẻ về việc có nhiều loại ký tự khác nhau trong mật khẩu.

6.5. Tôi đã lưu thông tin, dữ liệu và các tệp trên đám mây, sử dụng mã hóa đám mây để giữ an toàn từ tin tặc.



Hình 5: Sử dụng mã hóa đám mây

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

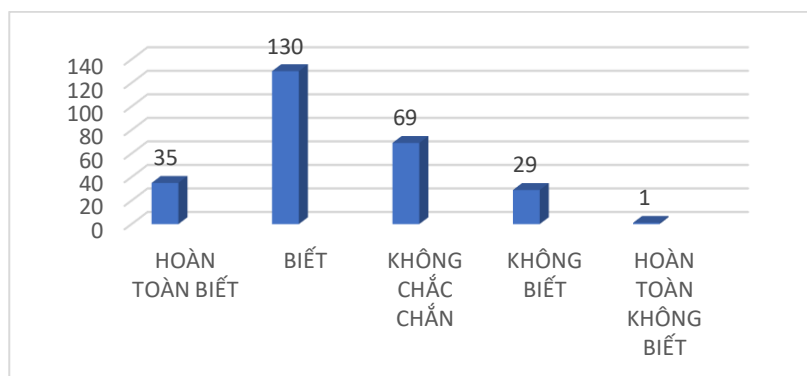
8,7% (23) hoàn toàn đồng ý, 27,3% (72) đồng ý, 41,3% (109) không chắc chắn, 12,1% (32) không đồng ý và 1,1% (3) hoàn toàn không đồng ý rằng họ đã lưu trữ thông tin, dữ liệu và các tệp trên đám mây, sử dụng mã hóa đám mây để giữ an toàn trước tin tặc.

Bảng 5: Sử dụng mã hóa đám mây

Giá trị trung bình	3.17
Sai số chuẩn	0.06
Độ lệch chuẩn	0.99
Độ tin cậy	0.12

Việc sử dụng mã hóa đám mây để lưu trữ thông tin, dữ liệu, tập tin của giới trẻ còn chưa phổ biến. Các giá trị trung bình là 3,17 với độ lệch chuẩn là 0,06 thể hiện rõ điều này.

6.6. *Bạn biết như thế nào về tính bảo mật và bảo vệ máy tính, điện thoại di động, iPad của mình và những thiết bị khác bằng tường lửa?*



Hình 6: Nhận thức về việc sử dụng tường lửa để bảo vệ các tiện ích

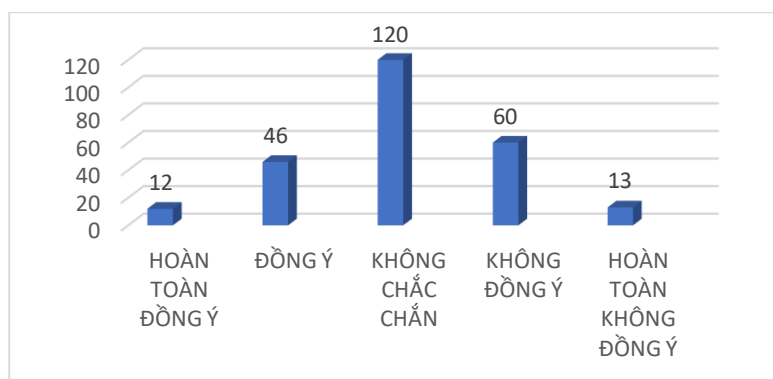
13,3% (35) hoàn toàn biết, 49,2% (130) biết, 26,1% (69) không chắc chắn và không biết 10,9% (29) về tính bảo mật và bảo vệ máy tính, điện thoại di động, iPad và các thiết bị khác bằng tường lửa.

Bảng 6: Nhận thức về việc sử dụng tường lửa để bảo vệ các thiết bị

Giá trị trung bình	3.64
Sai số chuẩn	0.05
Độ lệch chuẩn	0.85
Độ tin cậy	0.10

Nhận thức của các bạn trẻ về việc sử dụng tường lửa để bảo vệ các thiết bị được biểu thị bằng giá trị trung bình là 3,64 với sai số chuẩn là 0,05. Có một số người hoàn toàn không biết và một số người không chắc chắn hoặc không biết được biểu thị bằng độ lệch chuẩn.

6.7. *Trên điện thoại di động, máy tính xách tay, iPad, máy tính bảng hoặc phương tiện truyền thông xã hội khác, tôi đã sử dụng tường lửa.*



Hình 7: Số thanh niên sử dụng tường lửa

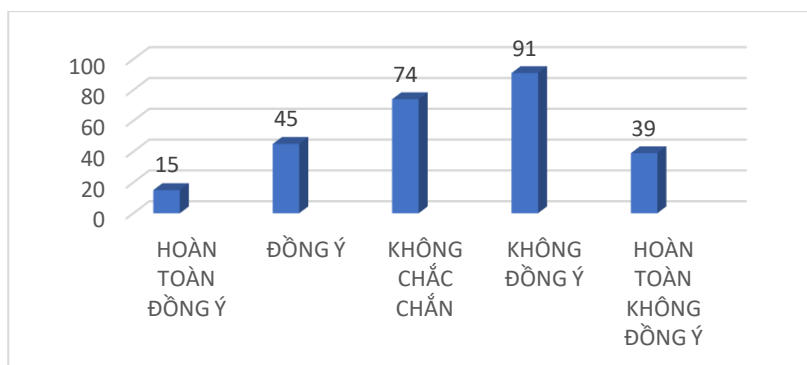
4,5% (12) hoàn toàn đồng ý, 17,4% (46) đồng ý, 45,5% (120) không chắc chắn, 22,7% (60) không đồng ý và 9,8% (26) hoàn toàn không đồng ý rằng họ đã sử dụng tường lửa trên điện thoại di động, máy tính xách tay, iPad, máy tính bảng hoặc phương tiện truyền thông xã hội khác.

Bảng 7: Thanh niên sử dụng tường lửa

Giá trị trung bình	2.85
Sai số chuẩn	0.06
Độ lệch chuẩn	0.97
Độ tin cậy	0.12

Việc sử dụng tường lửa trên thiết bị di động, máy tính xách tay, iPad, máy tính bảng hoặc các phương tiện truyền thông xã hội không phổ biến lắm trong giới trẻ. Đa số thanh niên cho biết họ không chắc chắn về việc sử dụng tường lửa và chỉ một số ít hoàn toàn đồng ý và nhiều người không đồng ý hoặc hoàn toàn không đồng ý được thể hiện bằng giá trị trung bình là 2,85 và độ lệch chuẩn là 0,97.

6.8. Tôi đã cài đặt trình chặn quảng cáo trên điện thoại di động, máy tính xách tay hoặc các thiết bị khác của mình, điều này sẽ giúp ngăn chặn quảng cáo và các công cụ theo dõi độc hại khác.



Hình 8: Sử dụng trình chặn quảng cáo

5,7% (15) hoàn toàn đồng ý, 17% (45) đồng ý, 28% (74) không chắc chắn, 34,4% (91) không đồng ý và 14,8% (39) hoàn toàn không đồng ý rằng họ đã cài đặt trình chặn

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

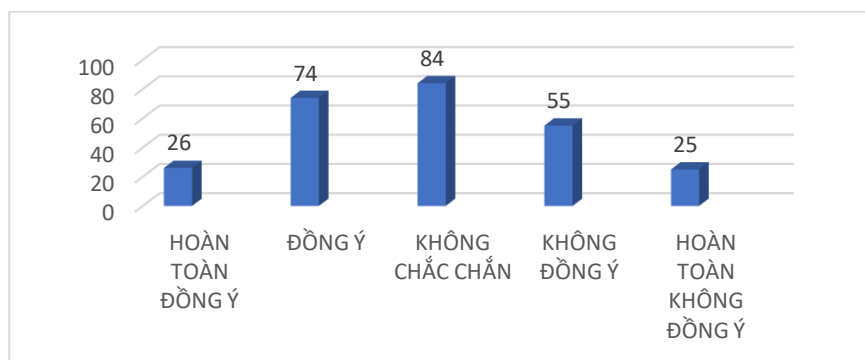
quảng cáo trên điện thoại di động, máy tính xách tay hoặc các thiết bị khác của họ, điều này sẽ giúp ngăn chặn quảng cáo và các công cụ theo dõi độc hại khác.

Bảng 8: Sử dụng trình chặn quảng cáo

Giá trị trung bình	2.63
Sai số chuẩn	0.07
Độ lệch chuẩn	1.10
Độ tin cậy	0.13

Các bạn trẻ không đồng ý, hoàn toàn không đồng ý hoặc không chắc chắn về việc cài đặt trình chặn quảng cáo trên điện thoại di động, máy tính xách tay và các thiết bị khác để giúp ngăn chặn quảng cáo và các công cụ theo dõi độc hại khác với giá trị trung bình là 2,63 và độ lệch chuẩn là 1,10.

6.9. *Tôi đã sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng. Phần mềm này có thể giúp xác định khi nào ai đó đã xâm nhập trái phép vào mạng của tôi hoặc cố truy cập vào tài khoản, tệp và thư mục của tôi.*



Hình 9: Sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng

9,8% (26) hoàn toàn đồng ý, 28% (74) đồng ý, 31,8% (84) không chắc chắn, 20,8% (55) không đồng ý và 9,5% (25) hoàn toàn không đồng ý rằng họ đã sử dụng phần mềm ngăn chặn và phát hiện xâm nhập mạng để giúp xác định khi nào ai đó đã xâm nhập trái phép vào mạng của họ hoặc cố gắng truy cập vào tài khoản, tập tin và thư mục của họ

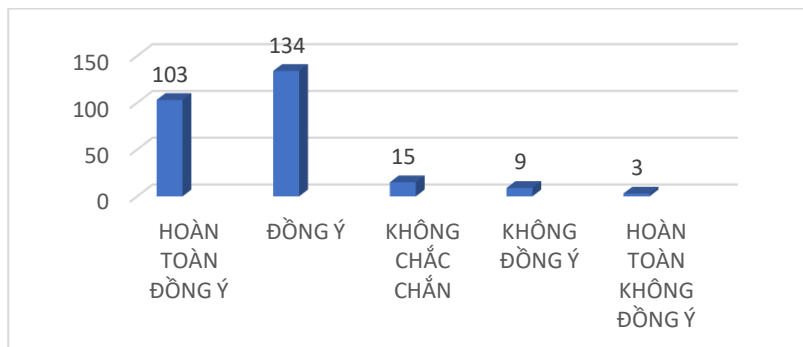
Bảng 9: Sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng

Giá trị trung bình	3.08
Sai số chuẩn	0.07
Độ lệch chuẩn	1.12
Độ tin cậy	0.14

Giá trị trung bình là 3,08 cho thấy thanh thiếu niên không chắc chắn liệu mình có sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng để xác định khi nào có ai đó đã xâm nhập trái phép vào mạng của mình hoặc cố gắng truy cập vào tài khoản, tập tin, thư mục hay không. Tuy nhiên, xét theo độ lệch chuẩn 1,12 thì số lượng thanh niên

đồng ý hoặc không đồng ý về việc sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng gần như bằng nhau.

6.10. Tôi thường xuyên cập nhật hệ thống và phần mềm trên điện thoại di động và máy tính xách tay của mình.



Hình 10: Cập nhật hệ thống và phần mềm

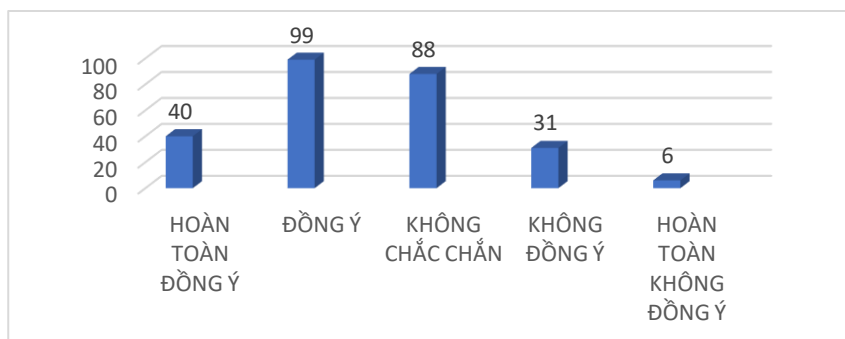
39% (103) hoàn toàn đồng ý, 50,8% (134) đồng ý, 5,7% (15) không chắc chắn, 3,4% (9) không đồng ý và 1,1% (3) hoàn toàn không đồng ý rằng họ cập nhật hệ thống và phần mềm trên điện thoại di động và máy tính xách tay của họ thường xuyên.

Bảng 10: Cập nhật hệ thống, phần mềm

Giá trị trung bình	4.22
Sai số chuẩn	0.05
Độ lệch chuẩn	0.81
Độ tin cậy	0.10

Các bạn trẻ đồng ý rằng họ liên tục cập nhật phần mềm và hệ thống trên điện thoại di động và máy tính xách tay của mình theo giá trị trung bình là 4,22 với độ lệch chuẩn là 0,81. Tuy nhiên, cũng có một số bạn trẻ không cập nhật hệ thống và phần mềm của mình.

6.11. Tôi đã mã hóa và khóa tất cả dữ liệu có trong điện thoại di động hoặc máy tính xách tay của mình.



Hình 11: Mã hóa và khóa dữ liệu

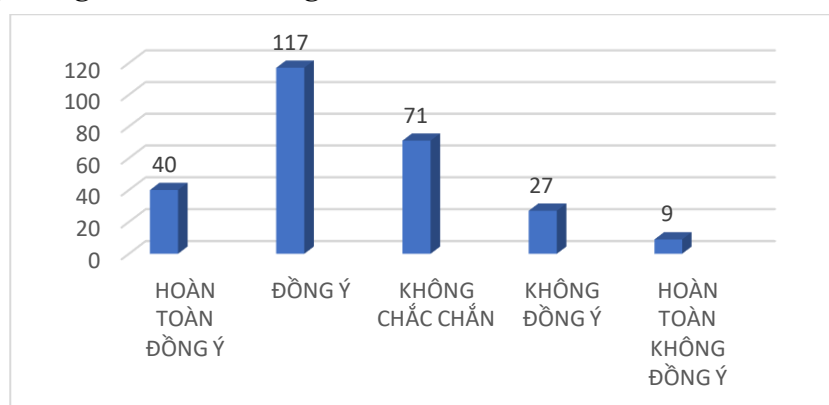
15,2% (40) hoàn toàn đồng ý, 37,5% (99) đồng ý, 33,3% (88) không chắc chắn, 11,7% (31) không đồng ý và 2,3% (6) hoàn toàn không đồng ý rằng họ đã mã hóa và khóa tất cả dữ liệu có trong điện thoại di động hoặc máy tính xách tay của họ.

Bảng 11: Mã hóa và khóa dữ liệu

Giá trị trung bình	3.52
Sai số chuẩn	0.06
Độ lệch chuẩn	0.96
Độ tin cậy	0.12

Các thanh niên đồng ý rằng họ đã mã hóa và khóa tất cả dữ liệu có trong điện thoại di động hoặc máy tính xách tay của họ được biểu thị bằng giá trị trung bình là 3,52 và độ lệch chuẩn là 0,96.

6.12. *Tôi giám sát mạng của mình và xem điều gì đang đi vào mạng của tôi và điều gì đang đi ra khỏi mạng.*



Hình 12: Mạng lưới giám sát

15,2% (40) hoàn toàn đồng ý, 44,3% (117) đồng ý, 26,9% (71) không chắc chắn, 10,2% (27) không đồng ý và 3,4% (9) hoàn toàn không đồng ý rằng họ giám sát mạng của mình và xem điều gì đang đi vào mạng của họ và điều gì đang đi ra khỏi mạng.

Bảng 12: Mạng lưới giám sát

Giá trị trung bình	3.58
Sai số chuẩn	0.06
Độ lệch chuẩn	0.97
Độ tin cậy	0.12

Các bạn trẻ đồng ý rằng họ giám sát mạng của mình và xem những gì đang đến với mạng lưới của họ và những gì đang vượt ra khỏi nó như được biểu thị bằng giá trị trung bình là 3,58 và độ lệch chuẩn là 0,97.

7. Thảo luận

7.1. Nhận thức về mối nguy hiểm của mối đe dọa an ninh mạng

Nhận thức được về những mối nguy hiểm của mối đe dọa an ninh mạng liên quan đến việc sử dụng điện thoại di động, máy tính xách tay, cũng như mạng xã hội và Internet là tốt. Có 20% (53) nhận thức đầy đủ và 58,3% (154) thanh niên nhận thức được mối

nguy hiểm từ mối đe dọa an ninh mạng khi sử dụng điện thoại di động, máy tính xách tay, mạng xã hội và Internet.

Ngoài ra còn có 19,6% (52) thanh niên chưa chắc chắn về vấn đề này, đây là điều đáng lo ngại. Phát hiện này được đưa ra dựa trên tài liệu tham khảo trong đó tuyên bố rằng thanh niên ngày nay thiếu các biện pháp phòng ngừa an toàn khi sử dụng các thiết bị thông minh như điện thoại di động, máy tính xách tay, máy tính để bàn, máy tính bảng và nhiều thiết bị khác.

7.2. Xác thực hai yếu tố

Kiến thức về xác thực hai yếu tố còn khá kém. Chỉ có 3,8% (10) biết mọi thứ và 31,4% (83) biết một vài điều về nó. Mặt khác, có 20,4% (54) biết ít và 14,7% (39) không biết gì và 29,5% (78) không chắc chắn về điều đó. Đây là mối lo ngại lớn vì có rất nhiều người chưa có kiến thức đầy đủ về xác thực hai yếu tố.

Do thiếu kiến thức, rủi ro an ninh mạng có thể dẫn đến các mối đe dọa đối với danh tính bí mật, danh tính cũng như quyền riêng tư đối với người dùng Internet cá nhân như đã đề cập trong tài liệu tham khảo.

7.3. Ký tự mật khẩu

Thanh niên đã tạo và sử dụng mật khẩu mạnh vì 48,8% (129) hoàn toàn đồng ý và 40,9% (108) đồng ý rằng tất cả mật khẩu họ tạo cho điện thoại di động, email, tài khoản mạng xã hội và các mật khẩu khác đều có từ 8 ký tự trở lên. Chỉ có 7,9% (21) thanh niên trả lời rằng họ không chắc chắn về điều đó. Hơn nữa, có 23,5% (62) thanh niên hoàn toàn đồng ý, 50,4%

(133) đồng ý, 12,9% (34) không chắc chắn và 12,1% (32) không đồng ý rằng có nhiều hơn ba loại ký tự khác nhau (bảng chữ cái, số). và ký hiệu) trong tất cả mật khẩu mà họ sử dụng. Việc sử dụng mật khẩu mạnh là một biện pháp để giảm thiểu các mối đe dọa trực tuyến. Những phát hiện từ điều này chỉ ra rằng giới trẻ hiểu rõ hơn về sự cần thiết của mật khẩu mạnh vì họ đã tạo mật khẩu có chứa hơn 8 ký tự. Đây là một trong những biện pháp an toàn tốt được các bạn trẻ thực hiện.

7.4. Sử dụng mã hóa đám mây

Có 8,7% (23) thanh niên hoàn toàn đồng ý, 27,3% (72) đồng ý, 41,3% (109) không chắc chắn, 12,1% (32) không đồng ý và 1,1% (3) hoàn toàn không đồng ý rằng họ đã lưu trữ thông tin, dữ liệu và các tệp trên đám mây, sử dụng mã hóa đám mây để giữ an toàn trước tin tặc. Điều này trở nên quan trọng vì nếu có người dùng trái phép truy cập vào dữ liệu, kẻ xâm nhập đó sẽ không thể giải mã được dữ liệu đó. Như vậy, mã hóa đám mây sẽ mang lại sự bảo mật tốt hơn.

7.5. Bảo mật và bảo vệ bằng tường lửa

Hệ thống tường lửa là cần thiết để triển khai và thực thi kiểm soát truy cập giữa hai mạng, thường bảo vệ mạng riêng nội bộ và khỏi các yếu tố bên ngoài có thể xâm

phạm quyền riêng tư và bảo mật bằng cách cho phép các dạng lưu lượng truy cập cụ thể lưu chuyển giữa chúng. Có 13,3% (35) thanh niên nhận thức đầy đủ và 49,2% (130) nhận thức được vấn đề an ninh, bảo vệ máy tính, điện thoại di động, iPad và các thiết bị khác có tường lửa. Các phát hiện chỉ ra rằng giới trẻ có nhận thức nhất định về việc sử dụng tường lửa để đảm bảo an ninh và bảo vệ. Tuy nhiên, có 26,1% (69) thanh niên chưa chắc chắn và 10,9% (29) chưa biết về hệ thống bảo vệ tường lửa.

Hơn nữa, chỉ có một số sinh viên sử dụng tường lửa trên điện thoại di động, máy tính xách tay, iPad, Máy tính bảng hoặc các phương tiện truyền thông xã hội khác vì chỉ có 4,5% (12) hoàn toàn đồng ý và 17,4% (46) đồng ý. Điều này càng được khẳng định khi có 45,5% (120) thanh niên không chắc chắn, 22,7% (60) không đồng ý và 9,8% (26) hoàn toàn không đồng ý rằng họ đã sử dụng tường lửa trên điện thoại di động, máy tính xách tay, iPad, Máy tính bảng hoặc phương tiện truyền thông xã hội khác.

7.6. Trình chặn quảng cáo

Việc sử dụng trình chặn quảng cáo không phổ biến trong giới trẻ vì chỉ có 5,7% (15) trong số họ hoàn toàn đồng ý và 17% (45) trong số họ đồng ý rằng họ đã cài đặt trình chặn quảng cáo trên điện thoại di động, máy tính xách tay hoặc thiết bị khác của họ. Mặt khác, có 77,2% (204) người không chắc chắn, không đồng ý và hoàn toàn không đồng ý việc họ cài đặt trình chặn quảng cáo trên thiết bị của mình. Phát hiện này chỉ ra rằng giới trẻ có nhiều khả năng gặp phải vấn đề hơn trong việc ngăn chặn quảng cáo và các công cụ theo dõi độc hại khác.

7.7. Mã hóa và khóa

Việc mã hóa và khóa dữ liệu được giới trẻ coi là quan trọng vì lý do an toàn và bảo mật. 15,2% (40) trong số họ hoàn toàn đồng ý và 37,5% (99) đồng ý rằng họ đã mã hóa và khóa dữ liệu trong máy tính xách tay hoặc điện thoại di động của mình. Tuy nhiên, cũng có rất nhiều bạn trẻ chưa mã hóa, khóa dữ liệu. 33,3% (88) trong số họ không chắc chắn, 11,7% (31) không đồng ý và 2,3% (6) trong số họ hoàn toàn không đồng ý rằng họ đã mã hóa và khóa tất cả dữ liệu có trong điện thoại di động hoặc máy tính xách tay của họ.

7.8. Sử dụng phần mềm và mạng giám sát

Những phát hiện từ nghiên cứu này cho thấy rằng mạng của họ có sự giám sát thích hợp và cũng kiểm tra những gì đang vào và ra khỏi mạng của họ. 15,2% (40) thanh niên hoàn toàn đồng ý và 44,3% (117) đồng ý rằng họ đã giám sát mạng lưới của mình. Các phát hiện cũng cho thấy có 26,9% (71) thanh niên không chắc chắn, 10,2% (27) không đồng ý và 3,4% (9) hoàn toàn không đồng ý rằng họ giám sát mạng của mình và xem điều gì đang xảy ra với mạng của họ và điều gì đang diễn ra từ nó

Chỉ có 37,9% (100) thanh niên hoàn toàn đồng ý và 28% (74) đồng ý rằng mình đã sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng. 62,1% (164) thanh niên

không chắc chắn, không đồng ý và hoàn toàn không đồng ý rằng họ đã sử dụng phần mềm phát hiện và ngăn chặn xâm nhập mạng giúp xác định khi nào ai đó đã xâm nhập trái phép vào mạng của họ hoặc cố gắng truy cập vào tài khoản, tập tin và thư mục của họ.

7.9. Cập nhật phần mềm và hệ thống

89,8% (237) thanh niên hoàn toàn đồng tình và nhất trí rằng họ cập nhật hệ thống cũng như phần mềm trên điện thoại di động và máy tính xách tay thường xuyên. Có một số ít trong số họ khoảng 5,7% (15) không chắc chắn, 3,4% (9) không đồng ý và 1,1% (3) hoàn toàn không đồng ý rằng họ cập nhật hệ thống và phần mềm trên điện thoại di động và máy tính xách tay của họ thường xuyên. Những phát hiện từ điều này cho thấy giới trẻ quan tâm nhiều hơn đến hệ thống và phần mềm trên điện thoại di động và máy tính xách tay của họ vì chúng dường như được cập nhật thường xuyên.

8. Kết luận

Mối đe dọa an ninh mạng là mối quan tâm lớn của mọi người; điều đó thậm chí còn nguy hiểm hơn đối với giới trẻ vì họ hầu hết sử dụng các thiết bị thông minh có kết nối Internet. Hơn nữa, hầu hết thanh niên không nhận thức được mối đe dọa an ninh mạng và rủi ro liên quan đến việc sử dụng Internet và các thiết bị tiện ích. Mặc dù có những biện pháp có thể được thực hiện để giảm thiểu các loại mối đe dọa khác nhau, nhưng nếu thanh niên không nhận thức được những biện pháp này thì họ rất dễ bị xâm hại.

Tuy nhiên, việc sử dụng mật khẩu mạnh và ký tự mật khẩu hơn 3 loại được giới trẻ biết đến và sử dụng. Điều này phục vụ như một cửa ngõ để ngăn chặn các mối đe dọa bên ngoài. Hơn nữa, một trong những phát hiện từ nghiên cứu này chỉ ra rằng giới trẻ luôn cập nhật điện thoại di động và các thiết bị khác của họ với hệ thống và phần mềm mới nhất. Điều này rất quan trọng đối với sự an toàn của các thiết bị cũng như người dùng. Mức độ nhận thức tốt cho việc sử dụng tường lửa để bảo vệ và bảo mật. Nhưng số thanh niên thực sự sử dụng tường lửa để bảo vệ và bảo mật điện thoại di động cũng như các thiết bị khác của họ lại rất ít như được chỉ ra trong các phát hiện trên. Vì vậy, chỉ nhận thức sẽ không giải quyết được bất kỳ vấn đề nào liên quan đến rủi ro và mối đe dọa an ninh nếu không áp dụng nó.

Nhận thức và kiến thức về lưu trữ, bảo quản an toàn dữ liệu đang là vấn đề đáng lo ngại vì phần lớn các bạn trẻ chưa có nhận thức và kiến thức đầy đủ. Chỉ có một số thanh niên đã mã hóa và khóa dữ liệu của họ trên điện thoại di động hoặc trong các tài khoản mạng xã hội. Việc giám sát mạng và sử dụng các phần mềm phát hiện, xâm nhập mạng chưa phổ biến trong giới trẻ. Đây có thể là mối lo ngại về mối đe dọa bảo mật hoặc rủi ro liên quan đến việc sử dụng Internet, thiết bị di động và các tiện ích khác.

Thanh thiếu niên phải được giáo dục đầy đủ về các mối đe dọa và rủi ro bảo mật để cung cấp một môi trường trực tuyến an toàn hơn.

Nếu không, giới trẻ sẽ tiếp tục sử dụng Internet và các thiết bị có nguy cơ gặp phải nhiều mối đe dọa và rủi ro trực tuyến khác nhau.

Xung đột lợi ích: Tác giả tuyên bố rằng không có bất kỳ xung đột lợi ích nào khi thực hiện nghiên cứu này.

TÀI LIỆU THAM KHẢO

- P. Bhatia and R. Sehrawat, “Types of security threats and prevention,” *International Journal for Scientific Research & Development*, vol. 2, no. 8, pp. 281–283, 2014.
- A. Mukherjee, *Network Security Strategies, Protect Your Network and Enterprise Against Advanced Cybersecurity Attacks and Threats*, 1st ed. Birmingham: Packt Publishing, Ltd., Livery Place, 2020.
- A. Farrukh, R. Sadwick and J. Villasenor, *Youth Internet Safety: Risks, Responses, and Research Recommendations*. Centre for Technology Innovation at Brookings, 2014.
- S. Z. Omar, K. Kovalan and J. Bolong, “Information security awareness among youth in Klang Valley: A focus group discussion,” *International Journal of Academic Research in Business & Social Sciences*, vol. 10, no. 16, pp. 193–205, 2020.
- M. Jouini, L. B. Arfa Rabai and A. B. Aissa, “Classification of security threats in information systems,” *Procedia Computer Science*, vol. 32, no. 2014, pp. 489–496, 2014.
- S. Bhola, S. Kaur and G. Kumar, “Internet threats and prevention—A brief review,” *International Journal of Computer Applications*, pp. 13–17, 2015.
- Common Wealth of Australia, *Protecting Yourself Online*, 2nd edition. Australian Government, 2011.
- A. Sundaram, “Understanding and protecting yourself against threats in the Internet,” *Asian Social Science*, vol.13, no. 12, pp. 201–226, 2017.
- P. Mai and A. Tick, “Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam,” *Acta Polytechnica*, vol. 18, no. 8, pp. 67–89, 2021.
- T. Alharbi and A. Tassaddiq, “Assessment of cybersecurity awareness among students of Majmaah University,” *Big Data and Cognitive Computing*, vol. 5, no. 23, 2021.
- Australian Computer Society, *Cybersecurity-Threats Challenges Opportunities*. ACS, 2016.

- National Children Bureau, Keeping Children and Young People Safe Online: An e-Safety Strategy and ThreeYear Action Plan for Northern Ireland 2019–2022. Northern Ireland Executives, 2019.148 JCS, 2021, vol.3, no.3
- N. Alsherif, University Youth and Online Safety in Egypt: Use and Trust, M.S. thesis. The American University in Cairo, School of Global Affairs and Public Policy, 2015.
- T. Spielhofer, Children’s Online Risks and Safety: A Review of the Available Evidence. United Kingdom Council for Child Internet Safety, 2010.
- D. Finkelhor, K. Walsh, L. Jones, K. Mitchell and A. Collier, “Youth Internet safety education: Aligning programs with the evidence base,” Trauma, Violence & Abuse, vol. 1, no. 15, pp. 1–15, 2020.
- V. Sithira and Y. Nguwi, “A study on the adolescent online security issues,” International Journal of Multidisciplinary and Current Research, vol. 2, no. 2014, pp. 596–601, 2014.
- S. Singla and J. Singh, “Cloud data security using authentication and encryption technique,” Global Journal of Computer Science and Technology Cloud and Distributed, vol. 13, no. 3, pp. 31–35, 2013.
- T. Chown, J. Read and D. DeRoure, The Use of Firewalls in an Academic Environment (JTAP-631). Department of Electronics and Computer Science, University of Southampton, 2000.

NHỮNG YẾU TỐ TÁC ĐỘNG ĐẾN QUYẾT ĐỊNH SỬ DỤNG VÍ ĐIỆN TỬ CỦA SINH VIÊN TRÊN ĐỊA BÀN TP. HỒ CHÍ MINH
FACTORS AFFECTING THE DECISION TO USE E-WALLETS BY STUDENTS IN HO CHI MINH CITY

Trần Nguyễn Thành Công

Đại học Kinh tế TP. Hồ Chí Minh

Tác giả liên hệ: thanhcongid2002@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Ý định hành vi, Hành vi thực, Ví điện tử, TP.HCM.	Mục tiêu của nghiên cứu này là khám phá mối quan hệ giữa sự bảo mật và riêng tư, nỗ lực kỳ vọng, hiệu quả kỳ vọng, ảnh hưởng xã hội, ý định hành vi, điều kiện thuận lợi và hành vi thực sử dụng ví điện tử. Nghiên cứu này đã thu thập dữ liệu bằng cách gửi một bảng câu hỏi trực tuyến đến 261 sinh viên đang học tập tại Thành phố Hồ Chí Minh (TP.HCM), những người được hỏi đã có trải nghiệm về sử dụng ví điện tử. Kết quả từ mô hình hóa phương trình cấu trúc bình phương nhỏ nhất từng phần (PLS-SEM) bằng cách sử dụng phần mềm SmartPLS 3.3.3, nghiên cứu chỉ ra rằng sự bảo mật và riêng tư, nỗ lực kỳ vọng, hiệu quả kỳ vọng, ảnh hưởng xã hội đã tác động tích cực đến ý định hành vi sử dụng ví điện tử viên. Bên cạnh đó, ý định hành vi và điều kiện thuận lợi cũng có tác động tích cực đến hành vi thực sử dụng ví điện tử. Cuối cùng, nghiên cứu đề xuất các kiến nghị nhằm nâng cao trải nghiệm, chất lượng từ đó làm tăng số lượng sinh viên sử dụng ví điện tử.

ABSTRACT

<i>Keywords:</i> Behavior intention, Actual Behavior, E-wallets, Ho Chi Minh City.	The aim of this research is to explore the relationship between security and privacy, effort expectancy, performance expectancy, social influence, behavioral intention, facilitating conditions, and actual behavior of e-wallets. The study collected data by sending an online questionnaire to 261 students studying in Ho Chi Minh City (HCMC), who had experience using e-wallets. Results from the Partial Least Squares-Structural Equation Modeling (PLS-SEM) using SmartPLS 3.3.3 software

showed that security and privacy, effort expectancy, performance expectancy, and social influence had a positive impact on the behavioral intention to use e-wallets. Additionally, behavioral intention and facilitating conditions also had a positive impact on the actual behavior of e-wallets. Finally, the study proposes recommendations to enhance the experience and quality, thereby increasing the number of students using e-wallets.

1. Giới thiệu:

Sự bùng nổ của Cuộc cách mạng Công nghiệp Thứ Tư trong lĩnh vực công nghệ thông tin đã mang đến nhiều đổi mới cho cuộc sống của chúng ta. Kết hợp với sự phát triển liên tục của công nghệ thông tin, mô hình kinh doanh này đã được nâng cao không chỉ ở Việt Nam mà còn trên toàn thế giới. Ngay sau đó, sự xuất hiện của ví điện tử là một thành tựu lớn đóng góp cho tương lai của thương mại điện tử. Hầu hết các giao dịch trên nền tảng công nghệ này được chuyển đổi thành giao dịch tiền điện tử trên toàn cầu. Giải pháp an toàn này được chấp nhận bởi cả nhà cung cấp và người tiêu dùng. Hiện nay, người tiêu dùng Việt Nam tiếp xúc và hiểu biết về công nghệ thông tin hơn. Các công dân đều sở hữu một chiếc điện thoại thông minh, vì vậy sử dụng ví điện tử sẽ trở nên thuận tiện hơn bao giờ hết. Tuy nhiên, theo thống kê từ Merchant Machine năm 2021, Việt Nam là một trong Top 10 quốc gia trên thế giới có tỷ lệ sử dụng tiền mặt cao nhất, xếp thứ hai trên toàn cầu với tỷ lệ 69% dân số không có quyền truy cập vào dịch vụ tài chính hoặc tài khoản ngân hàng. Trong khi thanh toán không dùng tiền mặt là một xu hướng toàn cầu và ngày càng phổ biến, nhiều người Việt vẫn chọn thanh toán bằng tiền mặt truyền thống. Như chúng ta có thể thấy, thói quen sử dụng tiền mặt vẫn rất phổ biến. Nhận thức được vấn đề này, tác giả đã thực hiện đề tài để xác định các yếu tố ảnh hưởng đến quyết định của sinh viên sử dụng ví điện tử tại Thành phố Hồ Chí Minh, cũng như để hiểu các lý do, mức độ sử dụng, ưu điểm và nhược điểm cần được khắc phục với phương thức thanh toán điện tử này.

2. Cơ sở lý thuyết:

2.1. Cơ sở lý thuyết:

Ý định hành vi là biểu hiện của sự sẵn sàng thực hiện một hành vi của mỗi người (Fishbein & Ajzen, 1975). Nó được coi là tiền đề trực tiếp dẫn đến hành vi theo Mô hình chấp nhận công nghệ (TAM) của Fishbein và Ajzen (1975). Theo Venkatesh và cộng sự, (2003), Lý thuyết thống nhất về chấp nhận và sử dụng công nghệ (UTAUT) được đề xuất có tính đến việc áp dụng công nghệ. Cụ thể hơn, UTAUT là sự kết hợp của các lý thuyết từ lý thuyết hành động hợp lý, mô hình chấp nhận công nghệ, lý thuyết hành vi

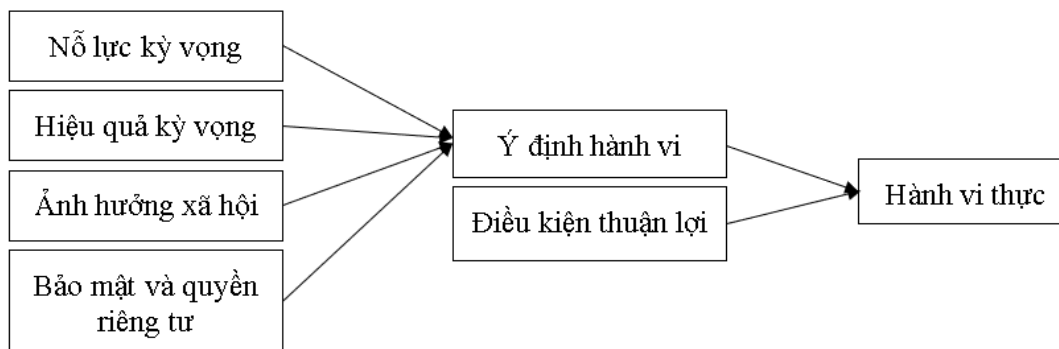
hoạch định, lý thuyết khuếch tán đổi mới và lý thuyết nhận thức xã hội. Cụ thể, ý định hành vi được xây dựng trên tám thang đo với kỳ vọng về hiệu suất, kỳ vọng về nỗ lực và các yếu tố xã hội có tác động trực tiếp đến ý định hành vi và yếu tố quyết định trực tiếp đến hành vi là các điều kiện thuận lợi. Williams, Rana, Dwivedi và Lal (2011) đã áp dụng lý thuyết UTAUT để kiểm tra một loạt công nghệ, Đồng thời, Junadi & Sfenrianto (2015); Slade, Dwivedi, Piercy & William (2015) cũng đã áp dụng lý thuyết UTAUT để khám phá lại các công cụ thanh toán trực tuyến khác nhau. Nghiên cứu này cũng tập trung vào chủ đề áp dụng công nghệ; do đó, việc sử dụng UTAUT làm cơ sở lý thuyết cho nghiên cứu này là phù hợp. Bốn cấu trúc độc lập quan trọng được áp dụng trong nghiên cứu này giống với lý thuyết UTAUT ban đầu. Nhóm nghiên cứu tin tưởng mạnh mẽ rằng để chấp nhận một phương thức thanh toán công nghệ mới như ví điện tử, người dùng Việt Nam sẽ phải cân nhắc các yếu tố đó.

UTAUT được đề xuất vào năm 2003; trọng tâm nghiên cứu của các tác giả khác về việc áp dụng lý thuyết của UTAUT được mở rộng thông qua việc sửa đổi và bổ sung các quan sát mở rộng thông qua việc sửa đổi và bổ sung các biến quan sát cũng như các thang đo. Các phép đo khác đã được xem xét bên cạnh việc kết hợp với các mô hình lý thuyết khác. Các tác giả tập trung vào việc xác định lại mối quan hệ nhân quả trong các mô hình khác với các biến UTAUT. Trong bài nghiên cứu này, nhóm nghiên cứu đã đặc biệt chú ý đến việc kết hợp các biến số này thông qua Lý thuyết về rủi ro nhận thức (TPR) do Bauer (1960) đề xuất. Bauer gợi ý rằng lợi ích thường gắn liền với rủi ro nhận thức được trong hành vi của người tiêu dùng, trong đó rủi ro được đề cập trong lý thuyết TPR là rủi ro được nhận thức. Sáu loại rủi ro nhận thức đã được nghiên cứu trong bối cảnh hành vi cá nhân, bao gồm rủi ro bảo mật thông tin, rủi ro quyền riêng tư cá nhân, rủi ro tài chính, rủi ro liên quan đến các mối quan hệ xã hội, rủi ro về thời gian / tiện lợi và rủi ro về hiệu suất. Theo Ostlund (1974) những rủi ro này được coi là rào cản đối với việc hình thành các sáng kiến.

Ví điện tử là một yếu tố của sự đổi mới trong công nghệ thanh toán của người tiêu dùng và nó tiềm ẩn nhiều rủi ro mà khách hàng lo lắng cả trực tiếp và gián tiếp, vì vậy lý thuyết này là phù hợp cho nghiên cứu này.

2.2. Giả thuyết và mô hình nghiên cứu đề xuất:

Dựa vào cơ sở lý thuyết đã trình bày ở trên và qua phân tích các nghiên cứu có sự tương đồng với đề tài này, với mục đích đánh giá mức độ chấp nhận của người dùng đối với việc sử dụng công nghệ mới, cụ thể là ví điện tử, nhóm tác giả đã đề xuất và xây dựng mô hình nghiên cứu về các yếu tố ảnh hưởng đến sự chậm phát triển trong việc sử dụng ví điện tử của sinh viên trên địa bàn TP.HCM được thể hiện trong hình 1.



Hình 1. Mô hình nghiên cứu đề xuất

Phần tiếp theo sẽ trình bày chi tiết các giả thuyết nghiên cứu trong mô hình.

2.2.1. Bảo mật và quyền riêng tư (Security and Privacy):

Theo Donald và Rémy (2012), tính bảo mật của ví điện tử là mức độ mà khách hàng tin rằng việc sử dụng một phương thức thanh toán cụ thể thông qua ứng dụng di động sẽ được giữ an toàn. Bảo mật liên quan đến xác thực, xác minh thông tin và bảo mật dữ liệu (Chen, 2008). Quyền riêng tư và bảo mật cũng làm tăng trải nghiệm của người tiêu dùng và nó cũng ảnh hưởng đáng kể đến khách hàng trong những rủi ro liên quan (Tran, 2020). Bên cạnh đó, quyền riêng tư của ví điện tử là quyền mà khách hàng mong muốn thông tin và giao dịch của họ được giữ bí mật (Chen, 2008). Nó bao gồm giữ thông tin nguyên vẹn, không có truy cập trái phép và không sử dụng thông tin cá nhân cho các mục đích khác. Theo Liu và Pham (2016), khi khách hàng tin tưởng vào phương thức thanh toán di động, họ liên quan đến sự trung thực và đáng tin cậy của các nhà cung cấp dịch vụ, khi đó, họ sẽ tăng ý định sử dụng hệ thống này. Donald và Rémy (2012) đã chỉ ra rằng bảo mật và quyền riêng tư trong thông tin cá nhân ảnh hưởng tích cực đến ý định hành vi. Do đó, dựa trên tổng quan lý thuyết, tác giả đề xuất giả thuyết sau:

H1: Bảo mật và quyền riêng tư ảnh hưởng tích cực đến ý định hành vi sử dụng ví điện tử.

2.2.2. Nỗ lực kỳ vọng (Effort Expectancy):

Nỗ lực kỳ vọng đề cập đến cách hệ thống được sử dụng hiệu quả. Nó bao gồm người dùng tương tác với hệ thống một cách rõ ràng, dễ hiểu và dễ sử dụng (Venkatesh và cộng sự, 2003). Bên cạnh đó, Junadi và Sfenrianto (2015) đã sử dụng thang đo nỗ lực kỳ vọng, bao gồm hệ thống thanh toán dễ sử dụng, giao dịch linh hoạt và hệ thống thanh toán dễ để học. Theo Nguyen và cộng sự (2014), bạn càng nỗ lực ít hơn trong việc sử dụng ví điện tử, bạn càng có dự định sử dụng nó nhiều hơn. Do đó, dựa trên tổng quan lý thuyết, tác giả đề xuất giả thuyết sau:

H2: Nỗ lực kỳ vọng ảnh hưởng tích cực đến ý định hành vi đối với ví điện tử.

2.2.3. Hiệu quả kỳ vọng (Performance Expectancy):

Hiệu quả kỳ vọng là mức độ mà người dùng tin rằng việc sử dụng ví điện tử sẽ giúp họ đạt được hiệu suất cao trong các phương thức thanh toán (Venkatesh và cộng sự, 2003). Theo Junadi và Sfenrianto (2015), hiệu quả kỳ vọng được định nghĩa khách hàng nhận được nhiều lợi ích hơn so với phương thức thanh toán truyền thống. Hiệu quả kỳ vọng được xem xét từ khía cạnh năng suất giao dịch, sự thuận tiện trong giao dịch và tốc độ trong giao dịch. Junadi and Sfenrianto (2015); Venkatesh và cộng sự (2003) đã chỉ ra rằng ý định sử dụng phương thức thanh toán bằng ví điện tử có lợi trong tất cả công việc của khách hàng. Do đó, dựa trên tổng quan lý thuyết, tác giả đề xuất giả thuyết sau:

H3: Hiệu quả kỳ vọng ảnh hưởng tích cực đến ý định hành vi sử dụng ví điện tử.

2.2.4. Ảnh hưởng xã hội (Social Influence):

Ảnh hưởng xã hội là mức độ một cá nhân bị ảnh hưởng bởi những người quan trọng với họ để tin rằng họ nên sử dụng một hệ thống công nghệ cụ thể (Venkatesh và cộng sự, 2003). Bên cạnh đó, với sự tiến bộ không ngừng của công nghệ và truyền thông kỹ thuật số cũng như mạng xã hội, các cá nhân cũng chịu ảnh hưởng lớn từ các nhóm và cộng đồng (Nguyen và cộng sự, 2014; Han, 2020). Venkatesh và cộng sự (2003) cho thấy ảnh hưởng xã hội là một trong bốn yếu tố ảnh hưởng trực tiếp và tích cực đến ý định của khách hàng. Các cá nhân có xu hướng bị ảnh hưởng bởi lời khuyên hoặc phản hồi từ mọi người trong giai đoạn đầu sử dụng công nghệ mà không có đủ kinh nghiệm và niềm tin. Do đó, dựa trên tổng quan lý thuyết, tác giả đề xuất giả thuyết sau:

H4: Ảnh hưởng xã hội ảnh hưởng tích cực đến ý định hành vi sử dụng ví điện tử.

2.3.5. Ý định hành vi (Behavior Intention):

Ý định hành vi là yếu tố tốt nhất để dự đoán một hành vi đúng (Fishbein & Ajzen, 1975). Theo đó, ý định được thể hiện ở sự sẵn sàng sử dụng sản phẩm / dịch vụ của người dùng (Venkatesh và cộng sự, 2003). Khi nghiên cứu ý định hành vi đối với ví điện tử trong thanh toán, bài nghiên cứu tập trung vào thang đo bao gồm ý định hành vi, kế hoạch sử dụng và dự đoán việc sử dụng hệ thống (Venkatesh và cộng sự, 2003). Cũng như các nghiên cứu trước đây, thái độ của người tiêu dùng ảnh hưởng tích cực đến ý định mua hàng. Bên cạnh đó, Kim và Won (2020) đồng tình rằng thái độ của người tiêu dùng đối với sản phẩm và dịch vụ có ảnh hưởng có ý nghĩa thống kê đến ý định mua hàng. Ý định sử dụng các hệ thống công nghệ có mối tương quan đáng kể với hành vi của người dùng (Fishbein & Ajzen, 1975). Có nghĩa là người tiêu dùng có ý định càng cao thì hành vi thực tế càng cao và ngược lại. Do đó, dựa trên tổng quan lý thuyết, tác giả đề xuất giả thuyết sau:

H5: Ý định hành vi ảnh hưởng tích cực đến hành vi thực sử dụng ví điện tử.

2.2.6. Điều kiện thuận lợi (Facilitating Conditions):

Điều kiện thuận lợi là cách các cá nhân tin rằng cơ sở hạ tầng kỹ thuật và tổ chức sẽ hỗ trợ việc thích nghi và sử dụng hệ thống công nghệ một cách thuận tiện. Khi nghiên

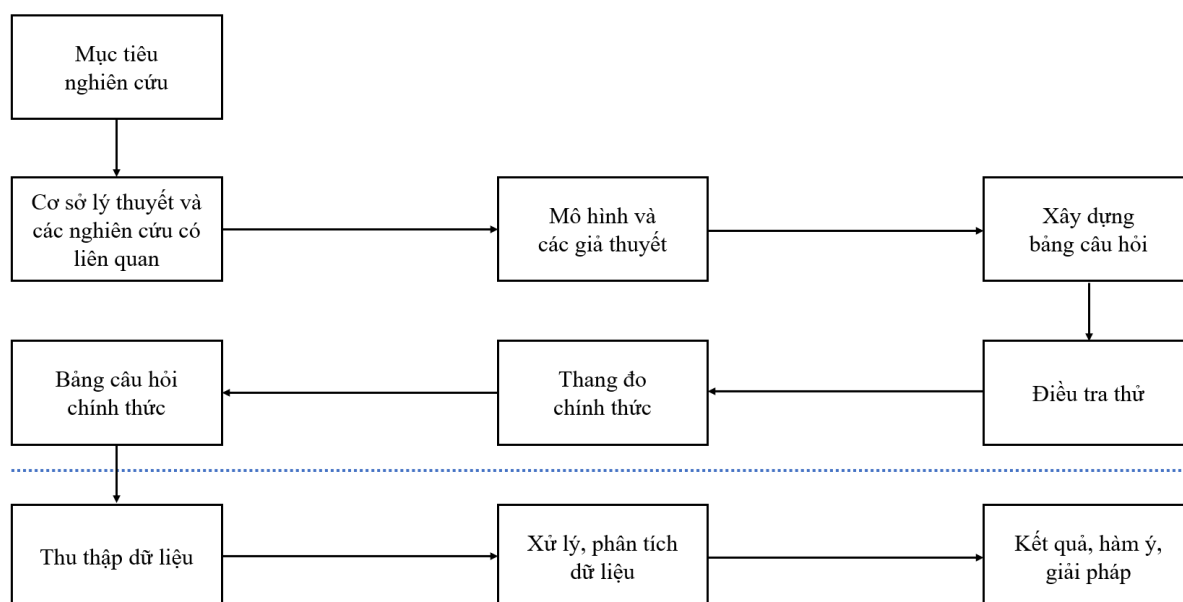
cứu các điều kiện thuận lợi, Venkatesh và cộng sự (2003) đã khám phá và xác định yếu tố có liên quan bao gồm các nguồn lực thiết yếu sẵn có để sử dụng hệ thống, khả năng tương thích với các hệ thống khác và một người (hoặc nhóm) cụ thể sẵn sàng hỗ trợ. Do đó, dựa trên tổng quan lý thuyết, nhóm tác giả đề xuất giả thuyết sau:

H6: Điều kiện thuận lợi ảnh hưởng tích cực đến hành vi thực sử dụng ví điện tử.

3. Phương pháp nghiên cứu:

3.1. Quy trình nghiên cứu:

Hình 2 thể hiện cụ thể và chi tiết quy trình nghiên cứu. Hai phương pháp chính được sử dụng trong mô hình này là (1) nghiên cứu sơ bộ nhằm mục đích xác định mô hình nghiên cứu đồng thời điều chỉnh thang đo phù hợp với phạm vi nghiên cứu; (2) nghiên cứu định lượng nhằm đánh giá mô hình đo lường và kiểm định mô hình cấu trúc. Nghiên cứu đánh giá độ tin cậy và giá trị (bao gồm giá trị hội tụ và giá trị phân biệt) của thang đo bằng cách sử dụng hệ số tin cậy Cronbach's alpha, hệ số tin cậy tổng hợp (CR) và phương sai trích trung bình (AVE), ma trận hệ số tương quan giữa các cấu trúc khái niệm (Fornell và Larcker, 1981), HTMT (Hair và cộng sự, 2016). Nghiên cứu cũng kiểm định sự đa cộng tuyến của thang đo thông qua hệ số VIF (Henseler và cộng sự, 2010). Tiếp theo đó, nghiên cứu sử dụng hệ số xác định (R^2) và sự liên quan của dự báo (Q^2) để đánh giá khả năng giải thích của các biến phụ thuộc. Quy trình bootstrapping (5000 mẫu) cũng được sử dụng để kiểm định các giả thuyết nghiên cứu thông qua kiểm định t-test (Hair và cộng sự, 2016).



Hình 2. Quy trình nghiên cứu

3.2. Phương pháp nghiên cứu:

Nghiên cứu sử dụng phương pháp tổng hợp và được tiến hành trong hai giai đoạn: nghiên cứu sơ bộ và nghiên cứu định lượng nhằm cung cấp kết quả chính xác nhất.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Phương pháp nghiên cứu sơ bộ được tiến hành bằng cách khảo sát, phỏng vấn và thu thập dữ liệu từ 10 sinh viên đã sử dụng ví điện tử trong một khoảng thời gian đủ để xây dựng và điều chỉnh mô hình. Tiếp theo, phương pháp nghiên cứu định lượng được thực hiện để xác minh độ chính xác của thang đo và tính phù hợp của mô hình nghiên cứu. Để thu thập dữ liệu, nhóm nghiên cứu phát triển một bảng câu hỏi khảo sát định lượng với 27 biến quan sát và đo bằng thang đo Likert 5 cấp độ. Tác giả chọn phương pháp mẫu tiện lợi. Sau một tháng tiến hành khảo sát và thu thập dữ liệu, tác giả đã chọn 261 bảng câu hỏi để phân tích sau khi thu thập, mã hóa và lựa chọn bằng phần mềm SPSS 20. Sau đó, thang đo được đánh giá và mô hình được kiểm tra bằng phần mềm SmartPLS 3.3.3 thông qua phương pháp phân tích PLS-SEM.

4. Kết quả nghiên cứu:

4.1. Mô tả nghiên cứu:

Việc thu thập dữ liệu được thực hiện bằng cách gửi một bảng câu hỏi trực tuyến cho sinh viên ở TP.HCM. Phương pháp lấy mẫu thuận tiện đã được thực hiện với những người có khả năng truy cập Internet và có kinh nghiệm sử dụng ví điện tử. Tổng số 280 bảng câu hỏi đã được phản hồi, trong đó 261 bảng câu hỏi có thể sử dụng được cho phân tích dữ liệu, với tỷ lệ phản hồi 93.2%. Thông tin nhân khẩu học của người trả lời được trình bày trong Bảng 1.

Bảng 1. Thống kê đặc điểm nhân khẩu học

N = 261		Tần số	%
Giới tính	Nữ	108	41.4
	Nam	153	58.6
Niên học	Năm 1	59	22.6
	Năm 2	79	30.3
	Năm 3	95	36.4
	Năm 4	28	10.7
Trình độ học vấn	Trung cấp, Cao đẳng	100	38.3
	Đại học	161	61.7

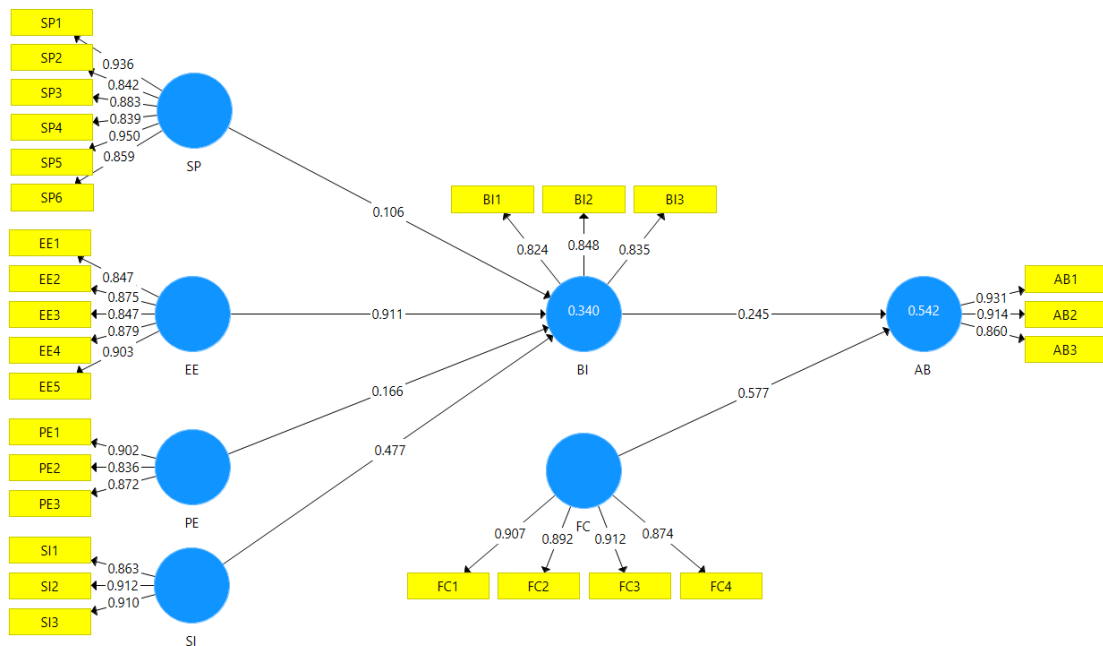
Về cơ cấu giới tính: Tỷ lệ Nam/ Nữ trong nghiên cứu này không chênh lệch nhiều: 58.6% là Nam và 41.4% là Nữ. Về cơ cấu theo niên học: Phần lớn sinh viên tham gia khảo sát đang học năm 2 và năm 3 chiếm tỷ lệ khá cao lần lượt là 30.3% và 36.4%. Về cơ cấu theo trình độ học vấn: Đối tượng tham gia khảo sát đa số đang theo học Đại học chiếm tỷ lệ 61.7%.

4.2. Đánh giá mô hình đo lường:

Kết quả mô hình đo lường các khái niệm (đã chuẩn hóa) được trình bày trong Hình 3, qua đó ta thấy được các chỉ tiêu đo lường trong mô hình này đều thỏa mãn yêu

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

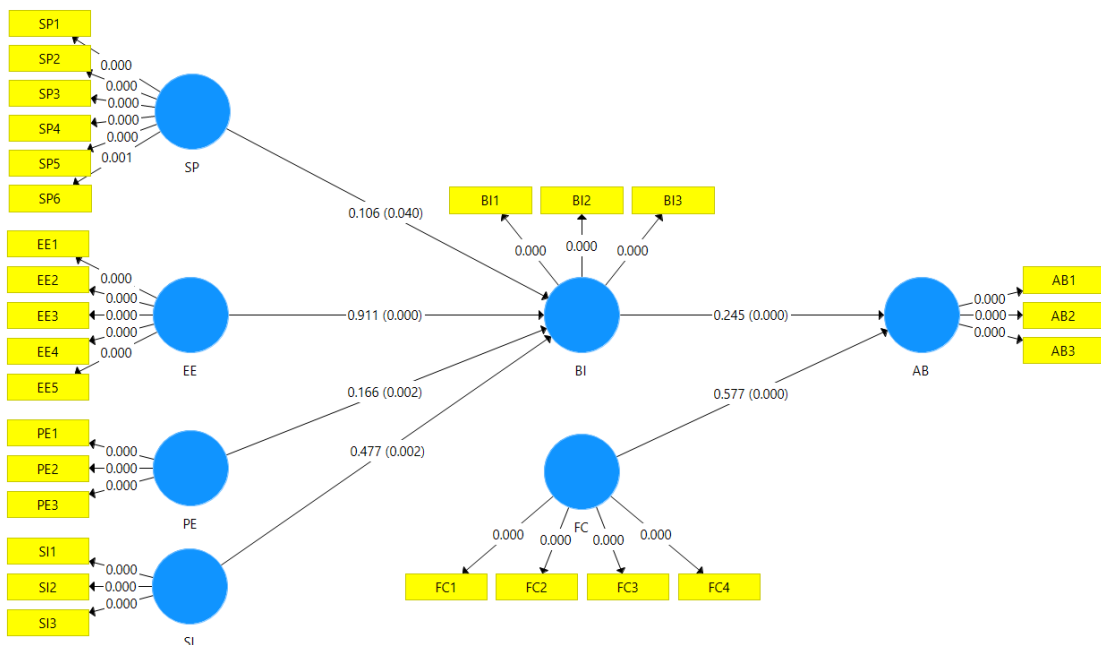
cầu và đủ điều kiện đưa vào phân tích mô hình cấu trúc tuyến tính SEM nhằm mục đích kiểm định các giả thuyết trong mô hình đề xuất nghiên cứu.



Hình 3: Mô hình đo lường các khái niệm (đã chuẩn hóa)

4.3. Đánh giá mô hình cấu trúc:

Kết quả ước lượng mô hình cấu trúc và kiểm định các giả thuyết trong mô hình được trình bày trong Hình 4 như sau



Hình 4. Kết quả kiểm định mô hình cấu trúc

Khi kiểm định sự đa cộng tuyến, VIF không được lớn hơn 5 (Hair và cộng sự, 2016). Tuy nhiên, các nhà nghiên cứu cũng có thể lựa chọn một tiêu chí nghiêm ngặt hơn trong đó VIF nên thấp hơn 3 (Hair và cộng sự, 2018). Qua kết quả kiểm định, hệ số

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

VIF của các cấu trúc khái niệm đều nhỏ hơn 3 (xem Bảng 2), cho thấy hiện tượng đa cộng tuyến giữa các biến giải thích (độc lập) không ảnh hưởng đến việc kiểm định giả thuyết nghiên cứu.

Bảng 2. Giá trị VIF

Giả thuyết		VIF
Sự bảo mật và riêng tư → Ý định hành vi	H1	1.146
Nỗ lực kỳ vọng → Ý định hành vi	H2	2.102
Hiệu quả kỳ vọng → Ý định hành vi	H3	1.110
Ảnh hưởng xã hội → Ý định hành vi	H4	1.778
Ý định hành vi → Hành vi thực	H5	1.412
Điều kiện thuận lợi → Hành vi thực	H6	1.412

(Nguồn: Từ kết quả tính toán của tác giả)

Mô hình cấu trúc tiếp tục được xem xét với việc sử dụng kỹ thuật bootstrapping cho lượng mẫu phóng đại có lặp lại là 5000 mẫu ($n = 5000$), với cỡ mẫu ban đầu là 261.

Bảng 3. Kết quả Bootstrapping mô hình cấu trúc và kiểm định các giả thuyết đề xuất

Giả thuyết	Mối tương quan	Trọng số hồi quy chuẩn hóa (β)	Độ lệch chuẩn	Giá trị t	Giá trị p	Kiểm định giả thuyết
H1	SP → BI	0.106	0.150	3.170	0.002	Chấp nhận
H2	EE → BI	0.911	0.158	5.776	0.000	Chấp nhận
H3	PE → BI	0.166	0.054	3.079	0.002	Chấp nhận
H4	SI → BI	0.477	0.150	3.170	0.002	Chấp nhận
H5	BI → AB	0.245	0.070	3.524	0.000	Chấp nhận
H6	FC → AB	0.577	0.065	8.904	0.000	Chấp nhận

(Nguồn: Từ kết quả tính toán của tác giả)

Từ bảng 3 cho thấy, trong 6 giả thuyết tác động trực tiếp mà tác giả đưa ra, tất cả các giả thuyết đều được chấp nhận vì có giá trị p-value < 0.05 . Trong đó giả thuyết H1 giả định rằng Sự bảo mật và riêng tư (SP) tác động tích cực đến Ý định hành vi (BI), được chấp nhận ($\beta = 0.106$, $p = 0.002$). Nỗ lực kỳ vọng (EE) có tác động tích cực đến Ý định hành vi (BI) ($\beta = 0.911$, $p = 0.000$) (H2 được chấp nhận). Hiệu quả kỳ vọng tác động tích cực đến Ý định hành vi (BI) ($\beta = 0.166$, $p = 0.002$) (H3 được chấp nhận). Ảnh

hưởng xã hội (SI) tác động tích cực đến Ý định hành vi (BI) ($\beta = 0.477$, $p = 0.002$), H4 được chấp nhận. Giả thuyết H5 giả định rằng Ý định hành vi (BI) tác động tích cực đến Hành vi thực (AB), được chấp nhận ($\beta = 0.245$, $p = 0.000$). Bên cạnh đó, Điều kiện thuận lợi (FC) có tác động tích cực làm tăng Hành vi thực ($\beta = 0.577$, $p = 0.000$) (H6 được chấp nhận).

4.4. Thảo luận kết quả nghiên cứu:

Sau kết quả phân tích, 6 giả thuyết ban đầu từ mô hình nghiên cứu đề xuất là đều được chấp nhận. Qua đó, chúng ta nhận thấy rõ mối quan hệ giữa các biến sự bảo mật và riêng tư, nỗ lực kỳ vọng, hiệu quả kỳ vọng, ảnh hưởng xã hội, điều kiện thuận lợi, ý định hành vi và hành vi thực sử dụng ví điện tử, cụ thể như sau:

Sự bảo mật và riêng tư có tác động tích cực đến ý định hành vi sử dụng ví điện tử (H1: $\beta = 0.106$). Kết quả này tương tự như các nghiên cứu trước đây. Nhóm tác giả cho rằng việc đảm bảo tính bảo mật và riêng tư cho thông tin cá nhân và giao dịch tài chính của sinh viên giúp tăng cường sự tin tưởng và an tâm cho người dùng. Sinh viên sẽ cảm thấy yên tâm và an toàn hơn khi sử dụng ví điện tử để thực hiện các giao dịch tài chính, tránh những rủi ro liên quan đến việc bị lộ thông tin cá nhân hay bị chiếm đoạt tài khoản. Sự bảo mật và riêng tư còn giúp đảm bảo tính hiệu quả của dịch vụ và đáp ứng yêu cầu pháp lý, điều này rất quan trọng với các sinh viên đã và đang sử dụng ví điện tử. Ngoài ra, sự bảo mật và riêng tư cũng đóng vai trò quan trọng trong việc tăng cường sự hài lòng và tín nhiệm của sinh viên đối với dịch vụ. Nếu sinh viên cảm thấy thông tin của mình được bảo vệ tốt và không bị lộ ra ngoài, họ sẽ có ý định sử dụng ví điện tử thường xuyên hơn, tăng tính tiện ích của dịch vụ này và đóng góp vào sự phát triển của ví điện tử.

Nỗ lực kỳ vọng có tác động mạnh nhất đến ý định hành vi sử dụng ví điện tử (H2: $\beta = 0.911$). Kết quả này tương tự như các nghiên cứu trước đây. Nhóm tác giả cho rằng do sinh viên là một nhóm người dùng tiềm năng quan trọng của ví điện tử, bởi họ thường xuyên thực hiện các giao dịch thanh toán nhỏ trong cuộc sống hàng ngày. Nếu trải nghiệm sử dụng ví điện tử của họ dễ dàng và tiện lợi, sẽ tạo ra nỗ lực kỳ vọng tích cực. Điều này có thể đưa đến ý định hành vi tích cực sử dụng ví điện tử của sinh viên, bởi họ có niềm tin vào tính tiện lợi và an toàn của dịch vụ này.

Hiệu quả kỳ vọng có tác động đến ý định hành vi sử dụng ví điện tử (H3: $\beta = 0.166$). Kết quả này tương tự như các nghiên cứu trước đây. Nhóm tác giả cho rằng sinh viên sẽ có xu hướng sử dụng ví điện tử nếu họ tin rằng sử dụng nó sẽ giúp họ tiết kiệm thời gian và tiền bạc trong các giao dịch thanh toán. Nếu các sinh viên tin rằng việc sử dụng Ví điện tử sẽ giúp họ tránh được các rủi ro liên quan đến tiền tệ và thời gian, như giả mạo thông tin thanh toán hay trễ hạn trong giao dịch, thì họ cũng sẽ có động lực cao hơn để sử dụng Ví điện tử.

Ảnh hưởng xã hội có tác động mạnh đến ý định hành vi sử dụng Ví điện tử (H4: $\beta = 0.477$). Kết quả này tương tự như các nghiên cứu trước đây. Nhóm tác giả cho rằng việc một số người trong mạng lưới xã hội của sinh viên sử dụng Ví điện tử có thể tạo ra sự ảnh hưởng đến sinh viên và khiến cho họ có xu hướng sử dụng nó. Điều này có thể xảy ra thông qua các đánh giá và đề xuất tích cực từ các bạn bè hoặc đồng nghiệp, hoặc thông qua các sự kiện, chương trình khuyến mãi và ưu đãi được tổ chức bởi Ví điện tử, mà có thể tạo ra sự hứng thú và thúc đẩy sử dụng Ví điện tử của sinh viên.

Ý định hành vi có tác động đến hành vi thực sử dụng Ví điện tử (H5: $\beta = 0.245$). Kết quả này tương tự như các nghiên cứu trước đây. Nhóm tác giả cho rằng nếu sinh viên có ý định sử dụng Ví điện tử, họ sẽ có xu hướng thực hiện việc sử dụng đó. Tuy nhiên, ý định hành vi cũng phụ thuộc vào nhiều yếu tố khác như hiệu quả kỳ vọng, ảnh hưởng xã hội, sự bảo mật và riêng tư, kinh nghiệm sử dụng dịch vụ thanh toán điện tử, và nhiều yếu tố khác. Nếu các yếu tố này được đáp ứng và đảm bảo, ý định hành vi sử dụng Ví điện tử của sinh viên sẽ được tăng cường và dẫn đến hành vi thực tế sử dụng Ví điện tử của họ. Điều này đặc biệt quan trọng trong việc xây dựng niềm tin và sự tin tưởng của khách hàng đối với Ví điện tử, đồng thời giúp tăng cường sự phát triển và phổ biến của hình thức thanh toán điện tử này.

Điều kiện thuận lợi có tác động mạnh đến hành vi thực sử dụng Ví điện tử (H6: $\beta = 0.577$). Kết quả này tương tự như các nghiên cứu trước đây. Nhóm tác giả cho rằng Khi có các điều kiện thuận lợi, như một môi trường kinh doanh phát triển và công nghệ thông tin phổ biến, việc sử dụng Ví điện tử sẽ trở nên dễ dàng và tiện lợi hơn cho sinh viên. Khi có các điều kiện thuận lợi như vậy, sinh viên sẽ dễ dàng tiếp cận và sử dụng Ví điện tử để thanh toán các giao dịch hàng hóa và dịch vụ. Từ đó làm gia tăng hành vi thực sử dụng Ví điện tử của sinh viên.

5. Kết luận và hàm ý:

5.1. Tóm tắt nội dung nghiên cứu:

Vấn đề nghiên cứu chính của đề tài là nghiên cứu các yếu tố ảnh hưởng đến việc sử dụng ví điện tử của sinh viên tại TP.HCM. Để xác định được mức độ tác động của các yếu tố đó trong vấn đề nghiên cứu này, phương pháp nghiên cứu sơ bộ và nghiên cứu định lượng được sử dụng phối hợp với nhau. Nghiên cứu sơ bộ được thực hiện dựa vào một số nghiên cứu trước đây ở trong nước và trên thế giới, qua đó 27 biến quan sát được thiết lập với 6 biến sự bảo mật và riêng tư, 5 biến về nỗ lực kỳ vọng, 3 biến về hiệu quả kỳ vọng, 3 biến về ảnh hưởng xã hội, 4 biến về điều kiện thuận lợi, 3 biến về ý định hành vi và 3 biến về hành vi thực. Nghiên cứu định lượng được thực hiện bằng hình thức gửi bảng câu hỏi khảo sát online cho đối tượng là sinh viên trên địa bàn TP.HCM. Kết quả là 261/280 bảng câu hỏi nghiên cứu có câu trả lời hợp lệ, thỏa số lượng yêu cầu để tiến hành kiểm định mô hình nghiên cứu. Tiếp đến, dữ liệu được đưa

vào phần mềm SPSS 20 và SmartPLS 3.3.3 để tiến hành bước đánh giá mô hình đo lường và đánh giá mô hình cấu trúc. Dùng phương pháp đánh giá mô hình đo lường để kiểm định giá trị của thang đo, kết quả là các thang đo đều đạt độ tin cậy. Phương pháp đánh giá mô hình cấu trúc được sử dụng để kiểm định các giả thuyết nghiên cứu. Từ kết quả phân tích, ta thấy tất cả các giả thuyết H1, H2, H3, H4, H5, H6 đều được chấp nhận.

5.2. Ý nghĩa và hàm ý quản trị:

Kết quả nghiên cứu của đề tài góp phần cung cấp cho sinh viên và các doanh nghiệp có cái nhìn rõ nét hơn về các yếu tố cốt lõi ảnh hưởng đến ý định hành vi và hành vi thực của nhóm khách hàng là sinh viên. Từ đó, có thể đưa ra những giải pháp phù hợp hơn để cải thiện hành vi thực sử dụng. Thông qua bài nghiên cứu, ta thấy được các yếu tố có tác động đến hành vi thực sử dụng của sinh viên là sự bảo mật và riêng tư, nỗ lực kỳ vọng, hiệu quả kỳ vọng, ảnh hưởng xã hội, ý định hành vi và điều kiện thuận lợi. Đây có thể là các yếu tố tạo giá trị cốt lõi trong việc quyết định hành vi thực của sinh viên.

Do đó để nâng cao hành vi thực của sinh viên cần điều chỉnh các yếu tố sự bảo mật và riêng tư, nỗ lực kỳ vọng, hiệu quả kỳ vọng, ảnh hưởng xã hội, ý định hành vi và điều kiện thuận lợi. Đây là 6 yếu tố có tác động đến hành vi thực của sinh viên. Do đó, nhóm tác giả đề xuất một số hàm ý quản trị nhằm giúp cải thiện hành vi thực sử dụng Ví điện tử của sinh viên như sau:

Về sự bảo mật và riêng tư: Ví điện tử cần tăng cường các biện pháp bảo mật và phân quyền truy cập, đồng thời cung cấp cho người dùng quyền kiểm soát thông tin cá nhân của mình. Ngoài ra, các chính sách bảo vệ quyền riêng tư và thông tin cần được công khai và minh bạch để người dùng có thể tin tưởng và sử dụng ứng dụng một cách an toàn. Ngoài ra, nhà quản trị cần tăng cường các hoạt động đào tạo và tư vấn cho người dùng về các vấn đề liên quan đến sự bảo mật và riêng tư, nhằm giúp họ hiểu rõ hơn về cách sử dụng và bảo vệ thông tin cá nhân của mình. Các chương trình khuyến khích sử dụng ví điện tử cần được thiết kế để đảm bảo sự tiện lợi và an toàn cho người dùng, đồng thời tăng cường giải đáp thắc mắc và hỗ trợ khách hàng để tạo sự tin tưởng và sự hài lòng của người dùng. Bên cạnh đó, Nhà quản trị nên luôn cập nhật và phát triển các tính năng mới để cải thiện trải nghiệm của người dùng, đồng thời nghiên cứu và ứng dụng các công nghệ mới nhằm đảm bảo sự bảo mật và riêng tư cho người dùng.

Về nỗ lực kỳ vọng: Đầu tiên, các quản trị viên có thể đưa ra các chương trình giáo dục và tài liệu hướng dẫn để giải thích cho sinh viên về lợi ích của việc sử dụng Ví điện tử, bao gồm các tính năng an toàn và tiện lợi của nó. Thứ hai, các quản trị viên cần đảm bảo rằng hệ thống thanh toán qua Ví điện tử của trường học hoặc các tổ chức liên kết được thiết lập một cách dễ dàng và an toàn để giúp sinh viên dễ dàng sử dụng. Cuối cùng, quản trị viên cần liên tục đánh giá và cải thiện trải nghiệm của sinh viên khi sử dụng Ví điện tử để đảm bảo rằng họ cảm thấy thoải mái và tin tưởng về việc sử dụng nó.

Về hiệu quả kỳ vọng: Các quản trị viên có thể thúc đẩy hiệu quả kỳ vọng để cải thiện hành vi thực sự sử dụng Ví điện tử của sinh viên bằng cách cung cấp cho họ thông tin chi tiết về các tính năng của ứng dụng và cách sử dụng chúng. Việc tạo ra các hướng dẫn sử dụng chi tiết và rõ ràng có thể giúp giảm sự bất mãn và tăng khả năng sinh viên sử dụng Ví điện tử một cách hiệu quả. Ngoài ra, việc giảm thiểu các rào cản kỹ thuật và hạn chế về khả năng truy cập cũng có thể tăng cường hiệu quả kỳ vọng của sinh viên đối với việc sử dụng Ví điện tử. Quản trị viên cần đảm bảo rằng ứng dụng của họ dễ sử dụng và cung cấp cho người dùng trải nghiệm tốt nhất có thể để thúc đẩy hành vi thực sự sử dụng Ví điện tử của sinh viên.

Về ảnh hưởng xã hội: Ví điện tử cần xây dựng một chính sách quản trị hiệu quả về ảnh hưởng xã hội có thể giúp cải thiện hành vi thực sử dụng Ví điện tử của sinh viên. Chính sách này có thể bao gồm các hoạt động như tăng cường quảng bá về tính an toàn và tiện lợi của Ví điện tử, tạo ra một môi trường ủng hộ sử dụng Ví điện tử bằng cách liên kết với các nhà cung cấp dịch vụ và các tổ chức địa phương để tăng cường ảnh hưởng xã hội tích cực, đồng thời xây dựng chương trình khuyến khích cho người dùng sử dụng Ví điện tử một cách đúng cách, đảm bảo thông tin cá nhân được bảo mật và tránh các hành vi lừa đảo trực tuyến.

Về ý định hành vi: Đầu tiên, cần tăng cường khả năng truyền tải thông tin về tính năng, đáng tin cậy và tiện lợi của Ví điện tử thông qua các kênh truyền thông và chiến dịch tiếp thị hiệu quả. Thứ hai, cần thiết lập mối quan hệ tin cậy với khách hàng thông qua chăm sóc khách hàng, hỗ trợ tốt hơn và đảm bảo chất lượng dịch vụ. Thứ ba, cần đưa ra các chính sách khuyến khích, giảm giá, ưu đãi cho khách hàng để tăng cường khả năng trao đổi thông tin giữa khách hàng và các nhà cung cấp dịch vụ. Cuối cùng, cần cải thiện trải nghiệm người dùng bằng cách cập nhật và nâng cấp liên tục ứng dụng, giải quyết các vấn đề kỹ thuật, giảm thiểu thời gian giao dịch và nâng cao trải nghiệm người dùng.

Về điều kiện thuận lợi: Để cải thiện hành vi thực sử dụng Ví điện tử của sinh viên thông qua việc tăng cường điều kiện thuận lợi, các quản trị viên nên đưa ra các giải pháp như tối ưu hóa giao diện ứng dụng, cải thiện trải nghiệm người dùng, tăng cường hỗ trợ khách hàng, đảm bảo tính bảo mật và an toàn cho người dùng khi giao dịch. Ngoài ra, cần phát triển các chương trình khuyến mãi, ưu đãi để thu hút và giữ chân người dùng. Các đối tác liên kết và nhà cung cấp dịch vụ cũng cần được lựa chọn kỹ càng để đảm bảo chất lượng và độ tin cậy của các dịch vụ liên quan đến Ví điện tử.

5.3. Hạn chế của đề tài và hướng nghiên cứu tiếp theo:

Nghiên cứu này nâng cao kiến thức về hành vi thực sử dụng Ví điện tử mà sinh viên đang có trải nghiệm thực tế. Tuy nhiên, giống như bất kỳ nghiên cứu nào, nó cũng có một số hạn chế.

Đầu tiên, trong quá trình thay đổi và hoàn thiện thang đo cũng gặp nhiều khó khăn và bất cập do những hạn chế trong khả năng nghiên cứu sơ bộ của nhóm tác giả. Vì vậy, những nghiên cứu sau có thể phát triển và tối ưu mức độ giải thích của mô hình.

Thứ hai, kích thước mẫu còn nhỏ so với các mức khuyến nghị khảo sát. Kết quả nghiên cứu này chưa phân tích được sự ảnh hưởng dựa theo năng lực, giới tính cũng như mục tiêu của những đối tượng khảo sát. Vì thế, có thể có rất nhiều yếu tố khác ảnh hưởng đến hành vi thực sử dụng Ví điện tử.

Cuối cùng, do chỉ tiến hành khảo sát sinh viên trên địa bàn TP.HCM, nên nghiên cứu này vẫn chưa thể khái quát hóa cho tất cả sinh viên trong cả nước. Trong khi đó, ở Việt Nam do ảnh hưởng của văn hóa vùng miền, nên quan điểm và nhận thức của sinh viên ở các trường thuộc các khu vực khác có thể có sự khác biệt. Vì vậy, cần thiết phải có nhiều nghiên cứu tiếp theo được thực hiện với việc khảo sát đầy đủ hơn trên địa bàn cả nước để đảm bảo cho mô hình nghiên cứu có thể đạt được kết quả toàn diện.

Dựa vào những hạn chế trên của đề tài, từng hạn chế đều có thể đưa ra xem xét và nghiên cứu, đây cũng là định hướng nghiên cứu chuyên sâu tiếp theo của đề tài.

LỜI CẢM ƠN

Tôi xin chân thành cảm ơn sự hỗ trợ và đóng góp của các cá nhân và tổ chức trong quá trình nghiên cứu của tôi. Đặc biệt, tôi muốn gửi lời cảm ơn đến Đại học Kinh tế TP.HCM đã cung cấp cho tôi tài liệu và thông tin quan trọng để hoàn thành nghiên cứu này. Sự đóng góp của họ đã giúp tôi có được kết quả nghiên cứu chính xác và đáng tin cậy. Tôi hy vọng rằng nghiên cứu của tôi sẽ đóng góp vào sự phát triển của lĩnh vực này và hỗ trợ cho các nghiên cứu tương lai.

REFERENCES

- Bauer, R. A. (1960). Consumer behavior as risk taking. Paper presented at the Proceedings of the 43rd National Conference of the American Marketing Association, June 15, 16, 17, Chicago, Illinois, 1960.
- Chen, L. (2008). A model of consumer acceptance of mobile payment. *International Journal of Mobile Communications*, 6(1), 32-52.
- Chen, L.-d. J. I. J. o. M. C. (2008). A model of consumer acceptance of mobile payment. 6(1), 32-52.
- Donald, L. A., & Rémy, M.-W. (2012). Building a Research Model for Mobile Wallet Consumer Adoption: The Case of Mobile Suica in Japan. *Journal of Theoretical and Applied Electronic Commerce Research*, 7(1), 94-110.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.
- Fishbein, M., Ajzen, I. J. P., & Rhetoric. (1977). Belief, attitude, intention, and behavior: An introduction to theory and research. 10(2).

- Fornell, C., & Bookstein, F. L. J. J. o. M. r. (1982). Two structural equation models: LISREL and PLS applied to consumer exit-voice theory. 19(4), 440-452.
- Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. J. I. J. o. M. D. A. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. 1(2), 107-123.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. J. U. S. R., NJ: Pearson Education. Haley, RI . Benefit segmentation: a decision-oriented research tool. The Journal of Marketing. (2010). Multivariate data analysis: International version. 32(3), 30-35.
- Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. J. L. R. P. (2012). Applications of partial least squares path modeling in management journals: A review of past practices and recommendations for future applications. 45(5-6), 320-340.
- Han, J. H. (2020). The Effects of Personality Traits on Subjective Well-being and Behavioral Intention Associated with Serious Leisure Experiences. Journal of Asian Finance, Economics and Business, 7(5), 167-176. <https://doi.org/10.13106/jafeb.2020.vol7.no5.167>.
- Henseler, J., Ringle, C. M., & Sarstedt, M. J. J. o. t. a. o. m. s. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. 43(1), 115-135.
- Junadia, & Sfenrianto. (2015). A Model of Factors Influencing Consumer's Intention to Use E-Payment System in Indonesia. Procedia Computer Science, 59, 214-220.
- Junadi^a, S. J. P. C. S. (2015). A model of factors influencing consumer's intention to use e-payment system in Indonesia. 59, 214-220.
- Nguyen, D. T., Nguyen, T. D., & Cao, T. H. (2014). Acceptance and Use of Cloud-based E-learning. Journal of Science and Technology Development, 17(Q3), 69-84.
- Nguyen, T. D., Nguyen, D. T., Cao, T. H. J. S., & Journal, T. D. (2014). Acceptance and Use of Cloud-based E-learning. 17(3), 71-87.
- Ostlund, L. E. J. J. o. c. r. (1974). Perceived innovation attributes as predictors of innovativeness. 1(2), 23-29.
- Tran, V. D. (2020). The Relationship among Product Risk, Perceived Satisfaction and Purchase Intentions for Online Shopping. Journal of Asian Finance, Economics and Business, 7(6), 221-231. <https://doi.org/10.13106/jafeb.2020.vol7.no6.221>.
- Venkatesh, V., Morris, G. M., Davis, B. G., & Davis, D. F. (2003). User Acceptance of Information Technology: Toward A Unified View. MIS Quarterly, 27(3), 425-478.

- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. J. M. q. (2003). User acceptance of information technology: Toward a unified view. 425-478.
- WON, J., Kim, B.-Y. J. T. J. o. A. F., Economics,, & Business. (2020). The effect of consumer motivations on purchase intention of online fashion-sharing platform. 7(6), 197-207.

**NHỮNG YẾU TỐ TÁC ĐỘNG TIÊU CỰC ĐẾN AN NINH
SINH VIÊN TRONG QUÁ TRÌNH CHUYỂN ĐỔI SỐ
FACTORS THAT NEGATIVELY IMPACT STUDENT
SECURITY IN THE DIGITAL TRANSFORMATION PROCESS**

TS. Trần Ngọc Mai

Trường Đại học An ninh nhân dân

Thông tin liên hệ: Tranngocmai3007@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Chuyển đổi số, giáo dục, đào tạo, sinh viên	Chuyển đổi số là một quá trình tất yếu trong giai đoạn hiện nay, diễn ra trên tất cả các lĩnh vực và tác động rất lớn đến đời sống xã hội. Một trong những lĩnh vực đang đẩy mạnh chuyển đổi số là giáo dục, đào tạo và sinh viên chính là lực lượng chịu sự ảnh hưởng lớn nhất của quá trình này, cả tích cực và tiêu cực. Trong phạm vi bài viết, tác giả chỉ ra một số yếu tố tác động tiêu cực đến an ninh sinh viên trong bối cảnh chuyển đổi số hiện nay và những vấn đề đặt ra đối với công tác bảo đảm an ninh sinh viên trong thời gian tới.
<i>Keywords:</i> digital transformation, education, the student	ABSTRACT Digital transformation is inevitable in nowadays eras, it happens in every fields of life and has huge impact on social life. Among these fields, education is currently pushing digital transformation and in the process, the student is the most affected, both positively and negatively. Within the context of this article, the author only shows some elements that have negative impact on the safety of students during digital transformation and some problems arise in protecting the safety of the student during the upcoming time.

1. Giới thiệu

Hiện nay, chuyển đổi số là một xu thế tất yếu, diễn ra trên phạm vi toàn cầu, đây là quá trình “không thể đảo ngược”, tạo ra nhiều thời cơ, thách thức cho mỗi quốc gia. Ngày 03/10/2020, Thủ tướng Chính phủ đã ký ban hành Quyết định số 749/QĐ-TTg về Phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”, điều đó cho thấy Việt Nam đang rất quan tâm đến vấn đề chuyển đổi số, đẩy mạnh ứng dụng công nghệ thông tin để nâng cao hiệu lực, hiệu quả quản lý nhà nước, phát triển kinh tế xã hội.

Giáo dục, đào tạo là một trong những lĩnh vực đang đẩy mạnh chuyển đổi số và sinh viên chính là lực lượng chịu sự ảnh hưởng lớn nhất của quá trình này, cả tích cực và tiêu cực. Dưới góc độ an ninh quốc gia và trật tự an toàn xã hội, những yếu tố tiêu cực tác động đến sinh viên tiềm ẩn nhiều vấn đề phức tạp liên quan đến xã hội, an ninh, trật tự, thậm chí là tội phạm. Vì lý do đó, chủ đề nghiên cứu của bài viết có tính cấp thiết cao. Trong phạm vi bài viết, tác giả chỉ ra một số yếu tố tác động tiêu cực đến an ninh sinh viên trong bối cảnh chuyển đổi số hiện nay và những vấn đề đặt ra đối với công tác bảo đảm an ninh sinh viên trong thời gian tới.

2. Cơ sở lý thuyết

Bài viết được nghiên cứu dựa trên lý thuyết của ngành khoa học an ninh và trật tự xã hội, trong đó vận dụng những lý luận cơ bản như: Lý luận quản lý nhà nước về an ninh quốc gia, trật tự an toàn xã hội; Lý luận bảo vệ an ninh chính trị nội bộ, Lý luận bảo vệ an ninh văn hóa, tư tưởng... Ngoài ra, bài viết còn vận dụng lý thuyết xã hội học như lý thuyết mâu thuẫn xã hội của C.Mác và Ph.Ăngghen.

3. Phương pháp nghiên cứu

Bài viết được nghiên cứu trên cơ sở phương pháp luận của chủ nghĩa Mác – Lênin, tư tưởng Hồ Chí Minh; quan điểm chỉ đạo của Đảng, Nhà nước, ngành Công an về bảo vệ an ninh quốc gia và giữ gìn trật tự, an toàn xã hội. Trên cơ sở phương pháp luận đã nêu, tác giả sử dụng một số phương pháp cụ thể sau:

- *Phương pháp nghiên cứu tài liệu*: Được sử dụng để nghiên cứu các báo cáo, công trình nghiên cứu, tài liệu có liên quan đến bài viết. Qua nghiên cứu những tài liệu này, tác giả có thêm thông tin về tình hình nghiên cứu, đồng thời kế thừa, phát triển những nội dung về an ninh sinh viên trong thời kỳ chuyển đổi số và những yếu tố tác động tiêu cực đến an ninh sinh viên.

- *Phương pháp phân tích, tổng hợp*: Được sử dụng để phân tích, tổng hợp thông tin và tài liệu liên quan đến an ninh sinh viên và quá trình chuyển đổi số; hệ thống hóa các thông tin, tài liệu này và tiến hành phân tích, rút ra những vấn đề có tính điển hình về an ninh sinh viên trong thời kỳ chuyển đổi số.

- *Phương pháp thống kê, so sánh*: Được sử dụng để thống kê tình hình của sinh viên có liên quan đến an ninh, trật tự; hệ thống hóa, thống kê số liệu thực tiễn.

- *Phương pháp nghiên cứu điển hình*: Được sử dụng để khảo sát thông tin, số liệu, vụ việc có tính chất điển hình về các yếu tố tác động tiêu cực đến an ninh sinh viên trên một địa bàn (Thành phố Hồ Chí Minh), một trường đại học cụ thể. Từ những thông tin, số liệu, vụ việc có tính chất điển hình này, tác giả đánh giá, rút ra những kết luận khoa học cho bài viết.

- *Phương pháp chuyên gia*: Được sử dụng để phỏng vấn trao đổi quan điểm, kinh nghiệm của nhà khoa học có nghiên cứu về an ninh sinh viên, cán bộ thực tiễn (đang

công tác trên lĩnh vực liên quan đến bảo vệ an ninh trên lĩnh vực giáo dục, đào tạo, trong đó có an ninh sinh viên).

4. Kết quả nghiên cứu

Quá trình chuyển đổi số diễn ra trên tất cả các ngành nghề và lĩnh vực, trong đó một số lĩnh vực được đặt trọng tâm, ưu tiên chuyển đổi số là: Y tế, giáo dục, tài chính, ngân hàng, nông nghiệp, giao thông vận tải và logistics, năng lượng, tài nguyên và môi trường, sản xuất công nghiệp. Như vậy, giáo dục là một trong 08 lĩnh vực được xác định là trọng tâm của Chương trình Chuyển đổi số quốc gia. Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 đã chỉ rõ những nội dung cụ thể của chuyển đổi số trên lĩnh vực giáo dục, đào tạo là: *“Phát triển nền tảng hỗ trợ dạy và học từ xa, ứng dụng triệt để công nghệ số trong công tác quản lý, giảng dạy và học tập; số hóa tài liệu, giáo trình; xây dựng nền tảng chia sẻ tài nguyên giảng dạy và học tập theo cả hình thức trực tiếp và trực tuyến. Phát triển công nghệ phục vụ giáo dục, hướng tới đào tạo cá thể hóa”* [1]. Như vậy, chuyển đổi số trong giáo dục, đào tạo theo cách hiểu đơn giản nhất đó là *“việc ứng dụng những công nghệ tiên tiến giúp nâng cao trải nghiệm của người học; cải thiện những phương pháp giảng dạy cũng như tạo môi trường để học tập thuận tiện nhất”* [2].

Quá trình chuyển đổi số này có tác động rất lớn đến những người làm công tác quản lý giáo dục, giáo viên và người học, có yếu tố tích cực nhưng cũng có nhiều vấn đề thuộc về khó khăn, hạn chế. Một trong những đối tượng chịu nhiều tác động nhất của quá trình chuyển đổi số này chính là sinh viên, lực lượng quan trọng của quá trình xây dựng, phát triển đất nước. Chỉ tính riêng địa bàn Thành phố Hồ Chí Minh, hiện nay có 52 trường đại học với 453.251 sinh viên và 547 cơ sở giáo dục nghề nghiệp với 400.690 người học⁸, đây là một con số rất lớn (khẳng định vai trò là một trong những trung tâm giáo dục, đào tạo uy tín bậc nhất cả nước) và là nguồn lực quan trọng để xây dựng, phát triển xã hội.

Với những địa bàn có đông sinh viên như Hà Nội, Thành phố Hồ Chí Minh, Đà Nẵng, Cần Thơ... vấn đề bảo đảm an ninh đối với lực lượng này là một vấn đề có ý nghĩa quan trọng. Số lượng sinh viên đông dẫn đến thành phần đa dạng, nơi cư trú phân tán... Và ở độ tuổi sinh viên, hầu hết còn những hạn chế nhất định về kinh nghiệm sống, vừa dễ tiếp thu cái mới nhưng cũng dễ bị tác động, lôi kéo... Do đó, trong thời gian qua, một số vụ việc phức tạp trong sinh viên đã xảy ra, tác động xấu đến tình hình an ninh,

⁸ Trong đó có khoảng 87% sinh viên là người ngoại tỉnh; trong khi đó chỉ có 38 trường có ký túc xá dành cho sinh viên nội trú với tổng sức chứa 79.000 sinh viên; số sinh viên còn lại tạm trú trong các nhà trọ, trong khu vực dân cư. Thành phần dân tộc của sinh viên rất đa dạng: số lượng sinh viên dân tộc thiểu số có 5.692 sinh viên, quốc tịch Lào và Campuchia: 945 sinh viên; Số lượng sinh viên theo tôn giáo tương đối đồng, nhất là Phật giáo và Công giáo. Số lượng sinh viên là Đảng viên có 2.566 người; số lượng sinh viên tham gia tổ chức hội sinh viên Việt Nam là 407.559 người.

trật tự của địa phương như: Tình trạng sinh viên bị các đối tượng xấu dụ dỗ, kích động tham gia hoạt động biểu tình; bị lôi kéo tham gia các tổ chức phản động; tham gia hoạt động tôn giáo trái pháp luật; vi phạm pháp luật về trật tự xã hội (đánh nhau, cho vay nặng lãi, đánh bạc, gian lận trong học tập thi cử hoặc các tệ nạn xã hội khác...).

Những vấn đề phức tạp trong an ninh sinh viên kể trên xuất phát từ nhiều nguyên nhân khác nhau và tồn tại trong các giai đoạn của sự phát triển xã hội, trong quá trình chuyển đổi số như hiện nay cũng không phải là ngoại lệ. Chuyển đổi số mang đến nhiều thuận lợi nhưng tiềm ẩn các nguy cơ, các yếu tố tác động tiêu cực đến sự an toàn, sự phát triển tích cực của lực lượng được xem là tương lai của đất nước. Một số yếu tố tác động tiêu cực đến tình hình an ninh sinh viên trong giai đoạn chuyển đổi số hiện nay có thể kể đến như sau:

Một là, hoạt động của các thế lực thù địch và những đối tượng xấu.

Các thế lực thù địch triệt để lợi dụng công nghệ thông tin để tuyên truyền phá hoại tư tưởng, nhất là thông qua mạng internet. Đẩy mạnh chuyển đổi số làm gia tăng thời gian sinh viên sử dụng các thiết bị công nghệ và ở trên môi trường mạng. Nếu không có sự “tỉnh táo” và khả năng chọn lọc, những thông tin xấu, độc sẽ dần thâm thấu, làm cho sinh viên nghe và tin theo luận điệu xuyên tạc của các đối tượng này. Biểu hiện thường thấy là tham gia các hội, nhóm trên mạng xã hội, có những bình luận tiêu cực, thậm chí là các hoạt động xuống đường biểu tình, gây rối an ninh, trật tự khi bị kích động.

Ngoài ra còn có tình trạng sinh viên bị các đối tượng xấu dụ dỗ, dẫn đến bỏ học để tham gia các lớp dạy làm giàu hoặc bán hàng đa cấp, có trường hợp còn gây sức ép để gia đình chuyển tiền cho sinh viên, dùng những suất học bổng không có thật để lừa tiền của gia đình⁹. Những sinh viên nhẹ dạ, thiếu hiểu biết đã trở thành con mồi của đối tượng xấu, việc học hành bị gián đoạn, tiêu tốn tiền bạc của bản thân và gia đình. Tình trạng sinh viên tham gia đánh bạc online cũng diễn ra, các trang web đánh bạc trực tuyến với nhiều chiêu trò đã thu hút sự chú ý và kích thích “máu ăn thua” của một bộ phận giới trẻ. Đây là những vấn đề đáng báo động, tiềm ẩn nguy cơ về tội phạm, bởi khi vỡ nợ, họ sẽ dễ dàng bị lôi kéo vào những hoạt động vi phạm pháp luật.

Hai là, vấn đề an toàn thông tin

Chuyển đổi số làm gia tăng lượng thông tin được cung cấp, chia sẻ, truyền tải và lưu trữ trên không gian mạng, trong những thông tin này có nhiều thông tin cá nhân của

⁹ Báo Pháp luật ngày 13/6/2020 (Cảnh báo tình trạng sinh viên bị dụ “làm giàu” bỏ học): Trường Đại học Sư phạm kỹ thuật Thành phố Hồ Chí Minh có một trường hợp Sinh viên khóa 19 của trường mất liên lạc với gia đình nhiều ngày. Sinh viên này từng về nhà và báo trúng tuyển “học bổng du học Canada” nên muốn xin gia đình hơn 400 triệu đồng để làm hồ sơ đi học. Tuy nhiên, phía nhà trường cho biết trường không có thông tin về chương trình du học này.

sinh viên, giáo viên... Đây là một nguồn tài nguyên có giá trị với hacker và các đối tượng xấu nhằm sử dụng vào nhiều mục đích khác nhau (thường là lừa đảo, sử dụng thông tin về nhân thân để vay tiền...). Với tình trạng các cuộc tấn công mạng diễn ra nhiều như hiện nay¹⁰, trong đó sử dụng thông tin để lừa đảo chiếm 1/3 số cuộc tấn công mạng, thì việc bảo vệ thông tin cá nhân của sinh viên, dữ liệu phục vụ quản lý của các nhà trường là việc vô cùng quan trọng. Tuy nhiên, trình độ công nghệ thông tin hạn chế và ý thức cũng như nhận thức về vấn đề bảo mật chưa cao làm gia tăng nguy cơ lộ thông tin, đây là một trong những yếu tố tác động phức tạp đến tình hình an ninh sinh viên trong giai đoạn hiện nay.

Ba là, những nguy cơ trong quá trình hợp tác quốc tế

Trong giai đoạn hiện nay, việc giao lưu, hợp tác quốc tế để phát triển là một xu thế tất yếu và giáo dục đào tạo đang là lĩnh vực được quan tâm rất lớn. Quá trình chuyển đổi số lại càng đặt ra nhu cầu hội nhập quốc tế mạnh mẽ nhằm học tập kinh nghiệm của các nước tiên tiến, rút ngắn con đường chuyển đổi số, hiện đại hóa ở nước ta. Hiện nay, các trường đại học, viện nghiên cứu trong nước đang hợp tác về nhiều mặt với các trường đại học lớn, có uy tín ở nước ngoài trong việc tài trợ học bổng, liên kết đào tạo, nghiên cứu¹¹... nhưng đây cũng là điều kiện thuận lợi để các thế lực thù địch, phản động, phản tử xấu lợi dụng hoạt động hợp tác quốc tế tác động vào sinh viên. Những đối tượng này lợi dụng sự phát triển của internet với nhiều thông tin xấu, độc, bịa đặt trên mạng xã hội chưa được kiểm soát chặt chẽ gây ảnh hưởng rất lớn đến tư duy và nhận thức của sinh viên. Nhận thức lệch lạc là tiền đề cơ bản để kẻ xấu lợi dụng, kích động gây mất an ninh, trật tự trong các trường học và ngoài xã hội. Một số sinh viên sau khi đã học tập ở nước ngoài không muốn quay về nước, đây cũng là vấn đề quan trọng, là sự chảy máu chất xám, ảnh hưởng không tốt đến việc phát triển nguồn nhân lực xây dựng đất nước.

Bốn là, những thành tựu của khoa học và công nghệ ảnh hưởng đến cơ hội về việc làm

Sự bùng nổ của cuộc cách mạng công nghiệp lần thứ 4 và quá trình chuyển đổi số đã làm thay đổi rất nhiều mặt của đời sống xã hội. Một trong số đó là việc sử dụng AI (trí tuệ nhân tạo), máy móc để thay thế sức lao động của con người, điều này làm cho cơ hội về việc làm của sinh viên sau khi ra trường bị thu hẹp lại. Theo kết quả nghiên cứu “Công nghệ và tương lai việc làm tại khu vực ASEAN”¹² dự đoán việc sử dụng trí

¹⁰ Theo thống kê của Bộ Thông tin và truyền thông, năm 2020 có 6.829 cuộc tấn công mạng, gây sự cố vào các hệ thống thông tin, trong đó có 2.349 cuộc tấn công lừa đảo, 2.234 cuộc tấn công lây nhiễm mã độc.

¹¹ Tính riêng quan hệ hợp tác trong giáo dục giữa Việt Nam và Hoa Kỳ thì Hiện có khoảng 50 trên tổng số hơn 400 chương trình liên kết đào tạo đang hoạt động giữa cơ sở giáo dục đại học, trong đó chủ yếu là bậc đại học và thạc sĩ (Theo Thông tấn xã Việt Nam).

¹² Nghiên cứu do Cisco tiến hành với sự hợp tác của Oxford Economics.

tuệ nhân tạo trong phần mềm, phần cứng cũng như robots “*sẽ làm thay đổi quan trọng bối cảnh việc làm tại sáu nền kinh tế lớn nhất ASEAN vào năm 2028*” [3].

Gần đây có hiện tượng nhiều sinh viên mới ra trường không tìm được việc làm theo chuyên ngành của mình nên đã mưu sinh bằng các nghề khác như giao hàng, chạy xe công nghệ... Theo dự báo, *có khoảng 86% lao động trong các ngành dệt may và giày dép ở Việt Nam có nguy cơ cao mất việc làm dưới tác động của cuộc Cách mạng công nghiệp lần thứ tư* [4]. Sau dịch covid-19, tình hình việc làm lại càng trở nên khó khăn hơn khi nhiều doanh nghiệp tiến hành sa thải nhân viên, nền kinh tế mặc dù có nhiều chuyển biến tích cực nhưng vẫn còn gặp nhiều khó khăn. Vấn đề thiếu việc làm gây ra nhiều hệ lụy tiêu cực cho xã hội, là mầm mống nảy sinh các tệ nạn xã hội nguy hiểm.

Năm là, nguy cơ tụt hậu

Đây là nguy cơ không chỉ trong lĩnh vực giáo dục, đào tạo mà nó tiềm ẩn và thậm chí hiện hữu ở các lĩnh vực khác. Chuyển đổi số sẽ rút ngắn con đường phát triển, tuy nhiên với tốc độ nhanh chóng như hiện nay, không phải bất cứ quốc gia, địa phương hay cá nhân nào cũng có thể tận dụng tốt những mặt thuận lợi và trang bị đủ điều kiện để tham gia có hiệu quả vào quá trình này. Đối với từng sinh viên, tùy môi trường, điều kiện và khả năng học tập mà mỗi sinh viên sẽ có mức độ tham gia hoặc bị tác động dưới quá trình chuyển đổi số khác nhau. Do đó, việc có một bộ phận sinh viên bị “đuối sức” hoặc tụt lại phía sau trong dòng chảy mạnh mẽ của khoa học công nghệ là điều không thể tránh khỏi. Các trường đại học ở tốp đầu hoặc sinh viên ở những thành phố lớn luôn có thể mạnh để tiếp cận, tham gia và thụ hưởng những thành quả của quá trình chuyển đổi số (thể mạnh đó là điều kiện về cơ sở vật chất, kỹ thuật, trình độ ngoại ngữ, tin học, quan hệ hợp tác quốc tế, tài chính...), và đây cũng là “*một nguyên nhân dẫn đến sự bất bình đẳng về cơ hội học tập, tiếp cận kiến thức giữa học sinh sinh viên ở các vùng miền, các nhà trường*” [5].

5. Kết luận và gợi ý

Từ những yếu tố tiêu cực tác động đến an ninh sinh viên trong quá trình chuyển đổi số như trên, công tác đảm bảo an ninh sinh viên cần chú ý đến một số vấn đề sau:

Một là, các đơn vị có liên quan cần bám sát và thực hiện tốt mục tiêu, yêu cầu và các chỉ tiêu cụ thể của Chương trình chuyển đổi số quốc gia. Bộ Giáo dục và Đào tạo đang khẩn trương thực hiện Đề án “Tăng cường ứng dụng công nghệ thông tin và chuyển đổi số giáo dục, đào tạo giai đoạn 2022 - 2025, định hướng đến năm 2030” theo Quyết định số 131/QĐ-TTg ngày 25/01/2022 của Thủ tướng Chính phủ, đây là một trong những nội dung cơ bản, quan trọng, phục vụ quá trình chuyển đổi số trong lĩnh vực giáo dục, đào tạo. Bám sát những tiêu chí, định hướng này sẽ tạo điều kiện thuận lợi cho quá trình học tập của sinh viên, góp phần tạo ra những sản phẩm có chất lượng cho xã hội. Theo Chương trình chuyển đổi số quốc gia, “*100% các cơ sở giáo dục sẽ triển khai*

công tác dạy và học từ xa, trong đó thử nghiệm chương trình đào tạo cho phép sinh viên học trực tuyến tối thiểu 20% nội dung chương trình” [1]. Ngoài ra, công tác quản lý giáo dục cũng cần đẩy mạnh, thậm chí là đi đầu trong chuyển đổi số để tạo ra một môi trường thuận lợi cho sinh viên học tập, nghiên cứu. Kích thích, khơi dậy đam mê học tập, nghiên cứu và cống hiến của sinh viên là một trong những yếu tố quan trọng để phòng ngừa, hạn chế những vấn đề phức tạp nảy sinh trong sinh viên.

Hai là, đẩy mạnh công tác nắm tình hình, nhất là tư tưởng chính trị của sinh viên, kịp thời phát hiện những hoạt động của các thế lực thù địch, tội phạm lợi dụng quá trình chuyển đổi số tác động xấu đến sinh viên. Đây là vấn đề mà nhà trường và các cơ quan chức năng cần đặc biệt quan tâm, bởi tác động của hành vi phá hoại tư tưởng thường trải qua một quá trình, diễn ra từ từ và rất khó phát hiện. Sinh viên là một lực lượng đang ở độ tuổi nhạy cảm, chưa thật sự có bản lĩnh và khả năng đề kháng trước những thông tin xấu độc. Do đó, thông qua các công tác chính trị, đoàn thể, phong trào sinh viên, nhà trường có thể nắm được tâm tư, tình cảm, nguyện vọng cũng như xu hướng phát triển của sinh viên để có kế hoạch bồi dưỡng, phát triển hoặc điều chỉnh nếu đó là những tư tưởng tiêu cực. Một vấn đề cần chú ý là cần tiến hành nắm tình hình tư tưởng của sinh viên trên không gian mạng, những hội nhóm mà sinh viên tham gia, kịp thời phát hiện những vấn đề liên quan đến an ninh, trật tự. Hiện nay mạng xã hội đang có ảnh hưởng rất lớn đối với đời sống xã hội, cả tích cực lẫn tiêu cực và sinh viên cũng không nằm ngoài sự tác động đó.

Ba là, quan tâm đến vấn đề bảo mật, phòng chống tấn công mạng, đây là trách nhiệm của các cơ quan chức năng, của nhà trường và cả sinh viên. Nếu mỗi người đều ý thức được việc bảo vệ thông tin cá nhân của mình thì sẽ góp phần hạn chế nguy cơ lộ thông tin, không kẻ xấu lợi dụng vào những hoạt động vi phạm pháp luật. Cùng với đó, nhà trường và các cơ quan chức năng cần đầu tư trang thiết bị, kỹ thuật và cả nhân lực để đảm bảo an toàn hệ thống thông tin, dữ liệu, hệ thống lưu trữ... Các cuộc tấn công mạng để lấy cắp thông tin ngày càng diễn ra tinh vi và phức tạp hơn, nhắm đến mọi cơ quan, tổ chức, do đó tất cả các đơn vị và nhà trường trước hết cần nâng cao nhận thức về vấn đề này, tiếp đến là kỹ năng bảo vệ an ninh mạng, đây thật sự là một thách thức trong quá trình chuyển đổi số.

Bốn là, trang bị thêm kiến thức, kỹ năng cho sinh viên để có thể đề kháng trước những tác động tiêu cực, tận dụng tốt những mặt tích cực từ đó nâng cao kết quả học tập và cơ hội việc làm. Trong bối cảnh khoa học và công nghệ phát triển như vũ bão, việc học không còn “như đi trên dòng nước ngược, không tiến ắt sẽ lùi” nữa, mà sẽ đối diện với nguy cơ tụt hậu. Sản phẩm của quá trình chuyển đổi số trong giáo dục, đào tạo phải là con người có trình độ về khoa học công nghệ, có kỹ năng, khả năng ứng dụng công nghệ thông tin phục vụ công việc, nghiên cứu, tạo ra những giá trị tốt đẹp cho xã hội.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Giờ đây, sinh viên phải chấp nhận một sự thật rằng, sự cạnh tranh cho vị trí việc làm không đơn thuần là giữa người với người nữa, mà còn là cuộc cạnh tranh của con người và trí tuệ nhân tạo, robot. Do đó, ngoài động lực của mỗi sinh viên, nhà trường cần trang bị thêm kiến thức ở trình độ cao, bắt kịp với sự phát triển của xã hội, cùng với đó là hỗ trợ khả năng có được việc làm sau quá trình học tập ở ghế nhà trường.

Trên đây là một số vấn đề đặt ra đối với công tác bảo đảm an ninh sinh viên, góp phần hạn chế những tác động tiêu cực từ quá trình chuyển đổi số đang diễn ra mạnh mẽ hiện nay. Bài viết rất mong nhận được sự trao đổi của quý đại biểu, các nhà khoa học tham gia hội thảo “An ninh sinh viên trong thời kỳ chuyển đổi số” do Thành đoàn Thành phố Hồ Chí Minh và Trường Đại học An ninh nhân dân đồng tổ chức. Xin trân trọng cảm ơn./.

T.N.M

Tài liệu tham khảo:

1. Chính phủ (2020), Quyết định số 749/QĐ-TTg về Phê duyệt “Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030”, ngày 03/10/2020 của Thủ tướng Chính phủ, Hà Nội.
2. Bùi Thị Huệ, Bùi Đức Thịnh, Vũ Thị Tuyết Lan (2022), Chuyển đổi số trong giáo dục và đào tạo: Thực trạng và Giải pháp, *Tạp chí Khoa học & Công nghệ online*, Bộ Khoa học và Công nghệ. *Link: [Chuyển đổi số trong giáo dục và đào tạo: Thực trạng và Giải pháp \(vjst.vn\)](#)*.
3. Chu Văn Vệ (2019), Chuyển đổi Số: Bối cảnh và thách thức, *Tạp chí Ngân hàng*, số tháng 4/2019, Hà Nội.
4. Nguyễn Tuấn Anh (2022), [Tác động của cuộc Cách mạng công nghiệp lần thứ tư đến thế giới, khu vực và Việt Nam](#), *tapchicongsan.org.vn*, 29/8/2022.
5. Tô Hồng Nam (2020), Chuyển đổi số trong lĩnh vực giáo dục và đào tạo: Thực trạng và giải pháp, *Tạp chí Thông tin và Truyền thông* số tháng 4/2020, Bộ Thông tin và Truyền thông.

**TÁC ĐỘNG TIÊU CỰC CỦA CHATGPT ĐẾN AN NINH
THÔNG TIN CỦA SINH VIÊN TRƯỜNG ĐẠI HỌC
KINH TẾ QUỐC DÂN**

**THE NEGATIVE IMPACTS OF CHATGPT TOWARDS
INFORMATION SECURITY AMONG STUDENTS AT
NATIONAL ECONOMICS UNIVERSITY**

Lê Thị Phương Linh¹, Lê Nguyễn Phương Chi¹, Mai Khánh Linh²,

Lê Ngọc Thái Hà³, Nguyễn Huyền Nhi³

¹Trường Đại học Kinh tế Quốc dân; ²Học viện Tài chính;

³Trường Đại học Ngoại ngữ, ĐHQG-HN

Thông tin liên hệ: 20le.phuong.linh@gmail.com

THÔNG TIN	TÓM TẮT
Từ khóa: <i>ChatGPT, an ninh sinh viên, mua bán thông tin, tintương ứng với câu hỏi và yêu cầu của người dùng) đến an giả, bản quyền.</i>	Nghiên cứu tập trung vào những tác động tiêu cực của ChatGPT (một chương trình chatbot AI được tạo ra nhằm cung cấp những câu trả lời sử dụng ngôn ngữ tự nhiên) đến an ninh thông tin cho sinh viên. Cụ thể, dựa trên kết quả khảo sát về mức độ, quy mô ảnh hưởng của chương trình này đối với sinh viên Trường Đại học Kinh Tế Quốc dân, bản tham luận sẽ đưa ra những phân tích về ba nguy cơ tiềm ẩn chính về an ninh thông tin khi sinh viên sử dụng ChatGPT trong môi trường Đại học là mua bán thông tin, vấn đề bản quyền và truyền bá thông tin sai lệch. Chúng tôi cũng nhấn mạnh rằng những thách thức này được đặt ra bởi ChatGPT có thể được kiểm soát bằng các giải pháp bảo mật và một số điều chỉnh trong quy định trường học thông qua khuyến nghị, và gợi ý.
Keywords: <i>ChatGPT, student security, information trading, fake news, copyright.</i>	ABSTRACT ChatGPT is an AI chatbot programmed to provide natural language responses to users' questions and prompts. This paper focuses on the negative impacts of ChatGPT to the information security of university students. Specifically, based on the survey results about the scale of these effects on students at National Economics University, we provide analysis on three main potential risks of

information security when students utilize ChatGPT for work at schools, namely information trading, copyright issues and spread of fake news. We also emphasize that these challenges posed by ChatGPT can be managed by security measures and adjustments to school regulations as in our Conclusion and suggestion.

1. Giới thiệu:

Trong những thập kỷ qua, với bối cảnh Cách mạng Công nghiệp 4.0 đang diễn ra trên toàn cầu, con người cũng như xã hội luôn không ngừng vận động và phát triển với những bước nhảy vọt về mọi mặt để bắt kịp với thời đại, điển hình là lĩnh vực công nghệ thông tin (Information Technology – IT) và trí tuệ nhân tạo (Artificial Intelligence – AI). Trí tuệ nhân tạo hiện đang là lĩnh vực nhận được nhiều sự quan tâm từ các lĩnh vực khác, một trong số đó là lĩnh vực giáo dục.

Thời gian gần đây, ChatGPT – một mô hình ngôn ngữ lớn được phát triển bởi OpenAI dựa trên nhiều mô hình trí tuệ nhân tạo với kiến trúc mạng nơ-ron sâu (kiến trúc Transformer¹³) đang thu hút sự quan tâm đông đảo của các nhà nghiên cứu trong lĩnh vực giáo dục. Mô hình này được xem là một công cụ tiềm năng để cải thiện tình trạng học tập qua nhiều nghiên cứu. Tuy nhiên, bên cạnh những lợi ích mà ChatGPT mang lại, mô hình này có thể tồn tại những rủi ro tiềm tàng đối với an ninh mạng.

Hiện nay, đã có một số nghiên cứu về ChatGPT nhưng còn tồn tại khoảng trống nhất định. Đa số nghiên cứu tập trung vào ứng dụng của ChatGPT trong một vài lĩnh vực như giáo dục, y tế,... Tuy nhiên, rất ít công trình tập trung vào tác động tiêu cực của ChatGPT đến an ninh thông tin sinh viên. Một số bài báo viết chỉ dừng lại ở góc độ dịch thuật hoặc nêu quan điểm. Do đó, việc nghiên cứu về tác động tiêu cực của ChatGPT đến an ninh thông tin cũng như phân tích hành vi sử dụng ứng dụng này của sinh viên có ý nghĩa quan trọng và cấp thiết.

Để có thể sử dụng ChatGPT trên quy mô lớn hơn với độ an toàn cao hơn, trước tiên chúng ta cần hiểu thêm về những mối đe dọa tiềm ẩn đến người dùng. Bài viết này sẽ thảo luận về một số tác động tiêu cực đến an ninh thông tin trong việc sử dụng ChatGPT của sinh viên và đưa ra những chính sách, kiến nghị giải pháp đối với vấn đề này.

2. Cơ sở lý thuyết

¹³ Kiến trúc Transformer: một kiến trúc mạng nơ-ron sâu (deep neural network) đặc biệt phát triển cho việc xử lý chuỗi dữ liệu, đặc biệt là trong lĩnh vực xử lý ngôn ngữ tự nhiên (NLP).

2.1. An ninh thông tin, an toàn thông tin

An ninh thông tin: Khoản 13 Điều 3 Quy chế quản lý, cung cấp và sử dụng dịch vụ Internet trong Quân đội nhân dân Việt Nam ban hành kèm theo Thông tư 110/2014/TT-BQP nêu rõ: “An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân”.

An toàn thông tin là bảo vệ thông tin và hệ thống thông tin nói chung khỏi các truy cập trái phép, sử dụng, làm lộ, làm hỏng, chỉnh sửa, ghi chép không được phép.... Khái niệm an toàn thông tin mạng, an toàn máy tính, đảm bảo thông tin được sử dụng hoán đổi cho nhau. Những lĩnh vực này liên quan nội bộ với nhau, thường xuyên chia sẻ những mục đích chính của việc bảo vệ các khía cạnh tính bí mật, toàn vẹn và tính sẵn sàng của thông tin nói chung. An toàn thông tin bao hàm một lĩnh vực rộng lớn các hoạt động gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin và dữ liệu. Mục đích là đảm bảo một môi trường thông tin tin cậy, an toàn và trong sạch cho mọi thành viên và tổ chức trong xã hội. Nếu không có biện pháp đảm bảo an toàn thông tin, tổ chức, doanh nghiệp rất dễ trở thành nạn nhân của các vụ tấn công.

2.2. ChatGPT

Theo OpenAI (2023), ChatGPT là giao diện trí tuệ nhân tạo đàm thoại sử dụng ngôn ngữ tự nhiên tương tác một cách thực tế và thậm chí trả lời các câu hỏi liên tiếp của người sử dụng. ChatGPT có khả năng duy trì phong cách trò chuyện với tính cách hoặc danh tính nhất quán trong suốt cuộc trò chuyện (Junaid Qadir, 2023). ChatGPT được đào tạo dựa trên nguồn dữ liệu khổng lồ từ sách, website, mạng xã hội, các đoạn hội thoại với người dùng,... tạo ra được nội dung đa dạng và phản hồi giống con người (Ahmed Tlili et al., 2023). Thu hút được hàng triệu người dùng có thể cung cấp cho ChatGPT thêm nguồn dữ liệu ngày một lớn. Nghiên cứu của Tiffany H. Kung (2023), ChatGPT là một mô hình ngôn ngữ lớn với thuật toán AI mới được đào tạo để dự đoán khả năng xảy ra của chuỗi từ nhất định trong ngữ cảnh của những từ đứng trước. So sánh với những chatbot truyền thống, ChatGPT dựa trên GPT-3 – phiên bản thứ ba của dòng GPT bởi OpenAI – có sự tân tiến hơn về quy mô, gồm 175 tỷ tham số, tăng thêm 1,5 tỷ so với GPT-2 (Tom B. Brown et al., 2020).

ChatGPT là công cụ đang được sử dụng rộng rãi trên toàn thế giới với nhiều tính năng vượt trội. OpenAI (2023) cho biết ChatGPT đã mở rộng tại 40 quốc gia và vùng lãnh thổ, nhưng chưa xuất hiện chính thức Việt Nam. Theo nghiên cứu của Tiffany H. Kung và cộng sự (2023), độ chính xác của ChatGPT là khoảng 60% và nó vẫn tồn tại nhiều sai lệch. Một số quốc gia như Hoa Kỳ hiện vẫn chưa có đề xuất quy định chính thức về giám sát AI. Bên cạnh đó, các quốc gia như Anh sẽ phác thảo một số quy định

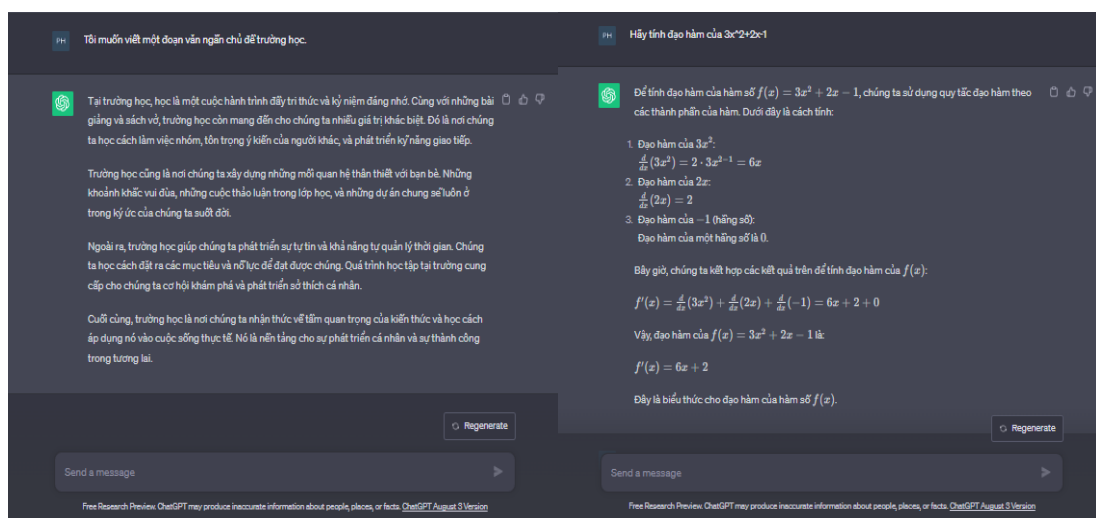
đảm bảo sử dụng các sản phẩm AI khi nhận thấy sự rủi ro tiềm ẩn khi sử dụng AI nói chung và ChatGPT nói riêng. Tuy nhiên, một số quốc gia hạn chế nghiêm trọng sử dụng AI, đặc biệt ở các lĩnh vực như giáo dục, hệ thống tư pháp, thi hành pháp luật hay trong các cơ sở hạ tầng quan trọng và những quốc gia như Trung Quốc hay Triều Tiên thì ChatGPT bị cấm một cách chính thức.

Nhiều nghiên cứu cho rằng, ChatGPT vẫn có thể xâm phạm quyền riêng tư và thông tin cá nhân người dùng giống các công nghệ khác. Ahmed Tlili và các cộng sự (2023) chỉ ra sau khi kiểm tra, người ta phát hiện các cuộc hội thoại được lưu trữ, xem xét và sử dụng để cải tiến hệ thống nhưng khi hỏi Chat GPT thì nó phủ nhận hoàn toàn về việc này. Bên cạnh đó, chính sách riêng tư của Open AI cũng viết rằng họ có thể sẽ tự thu thập thông tin và xác định danh tính của người dùng. Vì thế, vấn đề được quan tâm nhất lúc này đó chính là quyền riêng tư. Vấn đề này nhận được phản ứng vô cùng kịch liệt của các lập trình viên, các nhà làm luật,...

Nếu tạo tài khoản ChatGPT ở Việt Nam sẽ gặp nhiều khó khăn vì chatbot này bắt buộc phải có số điện thoại nước ngoài để nhận tin nhắn chứa mã kích hoạt. Lúc này, bạn sử dụng extension Proxy ¹⁴của Chrome hay các ứng dụng đổi VPN để giả mạo IP sang UK, US. Hiện tại đang trong giai đoạn thử nghiệm nên Chat GPT miễn phí cho người dùng phiên bản GPT-3.5 và mất phí \$20/1 tháng với phiên bản GPT-4. Dữ liệu phiên bản GPT-3.5 được cập nhật cho đến năm 2021, tuy không đầy đủ nhưng có thể đáp ứng các nhu cầu cơ bản nhất của người sử dụng nên theo thống kê, đã có trên 100 triệu người dùng trên toàn thế giới và hơn 10 triệu người dùng ở Việt Nam. Ở Việt Nam, có rất nhiều cá nhân sử dụng điểm này để kinh doanh, mua bán tài khoản hoặc nhận làm trung gian mở tài khoản ChatGPT cho người sử dụng.

Về tác động của ChatGPT trong giáo dục, nghiên cứu “Khả năng thực hiện bài kiểm tra định kì môn Toán và môn Ngữ văn cấp Trung học của công cụ ChatGPT” (Lê Anh Vinh, 2023), với đặc trưng của lĩnh vực Giáo dục đã chỉ ra việc ứng dụng ChatGPT hoàn toàn có thể thực hiện cơ bản một đề thi hoàn chỉnh như con người. Nhưng sử dụng công cụ này cần thận trọng, một mặt kế thừa những điểm mạnh để nâng cao chất lượng dạy và học, mặt khác cần nghiên cứu, đưa ra các giải pháp, hành động để phát huy ưu điểm và giảm thiểu các tác động tiêu cực trong giáo dục (nếu có). Chính vì thế, các nghiên cứu thử nghiệm, đánh giá rất cần thiết trong thời điểm này.

¹⁴ Extension Proxy: tiện ích mở rộng



Hình 1. GPT-3.5 thực hiện yêu cầu các môn học phổ thông

Ngày nay, ChatGPT gắn với vấn đề an ninh thông tin đã và đang đi vào mọi ngõ ngách của đời sống xã hội và dần trở thành một bộ phận quan trọng của an ninh quốc gia. Nguy cơ gây mất an ninh thông tin là mối đe dọa lớn và ngày càng gia tăng với mọi đối tượng, đặc biệt là sinh viên trẻ-đối tượng lớn trực tiếp sử dụng phần mềm này trong mọi mặt đời sống. Bài viết tập trung phân tích, làm rõ những tác động của ChatGPT lên đối tượng sinh viên trong điều kiện hiện nay, chỉ rõ những vấn đề đang đặt ra trong bảo đảm an ninh thông tin và đề xuất các giải pháp trọng tâm nhằm nâng cao hiệu quả bảo đảm an ninh thông tin của sinh viên khi sử dụng ChatGPT.

3. Phương pháp nghiên cứu

Đối tượng nghiên cứu: Tác động tiêu cực của Công cụ AI - ChatGPT đến an ninh thông tin của sinh viên Trường Đại học Kinh tế Quốc dân

Khách thể khảo sát: Sinh viên Trường Đại học Kinh tế Quốc dân, Giảng viên Trường Đại học Kinh tế Quốc dân.

Trong quá trình nghiên cứu thực trạng vấn đề, đề tài sử dụng các phương pháp (1) Nghiên cứu lý luận và (2) Nghiên cứu thực tiễn.

3.1. Phương pháp nghiên cứu lý luận

Mục đích của nghiên cứu khi sử dụng phương pháp nghiên cứu lý luận là xây dựng đề cương nghiên cứu, xác định cơ sở lý thuyết của vấn đề nghiên cứu. Qua quá trình nghiên cứu lý luận, các công trình nghiên cứu về Tác động tiêu cực của Công cụ AI – ChatGPT đến an ninh thông tin trong môi trường học đường được hệ thống hoá. Ngoài ra, từ nghiên cứu lý luận sẽ xác định được cơ sở lý luận của đề tài bao gồm các khái niệm cơ bản; những vấn đề liên quan. Thu thập, phân tích các nghiên cứu về so sánh xã hội trong học tập thông qua việc khảo cứu các tài liệu: sách, tạp chí, website,... Từ đó tiến hành tổng thuật, phân tích, đánh giá các dữ liệu thu thập được.

3.2. Phương pháp nghiên cứu thực tiễn

Sử dụng phương pháp nghiên cứu thực tiễn nhằm mục đích khảo sát, thu thập số liệu, phân tích thực trạng sử dụng và các yếu tố ảnh hưởng, tác động tiêu cực của Công cụ AI – ChatGPT đến an ninh thông tin trong môi trường học đường. Các phương pháp nghiên cứu thực tiễn bao gồm: Phương pháp điều tra bằng bảng hỏi, Phương pháp Phỏng vấn sâu, Phương pháp chuyên gia, Phương pháp thử nghiệm sử dụng Công cụ ChatGPT. Trong đó Phương pháp điều tra bằng bảng hỏi và Phương pháp Phỏng vấn sâu là các phương pháp chính được sử dụng trong nghiên cứu nhằm khảo sát thực trạng mức độ sử dụng, các yếu tố tác động tiêu cực từ đó đề xuất giải pháp hạn chế tác động tiêu cực của công cụ ChatGPT.

** Cách thức tiến hành của phương pháp nghiên cứu thực tiễn:*

- Phương pháp điều tra bằng bảng hỏi

Nghiên cứu thực hiện từ 20/08/2023 đến 08/09/2023 thông qua phương pháp điều tra bằng bảng hỏi, khách thể là sinh viên tại Trường Đại học Kinh tế Quốc dân, Hà Nội. Nhóm tác giả lựa chọn phương pháp chọn mẫu thuận tiện với số lượng 200 sinh viên Trường Đại học Kinh tế Quốc dân.

Về cơ cấu mẫu khảo sát được thể hiện qua Bảng 1:

Bảng 1: Đặc điểm mẫu khách thể khảo sát sinh viên

Phân loại	Đặc điểm	Học sinh	
		<i>Số lượng</i>	<i>Tỉ lệ (%)</i>
<i>Khối lớp</i>	<i>Sinh viên năm Nhất</i>	50	25
	<i>Sinh viên năm Hai</i>	60	30
	<i>Sinh viên năm Ba</i>	60	30
	<i>Sinh viên năm Tư</i>	30	15
<i>Giới tính</i>	<i>Nam</i>	87	43,5
	<i>Nữ</i>	113	56,5
<i>Học lực</i>	<i>Xuất sắc</i>	42	21
	<i>Giỏi</i>	107	53,5
	<i>Khá</i>	48	24
	<i>Trung bình</i>	3	1,5

(Nguồn: Khảo sát của nhóm tác giả)

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Từ bảng 1 cho thấy, đối với sinh viên, trong tổng số 200 sinh viên thì có 87 sinh viên là nam (43,5%) và 113 nữ (56,5%). Việc lựa chọn khách thể khảo sát giữa học sinh nam và học sinh nữ có sự cân bằng khá tương đối. Theo bảng 1, về khối lớp tham gia khảo sát, có 50 sinh viên năm nhất (25%), 60 sinh viên năm Hai (30%), 60 sinh viên năm Ba (30%), 30 sinh viên năm Tư (15%). Về đặc điểm học lực của đối tượng khảo sát có 42 sinh viên (21%) đạt học lực Xuất sắc, 107 sinh viên (53,5%) đạt học lực Giỏi, 48 sinh viên (24%) đạt học lực Khá và 3 sinh viên (1,5%) đạt học lực Trung bình.

Thiết kế bảng hỏi: Bảng hỏi được thiết kế gồm có 4 phần. Phần thứ nhất là các thông tin cá nhân, nhân khẩu học như: giới tính, lớp, trường,... (đối với sinh viên), trình độ học vấn,... bao gồm các câu hỏi lựa chọn 1 phương án. Phần thứ hai là những câu hỏi về thực trạng và mức sử dụng Công cụ AI – ChatGPT của sinh viên Trường Đại học Kinh tế Quốc dân trong môi trường học đường. Phần thứ ba là những câu hỏi về các biểu hiện và yếu tố tác động, ảnh hưởng tiêu cực của Công cụ AI – ChatGPT đến an ninh thông tin trong môi trường học đường. Phần thứ tư bao gồm các câu hỏi ghi thêm của đối tượng khảo sát là những đề xuất về giải pháp giảm thiểu ảnh hưởng tiêu cực đến an ninh thông tin trong môi trường học đường khi sử dụng Công cụ AI – ChatGPT.

- Phương pháp phỏng vấn sâu

Chúng tôi lựa chọn phỏng vấn 10 Giảng viên và 20 Sinh viên Trường Đại học Kinh tế Quốc dân để khai thác sâu hơn các khía cạnh của nghiên cứu.

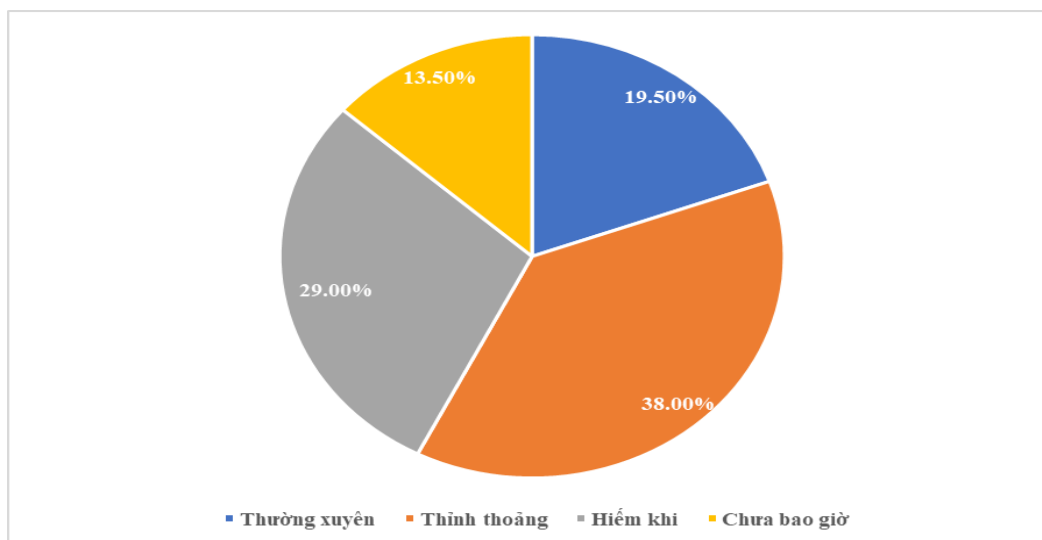
Thiết kế kịch bản phỏng vấn: Kịch bản phỏng vấn gồm 3 phần. Phần thứ nhất người phỏng vấn giới thiệu thông tin cá nhân, nhân khẩu học như: giới tính, lớp, trường,... (đối với sinh viên), trình độ học vấn,... Phần thứ hai là câu hỏi gợi mở về các biểu hiện và yếu tố tác động, ảnh hưởng tiêu cực của Công cụ AI – ChatGPT đến an ninh thông tin trong môi trường học đường. Phần thứ ba là các đề xuất về giải pháp nhằm giảm thiểu ảnh hưởng tiêu cực đến an ninh thông tin trong môi trường học đường khi sử dụng Công cụ AI – ChatGPT.

4. Kết quả nghiên cứu và thảo luận

4.1. Kết quả nghiên cứu

Kết quả khảo sát 200 sinh viên ở trường Đại học Kinh tế Quốc dân, có đến 173 (86,5%) sinh viên đã từng sử dụng công cụ ChatGPT trong học tập, công việc hay đời sống hằng ngày ở các mức độ khác nhau. Mức độ sinh viên thỉnh thoảng sử dụng ChatGPT chiếm tỷ lệ lớn nhất (38%). Bên cạnh đó, có đến 39 sinh viên (19,5%) thường xuyên sử dụng ChatGPT như một công cụ hỗ trợ mọi mặt trong cuộc sống. Qua phỏng vấn, phần lớn sinh viên sử dụng ChatGPT với mục đích học tập và hỗ trợ học tập như tìm kiếm thông tin, kiến thức liên quan đến môn học; tìm kiếm đáp án bài tập; hỗ trợ viết luận văn;... Trong cuộc sống hằng ngày, một vài sinh viên cho biết họ thường lên ChatGPT để đọc thông tin hay tìm kiếm điều mình muốn biết thay vì sử dụng Google

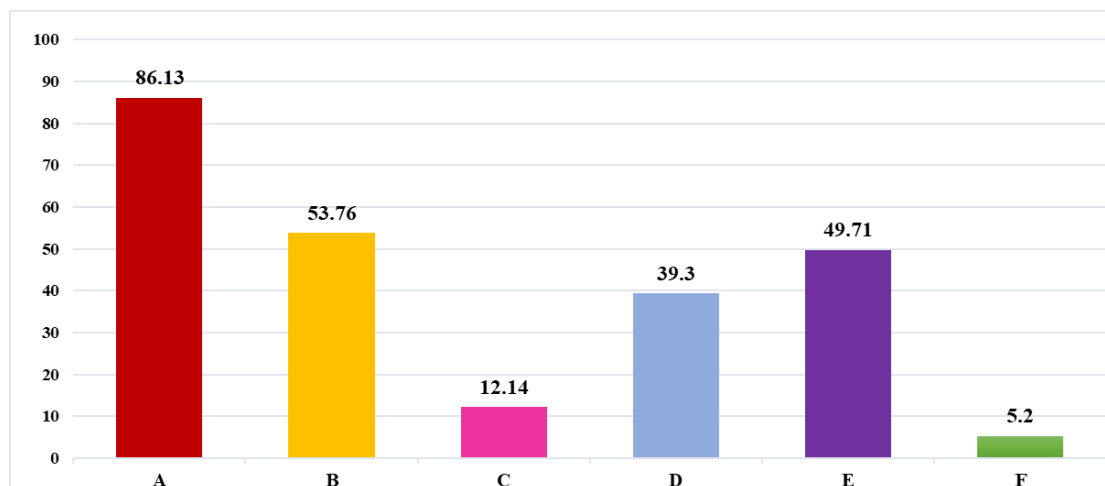
hoặc nghiên cứu trong sách báo như trước đây. Qua đó có thể thấy được sự chi phối của công cụ này lên đối tượng sinh viên là rất lớn, tác động làm thay đổi hành vi, thói quen tìm kiếm và sử dụng thông tin của người dùng (xem Hình 2).



Hình 2: Mức độ sử dụng Chat GPT của sinh viên

Nhằm khảo sát mục đích sử dụng ChatGPT của sinh viên, kết quả thu được sinh viên sử dụng ChatGPT với mục đích xem đề xuất ý tưởng, gợi ý hoặc hướng giải quyết cho một vấn đề bất kỳ chiếm tỷ lệ cao nhất (86,13%). Điều này cho thấy sinh viên coi việc sử dụng công cụ này như một điều tất yếu khi gặp bất cứ khúc mắc nào trong cuộc sống. Nếu như điều này diễn ra thường xuyên, liên tục và lâu dài sẽ không tránh khỏi việc sinh viên bị lệ thuộc quá mức vào những đáp án mà ChatGPT gây ra, làm giảm khả năng chủ động giải quyết vấn đề hay khả năng suy nghĩ độc lập, tư duy phản biện,... Ngoài ra, phần lớn sinh viên sử dụng công cụ này nhằm giải đáp thắc mắc trong học tập, công việc và cuộc sống (53,76%) và tra cứu thông tin về bài học, các sự kiện, câu đố, tóm tắt sách,... Hai mục đích này chiếm tỷ lệ khá cao. Không thể phủ nhận, ChatGPT là một công cụ hữu dụng, tiện ích với kho tri thức khổng lồ, đáp ứng được hầu hết mọi yêu cầu về thông tin của người sử dụng. Nếu biết cách khai thác và tìm kiếm có chọn lọc, ChatGPT sẽ là công cụ hữu dụng cho con người trong học tập, công việc và trong cuộc sống. Tuy nhiên, nếu quá phụ thuộc hoặc quá tin tưởng vào thông tin mà nó đưa ra sẽ dẫn đến nhiều hệ quả đáng lưu ý. Một vài hệ quả có thể kể đến là thông tin sai lệch hoặc chưa được kiểm chứng; bị lệ thuộc thông tin cá nhân,...

Qua biểu đồ, hai mục đích mà sinh viên ít sử dụng nhất là “kiểm tra, sửa lỗi ngữ pháp và chính tả” (12,14%) và “trò chuyện, tâm sự” (5,20%). Có thể thấy công cụ trí tuệ nhân tạo này vẫn không thể thay thế hoàn toàn được con người ở một vài khía cạnh (xem Hình 3).



- A. Xem đề xuất ý tưởng, gợi ý hoặc hướng giải quyết cho một vấn đề bất kì
- B. Giải đáp thắc mắc trong học tập, công việc và cuộc sống
- C. Kiểm tra, sửa lỗi ngữ pháp và chính tả
- D. Đánh giá, phân tích dữ liệu
- E. Tra cứu thông tin, ví dụ về các sự kiện, câu đố, tóm tắt sách,...
- F. Trò chuyện, tâm sự,...

Hình 3: Mục đích sử dụng Chat GPT của sinh viên (đơn vị: %)

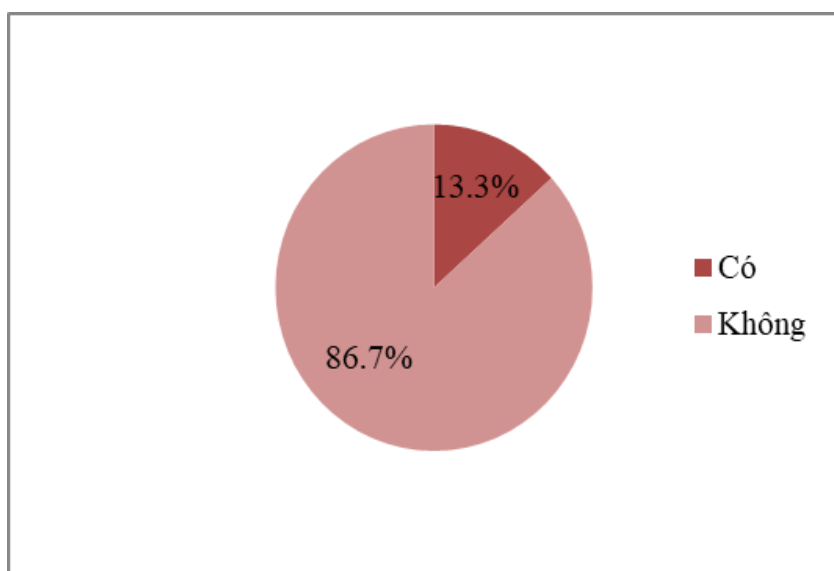
Người dùng hoàn toàn có thể nhận thức được tác động tiêu cực của ChatGPT gây ảnh hưởng đến họ. Theo kết quả khảo sát, nhận thấy 3/6 ảnh hưởng đưa ra có trên 50% cá nhân lựa chọn. Cụ thể, tác động gây ra ảnh hưởng tiêu cực đến người dùng chiếm tỷ lệ cao nhất là “Cung cấp thông tin không chính xác, không đáng tin cậy” (87,5%). Tác động có sự lựa chọn cao thứ hai là “Làm giảm khả năng tư duy phản biện”, chiếm 80%. Bên cạnh đó, “Hạn chế giao tiếp giữa người với người” và “Rò rỉ thông tin cá nhân, bí mật hoặc nhạy cảm” là hai sự lựa chọn có tỉ lệ tương đối cao trong bốn tác động còn lại, lần lượt chiếm 53,5% và 43%. Ngoài ra, 33,5 % và 26,5% theo thứ tự là tỉ lệ của các tác động “Bị tấn công bởi phishing” và “Tiềm ẩn rủi ro ChatGPT bị thao túng cho mục đích xấu, như tạo ra tin tức giả mạo hoặc tuyên truyền tư tưởng sai lệch”. Trong thực tế, ChatGPT là phần mềm được tạo ra nhờ dữ liệu từ Internet nên nó tiềm ẩn nhiều mặt hại đối với an ninh thông tin như việc ChatGPT có thể bị lợi dụng để hỗ trợ cho các cuộc tấn công phishing¹⁵. Từ đó người dùng có nguy cơ bị rò rỉ thông tin cá nhân như tên đăng nhập, mật khẩu, địa chỉ và nhiều thông tin bảo mật khác (Seymour, 2018). Không chỉ vậy, ChatGPT có thể cung cấp những thông tin không chính xác hoặc không phù hợp với các vấn đề như giáo dục, văn hóa, xã hội. (Xem Bảng 2)

¹⁵ Tấn công phishing: hình thức tấn công mạng bằng cách giả mạo để lừa đảo người dùng cung cấp thông tin cá nhân cho chúng

Bảng 2: Thực trạng nhận thức về tác động tiêu cực của ChatGPT đến người dùng

Tác động tiêu cực của ChatGPT đến người dùng	Tần số	Tỉ lệ (%)
Làm giảm khả năng tư duy phản biện	160	80%
Cung cấp thông tin không chính xác, không đáng tin cậy	175	87,5%
Tiềm ẩn rủi ro ChatGPT bị thao túng cho mục đích xấu, như tạo ra tin tức giả mạo hoặc tuyên truyền tư tưởng sai lệch	53	26,5%
Rò rỉ thông tin cá nhân, bí mật hoặc nhạy cảm	86	43%
Bị tấn công bởi phishing (* <i>phishing</i> : các đơn vị giả mạo để lừa đảo người dùng)	67	33,5%
Hạn chế giao tiếp giữa người với người	107	53,5%

Để khảo sát tình trạng xuất hiện quảng cáo có nội dung tương tự thông tin đã tìm kiếm trên ChatGPT, nhóm tác giả đã đưa ra câu hỏi “Bạn có từng gặp quảng cáo tương tự nội dung tìm kiếm trên ChatGPT không?” với hai lựa chọn “Có” và “Không”. Kết quả cho thấy tình trạng xuất hiện quảng cáo có nội dung tương tự sau khi tìm kiếm thông tin trên ChatGPT khá ít. Trong tổng 173 người sử dụng ChatGPT, mức độ người dùng đã từng gặp quảng cáo xuất hiện thường xuyên chiếm 13,3%. Ngược lại, chiếm tỉ lệ cao hơn là người dùng không gặp quảng cáo có nội dung tương tự với thông tin đã tìm kiếm trên ChatGPT (86,7%). Hiện nay, vấn đề này đối với người dùng ở Việt Nam dù chưa rõ ràng, nhưng đã có một vài nghiên cứu chỉ ra ChatGPT có mua bán thông tin của người sử dụng phần mềm này. Phòng vấn 1 sinh viên chọn câu trả lời “Có” cho câu hỏi này, nhận được ý kiến rằng sau khi tìm kiếm gợi ý về những bài hát đang nổi tiếng gần đây để nghe trên ChatGPT thì ngay sau đó, trang Facebook đã xuất hiện bài đăng quảng cáo từ Spotify (một ứng dụng nghe nhạc phổ biến đến từ Thụy Điển, có chức năng và mục đích hoạt động tương tự như Apple Music, Zing MP3,...) về bảng xếp hạng ca khúc hot của tuần. (Xem Hình 4)



Hình 4: Tỷ lệ xuất hiện quảng cáo tương tự nội dung đã kiểm trên ChatGPT

Về thực trạng sinh viên nhận được thông tin sai lệch từ ChatGPT, qua câu hỏi trắc nghiệm “Bạn đã bao giờ nhận được câu trả lời sai từ ChatGPT chưa?” với 2 lựa chọn “Chưa” và “Rồi”, nhóm tác giả đã thu thập kết quả và phân tích. Có 148/173 phiếu (85,55%) lựa chọn “rồi” trong câu hỏi này. Phỏng vấn thu thập được một số thông tin rằng ChatGPT thường xuyên sẽ có một vài lỗi sai khi thực hiện các phép tính nhân chia đơn giản, hoặc trả lời sai những câu hỏi về địa danh, nhân vật nổi tiếng trong một đất nước. Những sai lầm này đều mang tính lặp lại. Ngoài ra, còn tồn tại tình trạng “bịa” trích dẫn khoa học hay luận văn, tức nội dung trích dẫn không có thật từ ChatGPT. Điều này đặt ra thách thức lớn đối với sinh viên trong việc chọn lọc thông tin đúng và xác thực, bởi thường các câu trả lời trong ứng dụng này sẽ không nhắc đến nguồn tham khảo.

4.2. Thảo luận

ChatGPT có thể gây nên một số ảnh hưởng đến an ninh thông tin cá nhân trong môi trường học đường của sinh viên Trường Đại học Kinh tế Quốc dân.

ChatGPT mua bán thông tin người dùng cho bên thứ ba như một số nền tảng mạng xã hội Facebook, Tiktok. Theo nghiên cứu của Junaid Qadir (2022) , ChatGPT đã trả lời về lo ngại quyền riêng tư: “Có nhiều mối quan tâm về quyền riêng tư xoay quanh việc sử dụng ChatGPT và những công cụ AI khác ở môi trường học đường. Điều quan trọng là nhà trường có những chính sách rõ ràng liên quan đến việc sử dụng các công cụ này và đảm bảo dữ liệu sinh viên được bảo vệ đúng cách”. Một lập trình viên người Hoa Kỳ cho rằng: “Đây là một rủi ro bảo mật bao gồm quá trình tương tác với ChatGPT có thể tiết lộ quyền riêng tư cá nhân (tuổi, giới tính, thông tin liên lạc, sở thích và thậm chí tài khoản vốn và quyền riêng tư cá nhân khác). Nhiều thông tin cá nhân này bị lộ trong

quá trình giao tiếp vô thức của người dùng. Liệu tính hợp pháp của việc thu thập dữ liệu và phương pháp xử lý dữ liệu được giới hạn bởi luật pháp và quy định liên quan.” (Ahmed Tlili et al., 2023) Người dùng sẽ gặp những cuộc gọi bán hàng, tư vấn từ một bên mình không quan tâm và đăng ký thông tin cá nhân. Không chỉ số điện thoại mà thông tin về địa chỉ nhà, căn cước công dân cũng được đưa ra để trao đổi mua bán. Những nội dung được trao đổi trên ChatGPT có thể xuất hiện trên nền tảng xã hội khác. Ví dụ điển hình là nhân viên Samsung đã để lộ dữ liệu bí mật công ty khi sử dụng ChatGPT. Một phần nguyên nhân trong đó là do người dùng đã chủ quan khi cập nhật các thông tin cá nhân các nền tảng yêu cầu. Theo ông Nguyễn Minh Đức - Nhà sáng lập kiêm Giám đốc điều hành Công ty Cổ phần An toàn thông tin CyRadar: “Hầu hết các thông tin cá nhân của người sử dụng hiện nay ở Việt Nam thì đều do chính người sử dụng tự đưa lên, từ thông tin ngày sinh cho đến địa điểm đang làm việc ở đâu, rồi thông tin trong nhà có những gì...”. Bên cạnh trao đổi mua bán thông tin thì ChatGPT cũng là một cơ hội tiềm năng cho hacker xâm nhập và đánh cắp hồ sơ cá nhân được bảo mật. Nhiều vụ tấn công bảo mật vẫn xảy ra khó kiểm soát trên Facebook, Twitter, Google hay Youtube và ChatGPT khó có thể tránh khỏi tình huống này. Những tài khoản có mật khẩu yếu, ít phương thức xác thực đăng nhập, bảo mật có rủi ro cao hơn trong việc mất tài khoản cá nhân. Không chỉ bị lấy cắp thông tin, tội phạm mạng lấy cắp cả mật khẩu, tài khoản người dùng. “Mối quan tâm đến các nền tảng AI tạo sinh như ChatGPT ngày một nóng hơn, cả trong và ngoài nước. Chúng có thể đem lại hiệu quả nhưng rủi ro về bảo mật ngày càng tăng – Samsung gửi thông báo đến nhân viên. Những thông tin bị lấy cắp, trao đổi mua bán cho bên tội phạm thứ ba dùng cho các mục đích xấu như giả dạng danh tính vay tiền, rút tiền hoặc lừa đảo mua bán tài sản, thậm chí đe dọa, bắt cóc tống tiền.

ChatGPT có một số vấn đề về bản quyền. Với câu trả lời sáng tạo, giống với nội dung con người tạo ra, đây là công cụ được nhiều người tin tưởng và sử dụng. Trong nghiên cứu, Junaid Qadir (2022), ChatGPT đã trả lời về sự khác biệt giữa sử dụng ChatGPT được chấp nhận và đạo văn là ChatGPT sử dụng nguồn dữ liệu đưa ra ý tưởng, nguồn cảm hứng cho tác phẩm gốc thay vì sao chép, trình bày tác phẩm người khác như của riêng mình. Bên cạnh đó, nó còn trả lời để tránh tội đạo văn thì phải hiểu và tuân thủ nguyên tắc trích dẫn, luôn đưa ra nguồn gốc của bất kỳ ý tưởng hay nội dung nào mà sử dụng trong tác phẩm của mình và cần kiểm tra đảm bảo trích dẫn chính xác. Theo ông Kelber: “Theo Sách Xanh (Bluebook - cuốn sách hướng dẫn về việc trích dẫn theo luật sở hữu trí tuệ), việc trích dẫn đến những nguồn như ChatGPT là phù hợp” (Hương Hoàng, TheLEADER, 2023). Tuy nhiên, đa số câu trả lời ChatGPT không có trích dẫn nguồn dẫn đến nguy cơ vi phạm bản quyền tác giả. Có những nội dung của các tác giả không được công khai vì lý do bản quyền nhưng ChatGPT vẫn có thể sử dụng chúng vào

trong câu trả lời của mình. Điều đó có thể dẫn đến rò rỉ các ý tưởng của các tác giả cũng như người sử dụng câu trả lời có thông tin không được chấp thuận. Cùng với đó, nội dung ChatGPT tạo ra có chủ sở hữu là ai đang là vấn đề gây tranh cãi. Một số quan điểm cho rằng ChatGPT có quyền tác giả của nội dung nó tạo ra vì nó là chủ thể tạo ra nội dung, dựa vào nền tảng, không dựa vào trí tuệ người dùng. Ngược lại, có ý kiến ChatGPT không có quyền tác giả do nội dung được xây dựng dựa vào yêu cầu của người dùng cùng với việc người sử dụng chi tiền để có được nguồn dữ liệu của ChatGPT. Ngoài ra, một số luồng ý kiến cho rằng nội dung ấy do cả ChatGPT và người dùng cùng sở hữu.

ChatGPT đưa ra những nguồn thông tin sai lệch. ChatGPT có khả năng đưa ra các câu trả lời không trùng lặp nhưng phần lớn không có trích dẫn nguồn, nếu có thì thường nguồn không rõ ràng, thậm chí không đúng. Trong năm 2023, OpenAI – công ty sáng tạo ra ChatGPT đối mặt với nguy cơ bị kiện do sai lệch thông tin của một thị trường bang Victoria. “Nhiều câu trả lời của ChatGPT đã bị người dùng “dẫn dắt” dẫn đến việc từ trả lời đúng, ChatGPT bị “lái” theo người dùng dẫn đến trả lời sai” (Huyền Thanh, Báo điện tử Công an nhân dân, 2023). Junaid Qadir (2022) đã nghiên cứu đặt câu hỏi cho ChatGPT và nhận được câu trả lời về thông tin sai lệch: “ChatGPT và các công cụ AI chỉ hoạt động tốt khi họ dữ liệu và dữ liệu dựa trên chúng. Nếu dữ liệu không chính xác hoặc thuật toán có sai sót, kết quả có thể không chính xác hoặc gây hiểu nhầm. Điều quan trọng hơn là sinh viên phải phân biệt được sự chính xác của thông tin nhận được từ các công cụ và sử dụng đa nguồn khi nghiên cứu một chủ đề”. ChatGPT là một mô hình trí tuệ nhân tạo nên có thể tạo ra những thông tin vô nghĩa hoặc sai lệch bởi tính chất hạn chế của mô hình, chất lượng dữ liệu được đào tạo, thông tin đầu vào. Một lập trình viên người Hoa Kỳ nói rằng: “Nội dung ChatGPT trả lời phụ thuộc vào loại câu hỏi được đưa ra. Nếu nó quá gần đây, câu trả lời sẽ không quá tốt vì thiếu ngữ cảnh, nếu bạn không cung cấp câu hỏi cụ thể thì câu trả lời sẽ không thực sự tốt” (Ahmed Tlili et al., 2023). Một trợ lý giáo sư về công nghệ giảng dạy, Hoa Kỳ cho rằng mối quan tâm lớn của ChatGPT là tạo ra thông tin giả mạo và đáng tin cậy do máy tính tạo ra thay vì con người ra quyết định, vì vậy có nhiều lo ngại về đạo đức do học sinh dựa vào các câu trả lời mà không nhận thức được ý nghĩa của chúng (Ahmed Tlili et al., 2023). ChatGPT tuyên bố rõ ràng đôi khi sẽ tạo ra thông tin không chính xác hoặc nội dung sai lệch. Chất lượng nội dung ChatGPT cung cấp phụ thuộc vào câu hỏi, nếu câu hỏi không cụ thể, thiếu ngữ cảnh thì câu trả lời có thể có thông tin sai. Và những thông tin sai sự thật sẽ dẫn đến sai lệch về kiến thức, hiểu nhầm về một số thông tin và đối tượng, thậm chí thao túng tâm lý, lệch lạc tư tưởng người dùng. Một số đối tượng chống phá lợi dụng câu trả lời sai sót của ChatGPT (một công cụ được nhiều người tin cậy) đăng tải lên các trang Internet nhằm xuyên tạc, bôi nhọ danh dự nhà lãnh tụ, lịch sử đất nước.

Ngoài những kết luận mà nghiên cứu chỉ ra như trên, một số nghiên cứu trước đó cũng đã từng đề cập đến những tác động tiêu cực khác của ChatGPT đối với sinh viên, đặc biệt liên quan đến vấn đề học tập và nhận thức.

Thứ nhất, việc sinh viên sử dụng ChatGPT có thể dẫn đến sự suy giảm tư duy phản biện và khả năng giải quyết vấn đề (Kasneci et al., 2023). Cụ thể, do tính năng đưa ra những câu trả lời hợp lý của ChatGPT, việc sinh viên sử dụng chương trình này để hoàn thành các bài tập trên trường đang khiến quá trình này bị tối giản hóa và sinh viên sẽ không có quá nhiều sự chủ động đối với việc tìm kiếm và tổng hợp thông tin. Theo như kết quả khảo sát mà chúng tôi đã chỉ ra trước đó, tỷ lệ sinh viên trong Trường Đại học Kinh tế Quốc dân sử dụng ChatGPT để xem đề xuất ý tưởng, gợi ý hoặc hướng giải quyết cho một vấn đề lên đến 86,7%. Điều này có nghĩa, xu hướng sinh viên bị phụ thuộc vào ChatGPT trong học tập đang ngày càng tăng lên và nó sẽ có những tác động tiêu cực nhất định đến khả năng tư duy, sáng tạo và xử lý thông tin của sinh viên.

Thứ hai, ChatGPT có thể tạo ra những thách thức nhất định đối với việc kiểm tra và đánh giá kết quả học tập của sinh viên ở trường. Một trong những thách thức lớn nhất là vấn đề đạo văn, khi sinh viên sử dụng những sản phẩm của ChatGPT để nộp bài. Dựa trên một số từ khóa và gợi ý được người dùng đưa ra trước đó, ChatGPT có thể tạo ra những sản phẩm mang tính nguyên bản và hợp lý mà không cần đến sự chỉnh sửa của con người (Dehouche, 2021). Điểm mấu chốt ở đây là những thông tin mà chương trình này mang lại ở đây là tổng hợp từ nghiên cứu của rất nhiều học giả đi trước, cho nên không dễ để đưa ra một kết luận về đạo văn (Sadeghi, 2019). Như vậy, nếu sinh viên lợi dụng những tính năng này để phục vụ cho lợi ích cá nhân, điều này đi ngược với tính công bằng trong đánh giá học lực và làm giảm giá trị của bằng cấp. Ngoài ra, chính các giáo viên cũng sẽ gặp nhiều khó khăn hơn để đưa ra được đánh giá khách quan về năng lực thật sự của sinh viên (Cotton et al., 2023). Trên thực tế, rất khó để người chấm bài để có thể phân biệt một cách chính xác giữa một bài làm do người làm và một bài làm do máy làm, cho nên khi sinh viên sử dụng ChatGPT để làm những bài tập trên lớp thì không dễ để phản ánh được mức độ thông hiểu thực chất của sinh viên về vấn đề đang được đặt ra. Không chỉ vậy, ChatGPT còn có thể tạo ra những bất bình đẳng về cơ hội học tập (Cotton et al., 2023). Khi một sinh viên sử dụng chương trình để tạo ra những sản phẩm chất lượng cao và dùng những sản phẩm này để đạt kết quả tương ứng thì sẽ xảy ra tình trạng bất công đối với những đối tượng không có khả năng tiếp cận với ChatGPT. Theo khảo sát về mức độ sử dụng ChatGPT của sinh viên mà nhóm tác giả đưa ra, số lượng sinh viên chưa bao giờ sử dụng ứng dụng này đạt 13,5%. Nếu không nhanh chóng đưa ra những quy định hạn chế đối với ChatGPT thì sẽ tạo ra những bất cập nhất định trong việc đánh giá, xếp loại sinh viên.

Thứ ba, các câu trả lời của ChatGPT có thể bị ảnh hưởng bởi những định kiến vốn có trong dữ liệu ban đầu được dùng để đào tạo trong các thuật toán (Lund and Ting, 2023), dẫn đến đưa ra những thông tin có thể bất bình đẳng và sai lệch hướng đến một số nhóm đối tượng nhất định, cụ thể là về giới tính, sắc tộc và quan điểm chính trị (Addington, 2023). Ví dụ, nếu ChatGPT cho ra những phản hồi mang tính phân biệt đối với một giới tính hay chủng tộc nhất định, nó có thể góp phần rất lớn vào việc duy trì và quảng bá những định kiến tiêu cực này đến với người dùng (Addington, 2023).

5. Kết luận và gợi ý

5.1. Kết luận

Kết quả phân tích cho thấy số lượng sinh viên Trường Đại học Kinh tế Quốc dân hiện nay sử dụng Công cụ AI - Chat GPT trong học tập và cuộc sống tương đối lớn. Điều này đồng nghĩa sinh viên chịu sự chi phối của Chat GPT đến hành vi, thói quen tìm kiếm và sử dụng thông tin. Tuy vậy cả sinh viên, giảng viên, và cả hệ thống quản lý chưa có những quy định cụ thể về việc sử dụng Chat GPT trong môi trường học đường và đảm bảo an ninh thông tin trong môi trường học đường.

Ngoài ra, kết quả khảo sát còn cho thấy nhiều sinh viên đã nhận thức được về các tác động tiêu cực của Chat GPT đến an ninh thông tin trong môi trường học đường. Mặt khác tỉ lệ sinh viên thực tế trực tiếp chịu ảnh hưởng tiêu cực đến các vấn đề an ninh thông tin trong quá trình sử dụng Công cụ AI - Chat GPT tương đối cao.

5.2. Gợi ý

Qua kết quả phân tích, một số giải pháp để hạn chế tác động tiêu cực đến vấn đề an ninh thông tin trong môi trường học đường của người sử dụng Công cụ Chat GPT là sinh viên được đề xuất như sau:

Thứ nhất, sinh viên - chủ thể sử dụng Chat GPT cần có những nhận thức đúng đắn về giới hạn và lợi ích của ChatGPT đồng thời sử dụng ChatGPT an toàn, hiệu quả, có trách nhiệm, đảm bảo an ninh thông tin trong môi trường Đại học.

Thứ hai, nhà trường, các cơ sở giáo dục, các đơn vị có thẩm quyền cần xây dựng các quy định về việc sử dụng Chat GPT nói riêng và các công cụ AI nói chung phù hợp với đặc điểm quản lý, giáo dục đào tạo, các quy định, chuẩn mực về an ninh thông tin.

Thứ ba, việc nghiên cứu và cải tiến liên tục về tính bảo mật, tính chính xác và đáng tin cậy của ChatGPT là cần thiết.

LỜI CẢM ƠN

Xin cảm ơn sự hỗ trợ, cố vấn về mặt nội dung của TS. Trần Thị Thu Huyền - giảng viên Trường Đại học Kinh tế Quốc dân; TS. Đào Thị Diệu Linh - giảng viên Trường Đại học Ngoại ngữ, Đại học Quốc gia Hà Nội và bà Nguyễn Thị Khánh Trâm - Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh Hà Tĩnh đã góp phần hoàn thiện nội dung đề tài của nhóm tác giả.

TÀI LIỆU THAM KHẢO

- A. Tlili et al. (2023). What if the devil is my guardian angel: ChatGPT as a case study of using chatbots in education. **Smart Learn. Environ.**, 10(1), 1–24. doi: 10.1186/S40561-023- 00237-X/FIGURES/13.
- Addington, S. (2023). ChatGPT: cyber security threats and countermeasures. <https://doi.org/10.2139/ssrn.4425678>
- Choi, Jonathan H. and Hickman, Kristin E. and Monahan, Amy and Schwarcz, Daniel B. (2023). ChatGPT goes to law school. **Journal of Legal Education (Forthcoming)**. <http://dx.doi.org/10.2139/ssrn.4335905>
- Cotton, D. R., Cotton, P. A., and Shipway, J. R. (2023). Chatting and Cheating: ensuring academic integrity in the era of ChatGPT. **Innovations in Education and Teaching International**. doi: 10.1080/14703297.2023.2190148
- Dehouche, N. (2021). Plagiarism in the age of massive Generative Pre-trained Transformers (GPT-3). **Ethics in Science and Environmental Politics**, 21, 17-23. doi: 10.3354/esep00195
- J. Qadir (2023). Engineering education in the era of ChatGPT: promise and pitfalls of generative AI for education. **IEEE Glob. Eng. Educ. Conf.**, 1–9. doi: 10.1109/EDUCON54358.2023.10125121.
- Kasneci, E., Seßler, K., Küchemann, S., Bannert, M., Dementieva, D., Fischer, F., Kasneci, G. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. <https://doi.org/10.35542/osf.io/5er8f>
- Kung, T. H., Cheatham, M., ChatGPT, Medenilla, A., Sillos, C., Leon, L. D., Elepaño, C., Madriaga, M., Aggabao, R., Diaz-Candido, G., Maningo, J., & Tseng, V. (2022). Performance of ChatGPT on USMLE: Potential for AI-assisted medical education using large language models. **medRxiv**. doi:10.1371/journal.pdig.0000198.
- L.-A. Vinh, B.-T. Dien, L.-Q. Quan, V.-V. Luan (2023), Khả năng thực hiện bài kiểm tra định kì môn Toán và môn Ngữ văn cấp Trung học của công cụ ChatGPT: kết quả nghiên cứu và một số khuyến nghị ban đầu. **Tạp chí Khoa học Giáo dục Việt Nam**. 2. doi: 10.15625/2615-8957/12310201
- Lund, B. D., & Wang, T. (2023). Chatting about ChatGPT: how may AI and GPT impact academia and libraries? **Library Hi Tech News**, 40(3), 26-29. doi: 10.1108/LHTN-01-2023-0009
- Sadeghi R. (2019). The attitude of scholars has not changed towards plagiarism since the medieval period: definition of plagiarism according to Shams-e-Qays,

thirteenth-century Persian literary scientist. Sage Journal, 15(2).
<https://doi.org/10.1177/1747016116654065>

Seymour, J., & Tully, P. (2018). Generative models for spear phishing posts on social media. <https://doi.org/10.48550/arXiv.1802.05196>

T. B. Brown (2020). Language models are few-shot learners.
<https://doi.org/10.48550/arXiv.2005.14165>

X.-Q. Dao, N.-B. Le, X.-D. Phan, B.B. Ngo (2023). Can ChatGPT pass the Vietnamese national high school graduation examination?. doi:10.48550/arXiv.2306.09170.

**THÁI ĐỘ CỦA SINH VIÊN TẠI TP. HỒ CHÍ MINH VỀ
NHỮNG THÔNG TIN XẤU, ĐỘC TRÊN MẠNG XÃ HỘI VÀ
VIỆC ĐỀ XUẤT XÂY DỰNG MÔ HÌNH CÂU LẠC BỘ
“PHỦ XANH THÔNG TIN” TRONG CÁC TRƯỜNG ĐẠI HỌC
TRÊN ĐỊA BÀN THÀNH PHỐ HỒ CHÍ MINH
THE ATTITUDES OF STUDENTS IN HO CHI MINH CITY
ABOUT THE BAD, TOXIC CONTENTS ON SOCIAL
NETWORKS AND THE PROPOSAL OF BUILDING AN
“INFORMATION GREENING” CLUB IN UNIVERSITIES IN
HO CHI MINH CITY**

Nguyễn Thị Lâm, Trần Phạm Công Tuấn*, Nguyễn Quốc Kiệt

Trường Đại học An ninh nhân dân

*Tác giả liên hệ: tpct.tuan@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Thông tin xấu độc, mạng xã hội, sinh viên, câu lạc bộ “phủ xanh thông tin”	Nghiên cứu được thực hiện nhằm mục đích khảo sát thái độ của sinh viên tại Thành phố Hồ Chí Minh về những thông tin xấu, độc trên mạng xã hội. Dữ liệu nghiên cứu được thu thập thông qua công cụ chính là bảng hỏi được thiết kế trên Google Form. Nghiên cứu đã tìm ra được những điểm tích cực cũng như những tồn tại còn hạn chế trong thái độ của sinh viên tại Thành phố Hồ Chí Minh về những thông tin xấu, độc trên mạng xã hội. Từ đó đề xuất xây dựng mô hình Câu lạc bộ “phủ xanh thông tin” trong các trường đại học, cao đẳng tại Thành phố Hồ Chí Minh nhằm giải quyết các hạn chế còn tồn tại.
<i>Keywords:</i> Bad and toxic contents, social networks, students, “Information greening” club	ABSTRACT This study was conducted to survey the attitudes of students who are studying at a university or a college in Ho Chi Minh City about bad and toxic contents on social networks. Research data was collected through a questionnaire designed on Google Form. The study has found both positive and negative sides in the attitudes of students in Ho Chi Minh city about bad and toxic contents on social networks. On that basis, the research proposes to build an “Information Greening” Club in universities or colleges in Ho Chi Minh city to solve the negative sides.

1. Giới thiệu:

Trong những năm trở lại đây, Mạng xã hội (MXH) phát triển cực kì mạnh mẽ, ảnh hưởng sâu sắc đến nhiều mặt trong đời sống kinh tế, xã hội ở hầu hết các quốc gia trên thế giới, trong đó có Việt Nam. Định nghĩa về MXH, theo PGS. TS. Mai Đức Ngọc: *“Mạng xã hội là một dịch vụ trên mạng Internet, cho phép người dùng tương tác, giao tiếp, chia sẻ dữ liệu, thông tin, đồng thời cung cấp các dịch vụ cho phép các thành viên tương tác, phản hồi thông tin qua các tin nhắn, góp ý...”* [6, tr. 16]. Hay theo Khoản 22 Điều 3 Nghị định 72/2013/NĐ-CP ngày 15 tháng 7 năm 2013 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng nêu rõ về MXH:

“Mạng xã hội (social network) là hệ thống thông tin cung cấp cho cộng đồng người sử dụng mạng các dịch vụ lưu trữ, cung cấp, sử dụng, tìm kiếm, chia sẻ và trao đổi thông tin với nhau, bao gồm dịch vụ tạo trang thông tin điện tử cá nhân, diễn đàn (forum), trò chuyện (chat) trực tuyến, chia sẻ âm thanh, hình ảnh và các hình thức dịch vụ tương tự khác”. [1]

Tại Việt Nam, các MXH bắt đầu du nhập từ những năm 2000 dưới hình thức các trang nhật ký điện tử (blog). Theo Báo cáo Tổng quan phát triển kỹ thuật số Việt Nam 2023 do “We are social” công bố đầu năm 2023: Việt Nam có 77.93 triệu người sử dụng Internet (tương đương 79.1% so với tổng dân số, tăng 5.3 triệu người (tăng 7.3%) so với năm 2022). Cũng theo báo cáo này, vào tháng 1 năm 2023, Việt Nam có 70 triệu người dùng MXH và trong đó có 64,4 triệu người dùng từ 18 tuổi trở lên sử dụng MXH (tương đương với 89% tổng dân số từ 18 tuổi trở lên tại thời điểm đó). Thêm vào đó, 89,8% tổng số người dùng internet của Việt Nam (không phân biệt độ tuổi) đã sử dụng ít nhất một nền tảng MXH vào tháng 1 năm 2023. Và 5 nền tảng MXH được sử dụng nhiều nhất tại Việt Nam gồm: Facebook (91.6%), Zalo (90.1%), TikTok (77.5%), Facebook Messenger (77%) và Instagram (55.4%).

Số lượng người sử dụng MXH ngày càng đông đảo và tăng lên đặc biệt là thanh thiếu niên học sinh, sinh viên trong độ tuổi từ 16 đến 24. Có thể thấy, với sự phát triển nhanh chóng của khoa học công nghệ cùng với đời sống của người dân ngày một tăng lên, việc tiếp cận với những cái mới từ bên ngoài là điều không mấy khó khăn, đặc biệt là đối với giới trẻ.

MXH mang đến rất nhiều lợi ích cho các bạn sinh viên. Đây là một nguồn thông tin khổng lồ, đa dạng để các bạn tiếp cận hỗ trợ học tập cũng như vui chơi giải trí và chia sẻ thông tin lên đó; một nơi để kết nối bạn bè, người thân, kết bạn ở mọi nơi, v.v. Thế nhưng, do là một nguồn thông tin khổng lồ, có rất ít sự kiểm soát những thông tin trên đó, việc tồn tại những thông tin sai lệch, không đúng sự thật hay những thông tin độc hại vẫn còn là một hạn chế lớn. Việc tiếp cận những thông tin xấu, độc mà không có sự chọn lọc cẩn thận, xác minh tính đúng đắn sẽ gây ra rất nhiều tiêu cực, đặc biệt đối với các bạn

sinh viên. Điển hình gần đây, vụ việc tại Trường Quân sự Quân khu 7 vào tháng 01 năm 2023. Cụ thể, tối ngày 11/01/2023, trên MXH lan truyền thông tin trong thời điểm sinh viên Trường HUFLIT học quân sự tại Trung tâm Giáo dục quốc phòng và an ninh, Trường Quân sự Quân khu 7, có hai sinh viên nữ bị xâm hại tình dục dẫn đến tự tử khiến một nữ sinh tử vong và một nữ sinh bị liệt ngay trong trung tâm này. Đây là thông tin hoàn toàn sai sự thật, bịa đặt. Thông tin sai sự thật này đã được lan truyền đi rất nhanh qua các hội nhóm, các trang fanpage trên Facebook, Zalo, v.v gây sự hoang mang, tiêu cực trong dư luận, đặc biệt là tâm lý của các bạn sinh viên. Qua điều tra, xác minh vụ việc, cơ quan chức năng đã xác định và đưa ra xử lý các đối tượng có hành vi tuyên truyền, phát tán thông tin sai sự thật gây hoang mang trong dư luận. Và thực tế còn tồn tại rất nhiều vụ việc phát tán, tuyên truyền thông tin xấu, độc chưa được xử lý.

Sinh viên là đối tượng rất dễ bị tác động, ảnh hưởng, tin theo những thông tin xấu, độc trên MXH. Bởi các bạn sử dụng MXH rất thường xuyên, cập nhật thông tin rất nhạy bén; khi thấy các tin nóng, tin giật gân, vì sợ “lạc hậu” so với mọi người, các bạn hầu như sẽ tin tưởng mà không cần xác minh, nghi ngờ, và thậm chí còn chia sẻ rất “nồng nhiệt”. Đứng trước tình hình thực tế đó, cần đánh giá thái độ của các bạn sinh viên trên địa bàn Thành phố Hồ Chí Minh (TP.HCM) trước những thông tin xấu, độc trên MXH; đồng thời, đề xuất một số ý kiến, giải pháp nhằm nâng cao nhận thức của sinh viên. Thế nhưng hiện nay, vấn đề này chưa được nghiên cứu cụ thể. Vì vậy, nhóm nghiên cứu đã lựa chọn đề tài ***“Thái độ của sinh viên trên địa bàn Thành phố Hồ Chí Minh về những thông tin xấu, độc trên mạng xã hội và việc đề xuất xây dựng mô hình câu lạc bộ “phủ xanh thông tin” trong các trường đại học trên địa bàn Thành phố Hồ Chí Minh”*** để thực hiện.

Để tìm hiểu thái độ của sinh viên trên địa bàn TP.HCM trước những thông tin xấu, độc trên MXH, chúng tôi đã tiến hành phương pháp điều tra bằng bảng hỏi 300 sinh viên từ các trường đại học tại TP.HCM. Trong bài tham luận này, chúng tôi sẽ trình bày một số kết quả về: 1/ Mức độ sử dụng MXH của sinh viên tại TP.HCM, 2/ Thái độ của sinh viên tại TP.HCM trước những thông tin xấu, độc trên MXH, 3/ Đề xuất xây dựng mô hình Câu lạc bộ “phủ xanh thông tin” nhằm định hướng thái độ, hạn chế ảnh hưởng của thông tin xấu, độc đến sinh viên tại TP.HCM.

2. Cơ sở lý thuyết:

2.1. *Thái độ của sinh viên về thông tin xấu, độc*

Thái độ

Trong từ điển tiếng Việt, “thái độ” được định nghĩa là: “cách nhìn nhận, hành động của cá nhân về một hướng nào đó trước một vấn đề, một tình huống cần giải quyết. Đó là tổng thể những biểu hiện ra bên ngoài của ý nghĩ, tình cảm của cá nhân đối với con người hay một sự việc nào đó” [4, tr. 894].

Hay theo Tôn Nữ Cẩm Hương (2014) định nghĩa về thái độ là “một bộ phận hợp thành, một thuộc tính trọn vẹn của ý thức, quy định tính sẵn sàng hành động của con người đối với đối tượng theo một hướng nhất định, được bộc lộ ra bên ngoài thông qua hành vi, cử chỉ, nét mặt và lời nói của người đó trong những tình huống, điều kiện cụ thể”. [10, tr. 21]

Nhìn chung, thái độ có thể được xem là “cách ứng xử của cá nhân đối với các vấn đề, các tình huống xã hội”.

Thái độ được định nghĩa và hiểu theo nhiều cách khác nhau. Trước hết, thái độ được xem giống như “một hành động đánh giá đối với một số đối tượng được giới thiệu hoặc thái độ, được suy luận dựa trên niềm tin hoặc ý kiến của cá nhân về đối tượng đó”. [2, tr. 9]. Một nhà nghiên cứu khác cho rằng thái độ là “phản ứng của cá nhân đối với bất cứ điều gì liên quan đến bối cảnh trực tiếp mà ngôn ngữ được dạy” [7, tr. 172-173]. Garrett đưa ra một quan điểm khá tương đồng với Gardner và cho rằng thái độ là “một định hướng đánh giá đối với một đối tượng xã hội nào đó cho dù đó là ngôn ngữ hay chính sách mới của chính phủ, v.v.” [3, tr. 20]. Thêm vào đó, ông mô tả thái độ trong mối tương quan với giá trị, thói quen, quan điểm, niềm tin, khuôn mẫu xã hội và hệ tư tưởng tương ứng với mục đích để phân biệt chúng.

Thái độ bao gồm 03 yếu tố chính: nhận thức, tình cảm, hành động [5, 3, 2]. Yếu tố nhận thức là thể hiện niềm tin, suy nghĩ hoặc quan điểm của một người đối với một đồ vật. Yếu tố tình cảm là cách cá nhân thể hiện tình cảm, cảm xúc về đối tượng dù thích hay không thích và dẫn đến hành vi của cá nhân đó (được gọi là khía cạnh thứ ba của thái độ) trong một tình huống học tập nhất định.

Qua nghiên cứu và xem xét, nhóm nghiên cứu nhận thấy thái độ phải có sự kết hợp biện chứng giữa nhận thức, tình cảm và hành vi; phải hiểu biết về đối tượng, phải có tình cảm, cảm xúc với đối tượng thì bản thân mới có thể hình thành thái độ, hành vi phù hợp đối với đối tượng. Vì vậy, nhóm nghiên cứu lựa chọn quan điểm ba thành phần thống nhất làm cơ sở cho việc nghiên cứu.

Thông tin xấu, độc

Theo Điều 2 Luật Tiếp cận thông tin 2016, thông tin được định nghĩa là: “tin, dữ liệu được chứa đựng trong văn bản, hồ sơ, tài liệu có sẵn, tồn tại dưới dạng bản viết, bản

in, bản điện tử, tranh, ảnh, bản vẽ, băng, đĩa, bản ghi hình, ghi âm hoặc các dạng khác do cơ quan nhà nước tạo ra” [9].

Theo Từ điển Tiếng Việt, xấu mang nhiều nét nghĩa khác nhau bao gồm:

“1 Có hình thức, vẻ ngoài khó coi, gây cảm giác khó chịu, làm cho không muốn nhìn ngắm; trái với đẹp. ... 2 Có giá trị, phẩm chất kém, đáng chê; trái với tốt. ... 3 Thuộc loại có thể gây hại, mang lại điều không hay, đáng phàn nàn; trái với tốt. ... 4 Trái với đạo đức, đáng chê trách; trái với tốt. ... 5 Có giá trị đạo đức, tinh thần kém, đáng khinh, đáng xấu hổ. ...”. [4, tr. 1451]

Tương tự như vậy, độc được hiểu là: “1 Có tác dụng làm hại sức khỏe hoặc làm cho chết. ... 2 Hiểm ác, làm hại người. ... 3 (Lời nói) có thể mang lại tai họa, sự chết chóc, theo mê tín. ...” [4, tr. 423].

Vậy thông tin xấu, độc trong nghiên cứu này được hiểu là những thông tin chứa nội dung độc hại, có thể gây ảnh hưởng xấu đến nhận thức, tinh thần thậm chí là sức khỏe của con người. Thông tin xấu, độc phát tán trên MXH về nội dung và bản chất, là những thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, “đổi trắng, thay đen”, lẫn lộn đúng sai, thật giả hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng luận điệu thù địch.

2.2. Ảnh hưởng tiêu cực của những thông tin xấu, độc trên mạng xã hội đối với sinh viên trên địa bàn Thành phố Hồ Chí Minh

Thông tin xấu, độc trên mạng xã hội khiến sinh viên hiểu sai về các chủ trương, đường lối của Đảng và chính sách, pháp luật của Nhà nước, gây mất niềm tin vào Đảng, Nhà nước, chính quyền.

Thực tế cho thấy sinh viên là lực lượng rất nhạy cảm, thường rất dễ bị lôi kéo và kích động. Vì thế, các thế lực thù địch, phản động trong và ngoài nước luôn xem sinh viên là đối tượng đặc biệt để thực hiện các âm mưu “diễn biến hòa bình”. Chúng lợi dụng sự phát triển của công nghệ thông tin, Internet để phát tán tài liệu có nội dung phản động, thông tin xấu, độc, ấn phẩm văn hóa đồi trụy để dần dần “chuyển hóa” giới trẻ, nhằm tạo ra một thế hệ trẻ sống theo chủ nghĩa thực dụng, vụ lợi, vị kỷ, sẵn sàng xét đoán quá khứ và vai trò lãnh đạo của Đảng, Nhà nước ta. Những thông tin xấu, độc nếu không kịp thời ngăn chặn sẽ tác động tiêu cực đến tư tưởng, gieo rắc sự hoài nghi, làm giảm sút lòng tin của thế hệ trẻ đối với Đảng, Nhà nước.

Thông tin xấu, độc làm ảnh hưởng đến tinh thần, đời sống, thậm chí là sức khỏe của sinh viên.

Một bộ phận người sử dụng MXH ở Việt Nam thường có xu hướng quan tâm, thích (like) hoặc chia sẻ (share) thông tin giật gân, tiêu cực, trái chiều hơn thông tin tích cực. Nhiều người cho rằng MXH là ảo, không phải chịu trách nhiệm về những phát ngôn, hành xử của mình. Tâm lý đó cộng hưởng với các công cụ được tạo ra để thu hút

người dùng của truyền thông xã hội, cùng với sự bất cập, hạn chế trong quản lý của các cơ quan chức năng càng làm cho việc phát tán thông tin xấu, độc trở nên dễ dàng và nguy hiểm. Những nghiên cứu gần đây chỉ ra, hiện tượng tin giả, các phát ngôn thù ghét, nói xấu, phỉ báng, bịa đặt, kỳ thị dân tộc, tôn giáo, kỳ thị giới tính, các hành vi gây hấn, tấn công trên mạng, v.v đang trở nên đáng báo động. Những hành vi lệch lạc này có thể làm khủng hoảng đời sống cá nhân, có cá nhân đã lựa chọn cái chết làm lối thoát.

Hơn nữa, với đặc tính hấp dẫn, lôi cuốn của thông tin xấu, độc trên các trang MXH rất dễ làm cho người tham gia bị sa đà vào “biển thông tin” hỗn loạn đó lúc nào mà không hay biết, làm cho các bạn sinh viên sao nhãng việc học hành, giảm năng suất lao động, tinh thần uể oải, sa sút, đắm chìm vào thế giới ảo trong đời sống thực. Đây chính là tác nhân làm ảnh hưởng nghiêm trọng đến sức khỏe, tâm sinh lý của giới trẻ.

Những thông tin xấu, độc tác động, làm lệch lạc về hành vi, suy nghĩ, tư tưởng, nhân cách sống của sinh viên, dẫn tới hậu quả khó lường, thậm chí là vi phạm pháp luật.

Giới trẻ sử dụng MXH như một công cụ để tìm kiếm tài liệu phục vụ học tập, trao đổi thông tin hữu ích, chia sẻ, kết nối bạn bè. Tuy nhiên trên mạng hiện nay có vô số thông tin, hình ảnh nội dung xấu, độc tác động, làm lệch lạc về hành vi, nhân cách sống của sinh viên, dẫn tới các hậu quả khó lường, các hành vi vi phạm pháp luật.

2.3. Một số cách thức nhận biết thông tin xấu, độc trên mạng xã hội

Thông tin xấu, độc có ảnh hưởng rất tiêu cực đến mọi người, đặc biệt là sinh viên, vì vậy, kỹ năng phân biệt, nhận diện thông tin xấu, độc là rất quan trọng. Một số kỹ năng khi tiếp cận thông tin trên không gian mạng cần chú ý kiểm tra, đánh giá thông tin đó là:

Một là, cần tuyệt đối cẩn trọng với những bài viết có nội dung giật gân, gây sốc. Vì những thông tin xấu, độc thường có tiêu đề, nội dung hấp dẫn, gây sốc, giật gân.

Hai là, chú ý đến đường dẫn liên kết. Cảnh giác trước các đường dẫn có dấu hiệu như: Lỗi chính tả, sai khác (lấy đường dẫn khác, nhưng tên website giống hệt), thiếu hoặc thừa một vài ký tự, hoặc thay thế một vài ký tự với ký tự khác gần giống (như “l” thay bằng “1”).

Ba là, kiểm chứng nguồn tin có phải là một cá nhân, tổ chức có uy tín cao, có phải là trang thông tin chính thống.

Bốn là, xác định đối tượng tán phát: Các thông tin bắt nguồn từ các đối tượng phản động chống đối, cá nhân thiếu hiểu biết.

Năm là, đánh giá về hình thức, nội dung: Tin tức xấu, độc hay bị lỗi chính tả hoặc có bố cục lộn xộn, các hình ảnh, video trong tin xấu, độc thường bị chỉnh sửa, cắt ghép, thay đổi nội dung, ngày tháng của sự kiện thường bị thay đổi. Nội dung chứa lỗi chính tả. Nguyên nhân là do các trang web giả mạo thường không kiểm duyệt kỹ nội dung.

Hoặc, các trang này được tạo bởi kẻ xấu ở nước ngoài mà họ không thành thạo ngôn ngữ được sử dụng để lừa đảo.

Sáu là, kiểm tra hình ảnh: Những thông tin xấu, độc thường chứa hình ảnh hoặc video bị chỉnh sửa. Đôi khi bức ảnh được các đối tượng cố tình đưa ra khỏi bối cảnh gốc gây nhầm lẫn, làm tưởng cho người xem.

2.4. Một số nghiên cứu có liên quan

Nhóm tác giả Trần Thị Hoan và Nguyễn Thị Nhung đã công bố đề tài “*Tìm hiểu một số tác động của mạng xã hội đối với sinh viên Việt Nam hiện nay*” [11]. Đề tài đã khảo sát, đánh giá thực trạng sử dụng MXH của sinh viên, từ đó chỉ rõ những tác động tích cực và tiêu cực của MXH đối với sinh viên.

Ở một khía cạnh cụ thể hơn về một MXH nhất định, tác giả Nguyễn Lan Nguyên đã nghiên cứu ảnh hưởng của việc sử dụng MXH Facebook đến sinh viên hiện nay [8]. Sau khi khảo sát và phân tích, nghiên cứu đã chỉ ra những ảnh hưởng tích cực và tiêu cực của MXH Facebook đối với sinh viên ở nhiều mặt, cụ thể: việc học tập, mối quan hệ với gia đình và bạn bè, hoạt động ngoại khóa, vấn đề việc làm.

Về khía cạnh định hướng dư luận sinh viên, nghiên cứu “*Ứng dụng mạng xã hội trong việc định hướng dư luận sinh viên tại các trường đại học ở Việt Nam*” [12] do nhóm tác giả Vũ Nhật Phương, Nguyễn Xuân Nhĩ, Trần Thanh Tùng, Trương Thị Lệ Hằng đã thực hiện trên đối tượng cụ thể là nhận thức, quan điểm, dư luận trong sinh viên khi sử dụng MXH. Nghiên cứu đã làm rõ được thực trạng sử dụng các MXH trong sinh viên hiện nay, sức ảnh hưởng của MXH đến quan điểm, nhân cách của sinh viên.

Qua tham khảo một số nghiên cứu có liên quan, nhóm nghiên cứu nhận thấy đa phần các đề tài đều làm rõ vấn đề về tác động, ảnh hưởng của MXH đối với sinh viên, nhưng chưa có bất kỳ đề tài nào nghiên cứu về thái độ của sinh viên tại TP.HCM về những thông tin xấu, độc trên MXH. Đề tài đã nghiên cứu, khảo sát và làm rõ được thái độ, nhận thức của sinh viên tại TP.HCM trước những thông tin xấu, độc trên MXH. Từ đó, đề xuất xây dựng mô hình Câu lạc bộ “phủ xanh thông tin” để khắc phục những hạn chế còn tồn tại.

3. Phương pháp nghiên cứu

3.1. Phương pháp nghiên cứu

Đề tài nghiên cứu dựa trên cơ sở phương pháp luận của chủ nghĩa Mác-Lênin, tư tưởng Hồ Chí Minh, chủ trương, đường lối chính sách của Đảng và pháp luật của Nhà nước. Ngoài ra, đề tài còn sử dụng một số phương pháp nghiên cứu cụ thể như sau:

Phương pháp thu thập thông tin: nhóm nghiên cứu tiến hành nghiên cứu, tham khảo những thông tin cần thiết có liên quan từ các nguồn tài liệu, khác nhau như: sách chuyên khảo, báo, tạp chí, đề tài, công trình khoa học của các nhà nghiên cứu, các

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

chuyên gia, v.v. Trên cơ sở đó, tiến hành chọn lọc và sử dụng những thông tin cần thiết vào việc phân tích, làm rõ các vấn đề đặt ra.

Phương pháp điều tra bằng bảng hỏi: Nhóm nghiên cứu sử dụng phương pháp điều tra bằng bảng hỏi trên mẫu gồm 300 sinh viên đang học tập tại các trường đại học, cao đẳng trên địa bàn TP.HCM để đánh giá thái độ của các bạn sinh viên trước những thông tin xấu, độc trên MXH.

Phương pháp phân tích, tổng hợp: Trên cơ sở các số liệu đã thu thập, xử lý, tác giả tiến hành phân tích, làm rõ thái độ của sinh viên tại TP.HCM trước những thông tin xấu, độc trên MXH.

Phương pháp dự báo khoa học: Trên cơ sở nghiên cứu tình hình, thực trạng, tác giả sử dụng phương pháp dự báo khoa học để chỉ ra các vấn đề có liên quan trong thời gian tới và đề xuất một số ý kiến nhằm nâng cao thái độ của sinh viên trên địa bàn TP.HCM trước những thông tin xấu, độc trên MXH.

3.2. Mẫu nghiên cứu

Nghiên cứu bao gồm 300 sinh viên đang học tập tại 06 trường đại học trên địa bàn TP.HCM, số lượng và tỉ lệ được minh họa cụ thể trong Bảng 1.

Bảng 1

Thống kê số lượng và tỉ lệ sinh viên tại mỗi trường trong mẫu nghiên cứu

Tên trường	Số lượng (sinh viên)	Tỉ lệ (%)
Trường Đại học An ninh nhân dân	60	20
Trường Đại học Cảnh sát nhân dân	40	13.3
Trường Đại học Khoa học Xã hội và Nhân văn	80	26.7
Trường Đại học Ngân hàng TP. HCM	50	16.7
Trường Đại học Công nghệ thông tin	40	13.3
Trường Đại học Sư phạm Kỹ thuật	30	10
Tổng	300	100

Nhóm tuổi có tỉ lệ cao nhất là từ 16 đến 20 tuổi (62.3%), sau đó là nhóm tuổi từ 21 đến 25 tuổi (36.3%) và thấp nhất là nhóm tuổi trên 26 tuổi (1.3%). Các bạn sinh viên tham gia khảo sát đa phần đang học năm 3 với tỉ lệ cao nhất là 42%, sau đó là năm 4 (22.7%) và năm 2 (20%); một số ít các bạn đang học năm 1 (9.3%) và ngoài năm 4 (6%) trong số lượng sinh viên tham gia vào nghiên cứu.

3.3. Cách thu thập và phân tích số liệu

Đề tài sử dụng bảng hỏi để khảo sát thu thập số liệu. Nhóm nghiên cứu thiết kế bảng hỏi trên Google Form (một nền tảng tạo và thực hiện khảo sát). Liên kết (Link)

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

dẫn đến bảng khảo sát đã được gửi đến các bạn sinh viên trong khoảng thời gian từ ngày 01/8/2023 đến ngày 15/8/2023 để tiến hành khảo sát và thu thập số liệu.

Sau khi đã thu thập được số liệu khảo sát, nhóm nghiên cứu sử dụng phần mềm thống kê và phân tích dữ liệu (SPSS phiên bản 20) để hỗ trợ quá trình phân tích.

4. Kết quả nghiên cứu và thảo luận

4.1. Kết quả nghiên cứu

4.1.1. Mức độ sử dụng mạng xã hội của sinh viên tại Thành phố Hồ Chí Minh

Thứ nhất, về câu hỏi “Các MXH bạn đang sử dụng là gì?”, kết quả thu thập được phân tích và trình bày trong Bảng 2.

Bảng 2

Kết quả phân tích số liệu về câu hỏi: “Các MXH bạn đang sử dụng là gì?”

	Phản hồi		Tỷ lệ phần trăm so với cỡ mẫu
	Tần suất	Phần trăm	
Facebook	280	25.9%	93.3%
Tiktok	206	19.0%	68.7%
Zalo	266	24.6%	88.7%
Instagram	211	19.5%	70.3%
X (Twitter)	70	6.5%	23.3%
Telegram	49	4.5%	16.3%
Tổng	1082	100.0%	360.7%

Từ số liệu trên cho thấy sinh viên trên địa bàn TP.HCM sử dụng đa dạng các MXH. Tất cả sinh viên được khảo sát đều sử dụng một hoặc nhiều hơn những MXH này. Trong đó, có 04 MXH được hầu hết các bạn sinh viên lựa chọn là Facebook, Tiktok, Zalo và Instagram. Số lượng sinh viên sử dụng 04 MXH này chiếm tỉ lệ rất cao, đều trên 70% và đặc biệt trong đó là MXH Facebook được đông đảo sinh viên sử dụng nhất với 280 trên tổng số 300 sinh viên, chiếm tỉ lệ 93,3%.

Thứ hai, khi được hỏi: “Bạn dành bao nhiêu giờ một ngày để sử dụng MXH?”, kết quả khảo sát như Bảng 3.

Bảng 3

Kết quả phân tích số liệu về câu hỏi: “Bạn dành bao nhiêu giờ một ngày để sử dụng MXH?”

	Tần suất	Phần trăm	Tỷ lệ phần trăm trên các giá trị hợp lệ	Tỷ lệ phần trăm tích lũy trên các giá trị hợp lệ
Từ 1 đến 3 giờ	112	37.3%	37.3%	37.3%
Từ 4 đến 6 giờ	152	50.7%	50.7%	88.0%
Từ 7 đến 9 giờ	29	9.7%	9.7%	97.7%
Từ 10 giờ trở lên	7	2.3%	2.3%	100.0%
Tổng	300	100.0%	100.0%	

Từ kết quả khảo sát trong Bảng 3 có thể thấy sinh viên dành khá nhiều thời gian một ngày để sử dụng MXH. Với tỷ lệ cao nhất, có đến 152 sinh viên (50.7%) dành từ 4 đến 6 giờ một ngày để sử dụng MXH. Kế đến là 112 sinh viên (37.3%) dành từ 1 đến 3 giờ một ngày để sử dụng MXH. Thời gian sử dụng trên 7 giờ một ngày chiếm tỷ lệ rất thấp. Qua đó, có thể thấy, các bạn sinh viên dành tương đối nhiều thời gian sử dụng MXH.

Thứ ba, nghiên cứu khảo sát mục đích sử dụng MXH của sinh viên tại TP.HCM và nhận được kết quả như Bảng 4.

Bảng 4

Kết quả phân tích số liệu về câu hỏi: “Bạn sử dụng MXH cho những mục đích gì?”

	Phản hồi		Tỷ lệ phần trăm so với cơ mẫu
	Tần suất	Phần trăm	
Học tập, nghiên cứu tài liệu, thu thập thông tin phục vụ cho việc học	222	24.9%	74.0%
Kết nối với bạn bè, người thân, làm quen bạn mới	211	23.7%	70.3%
Giải trí (xem phim, nghe nhạc, v.v.)	216	24.3%	72.0%
Để xây dựng hình ảnh bản thân để nhiều người biết đến	83	9.3%	27.7%
Cập nhật thông tin, tin tức, v.v.	158	17.8%	52.7%
Tổng	890	100.0%	296.7%

Quan sát bảng 4 cho thấy, sinh viên trên địa bàn TP.HCM sử dụng các ứng dụng MXH với đa dạng mục đích khác nhau như học tập, nghiên cứu, giải trí, kết bạn, cập

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

nhật tin tức, v.v. Trong đó, mục đích được sinh viên lựa chọn nhiều nhất là học tập, nghiên cứu tài liệu, thu thập thông tin phục vụ việc học với 222 sinh viên trên tổng số 300 sinh viên, chiếm tỉ lệ 74.0%. Một mục đích khác cũng được nhiều sinh viên lựa chọn đó chính là kết nối với bạn bè, người thân, làm quen bạn mới với 211 sinh viên trên tổng số 300 sinh viên, chiếm tỉ lệ 70.3%. Hơn nữa, câu hỏi nhận được một số câu trả lời mục đích khác như: mua sắm trực tuyến hoặc bán hàng trực tuyến.

Cuối cùng, khảo sát về mức độ hữu ích của MXH đối với sinh viên, câu hỏi được xây dựng trên thang Likert với 05 mức độ (từ 1 đến 5) tương ứng với từ “Rất hữu ích” đến “Rất không hữu ích”, nhóm nghiên cứu nhận được kết quả phân tích như Bảng 5.

Bảng 5

Kết quả phân tích số liệu về câu hỏi: “Bạn đánh giá MXH có hữu ích không?”

Question	Number (Số lượng)	Mean (Giá trị trung bình)	Median (Trung vị)	Std. Deviation (Độ lệch chuẩn)	Minimum (Giá trị nhỏ nhất)	Maximum (Giá trị lớn nhất)
Bạn đánh giá MXH có hữu ích không.	300	2.05	2.00	1.084	1	5

	Tần suất	Phần trăm
Rất hữu ích	110	36.7%
Hữu ích	114	38.0%
Bình thường	39	13.0%
Không hữu ích	26	8.7%
Rất không hữu ích	11	3.7%
Tổng	300	100.0%

Quan sát Bảng 5, với giá trị trung bình các câu trả lời (Mean) là 2.05, có nghĩa đa số sinh viên đánh giá MXH khá hữu ích với bản thân. Hơn nữa, giá trị trung vị (Median) là 2 cho thấy đa số sinh viên đồng ý rằng MXH là hữu ích. Có đến 74.7% tương ứng 224 sinh viên đánh giá MXH Hữu ích đến Rất hữu ích. Từ đó thấy được MXH mang đến rất nhiều lợi ích, hỗ trợ sinh viên rất nhiều trong học tập và cuộc sống.

4.1.2. Thái độ của sinh viên tại Thành phố Hồ Chí Minh trước những thông xấu, độc trên mạng xã hội

Để khảo sát về tần suất tiếp xúc với các tin xấu, độc của sinh viên tại TP.HCM, nhóm nghiên cứu sử dụng câu hỏi “Bạn có thường bắt gặp những thông tin chứa nội dung xấu, độc trên MXH không?”. Và câu trả lời sẽ là 4 mức độ: Hiếm khi, gần như

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

không gặp phải; Thỉnh thoảng; Thường xuyên; Rất thường xuyên. Kết quả khảo sát được phân tích và thể hiện qua Bảng 6.

Bảng 6

Kết quả phân tích số liệu về câu hỏi: “Bạn có thường bắt gặp những thông tin chứa các nội dung chứa nội dung xấu, độc trên MXH không?”

	Tần suất	Phần trăm	Tỉ lệ phần trăm trên các giá trị hợp lệ	Tỉ lệ phần trăm tích lũy trên các giá trị hợp lệ
Hiếm khi, gần như không	10	3.3	3.3%	3.3%
Thỉnh thoảng	110	36.7	36.7%	40.0%
Thường xuyên	106	35.3	35.3%	75.3%
Rất thường xuyên	74	24.7	24.7%	100.0%
Tổng	300	100.0	100.0%	

Quan sát Bảng 6, có thể thấy sinh viên tại TP.HCM khá thường xuyên tiếp xúc với những tin xấu, độc trên MXH với kết quả khi được hỏi, có 110 sinh viên trả lời thỉnh thoảng bắt gặp những tin xấu, độc (chiếm 36.7%), xấp xỉ sau đó là 106 sinh viên trả lời thường xuyên (chiếm 35.3%); và thấp hơn là mức độ Rất thường xuyên với 74 sinh viên (chiếm 24.7%). Và chỉ có 10 sinh viên (chiếm 3,3%) hiếm khi, gần như không bắt gặp. Như vậy, sinh viên tại TP.HCM tiếp xúc với các tin xấu, độc là khá thường xuyên, và đây là một mối nguy cơ rất lớn có thể gây ra những tác động tiêu cực.

Đứng trước mối nguy cơ khá nguy hiểm đó, nhóm nghiên cứu đặt ra câu hỏi “Bạn nghĩ bản thân có khả năng nhận biết các thông tin chứa nội dung xấu, độc trên MXH không?” để khảo sát kỹ năng nhận diện những thông tin xấu, độc trên MXH của sinh viên tại TP.HCM và câu trả lời với ba mức độ: Gần như không thể; Phân vân, đôi lúc có thể nhận biết, hoặc không; Có thể nhận biết. Và kết quả sau phân tích thể hiện tại Bảng 7.

Bảng 7

Kết quả phân tích số liệu về câu hỏi: “Bạn nghĩ bản thân có khả năng nhận biết các thông tin chứa nội dung xấu, độc trên MXH không?”

	Tần suất	Phần trăm	Tỉ lệ phần trăm trên các giá trị hợp lệ	Tỉ lệ phần trăm tích lũy trên các giá trị hợp lệ
Gần như không thể	58	19.3	19.3	19.3
Phân vân, đôi lúc có thể nhận biết, hoặc không	109	36.3	36.3	55.7
Có thể nhận biết	133	44.3	44.3	100.0
Tổng	300	100.0	100.0	

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Từ Bảng 7, có thể thấy một điều rất khả quan, số lượng sinh viên có thể nhận biết, phân biệt tin xấu, độc trên MXH chiếm tỉ lệ cao nhất, với 133 sinh viên (44.3%). Nhưng vẫn còn hơn 50% các bạn vẫn còn phân vân hoặc thậm chí là không thể nhận biết, cụ thể: 109 sinh viên phân vân, hoặc có thể hoặc không thể nhận biết (36.3%) và có đến 53 sinh viên gần như không thể nhận biết (19.3%). Con số này đang rất đáng báo động về kỹ năng nhận biết, phân biệt tin xấu, độc để tự bảo vệ bản thân của sinh viên tại TP.HCM.

Câu hỏi “Thái độ của bạn đối với các thông tin chứa nội dung xấu, độc trên MXH” với câu trả lời được xây dựng trên thang Likert với 05 mức độ từ 1 đến 5 tương ứng với mức độ tăng dần từ “Thờ ơ, không quan tâm” đến “Rất bức xúc” nhằm khảo sát thái độ của sinh viên tại TP.HCM về những thông tin xấu, độc trên MXH. Kết quả sau phân tích thể hiện tại Bảng 8.

Bảng 8

Kết quả phân tích số liệu về câu hỏi: “Thái độ của bạn đối với các thông tin chứa nội dung xấu, độc trên MXH.”

Question	Number (Số lượng)	Mean (Giá trị trung bình)	Median (Trung vị)	Std. Deviation (Độ lệch chuẩn)	Minimum (Giá trị nhỏ nhất)	Maximum (Giá trị lớn nhất)
Thái độ của bạn đối với các thông tin chứa nội dung xấu, độc trên MXH.	300	3.34	3.00	1.253	1	5

	Tần suất	Phần trăm
1	31	10.3%
2	45	15.0%
3	78	26.0%
4	83	27.7%
5	63	21.0%
Tổng	300	100.0%

Quan sát Bảng 8, giá trị trung bình (Mean) là 3.34 tương ứng với mức độ Trung lập, có nghĩa là thái độ của đa số sinh viên tại TP.HCM về những thông tin xấu, độc trên MXH là Trung lập. Từ giá trị nhỏ nhất (Min) là 1 cho đến giá trị lớn nhất (Max) là 5 cho

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

thấy sự đa dạng trong câu trả lời của sinh viên. Có 146 sinh viên (48.7%) có thái độ trên mức trung lập (Bức xúc và Rất bức xúc). Tuy nhiên, có 154 sinh viên (51.3%) có thái độ Trung lập và dưới mức trung lập (Thờ ơ và Rất thờ ơ) với những thông tin xấu, độc trên MXH. Có thể các bạn vẫn chưa nhận thức rõ được ảnh hưởng tiêu cực của các thông tin xấu, độc đó.

Khi khảo sát về kỹ năng xác thực tính xác đáng, đáng tin cậy của thông tin, nhóm khảo sát đã đặt ra câu hỏi “Để xác minh tính xác thực của một nội dung trên MXH, bạn thường làm gì?” và nhận được kết quả qua phân tích như Bảng 9.

Bảng 9

Kết quả phân tích số liệu về câu hỏi: “Để xác minh tính xác thực của một nội dung trên MXH, bạn thường làm gì?”

	Phản hồi		Tỷ lệ phần trăm so với cỡ mẫu
	Tần suất	Phần trăm	
Không biết cách để xác minh tính xác thực của thông tin	69	9.9%	23.2%
Đi hỏi bạn bè, người thân	86	12.4%	29.0%
Đi hỏi những người có liên quan đến thông tin đó (Người có liên quan, xuất hiện trong vụ việc, thông tin đó, v.v.)	75	10.8%	25.3%
Cẩn thận kiểm tra hình ảnh, thời gian, địa điểm để xác minh tính xác thực của thông tin	168	24.2%	56.6%
Vào bình luận để xem mọi người bàn tán thế nào về nội dung đó	147	21.2%	49.5%
Xem người đăng tin, cơ quan, tổ chức, nhóm đăng tin có đáng tin, chính thống không	149	21.5%	50.2%
Tổng	694	100.0%	233.7%

Quan sát Bảng 9 cho thấy, sinh viên trên địa bàn TP.HCM có sự cẩn thận nhất định trước những thông tin trên MXH thông qua đa dạng cách thức để xác minh tính xác thực của thông tin đó. Trong đó, sinh viên lựa chọn nhiều nhất đối việc cẩn thận kiểm tra hình ảnh, thời gian, địa điểm để xác minh tính xác thực của thông tin với 168 sinh viên trên tổng số 300 sinh viên (56,6%). Tiếp theo sinh viên có thể xác minh tính xác thực của thông tin thông qua việc xem người đăng tin, cơ quan, tổ chức, nhóm đăng tin có đáng tin không, chính thống không với 149 sinh viên trên tổng số 300 sinh viên (50,2%). Một cách thức xác minh tính xác thực của thông tin được đa số sinh viên lựa chọn là vào bình luận để xem mọi người bàn tán thế nào về nội dung đó với 147 sinh viên trên tổng số 300 sinh viên (49,5%). Sinh viên còn lựa chọn đi hỏi bạn bè, người

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

thân hoặc đi hỏi những người có liên quan đến thông tin đó để xác minh tính xác thực của thông tin, tuy nhiên hiệu quả xác thực của 02 cách thức trên không đáng kể, thậm chí có thể gây hoang mang cho một bộ phận sinh viên khi tiếp thu quá nhiều ý kiến, nhận xét về thông tin cần được xác thực. Bên cạnh đó cũng có một số sinh viên không biết cách để xác minh tính xác thực của thông tin, đây là một điểm cần chú ý.

Khi được khảo sát về hành động của sinh viên khi gặp phải một thông tin nóng, giật gân nhưng bạn không biết đó có phải là thông tin đúng sự thật, thông tin hữu ích không, nhóm nghiên cứu nhận được kết quả sau phân tích như Bảng 10.

Bảng 10

Kết quả phân tích số liệu về câu hỏi: “Hành động của bạn khi gặp phải một thông tin nóng, giật gân nhưng bạn không biết đó có phải là thông tin đúng sự thật, thông tin hữu ích không”.

	Phản hồi		Tỷ lệ phần trăm so với cỡ mẫu
	Tần suất	Phần trăm	
Nhanh chóng chia sẻ để "câu" tương tác, nếu có sai thì xóa, không sao cả	40	8.5%	13.5%
Chia sẻ cho hội bạn thân, những nhóm chung để mọi người cùng "hóng hớt"	70	14.9%	23.6%
Nghi ngờ, đặt câu hỏi nhưng không biết phải làm gì, cứ lướt qua	105	22.3%	35.4%
Nghi ngờ, đặt câu hỏi, cố gắng tìm hiểu xác thực thông tin	137	29.1%	46.1%
Nếu là tin giả, chia sẻ tính xác thực cho mọi người, báo cáo với quản trị viên của MXH	119	25.3%	40.1%
Tổng	471	100.0%	158.6%

Quan sát Bảng 10 cho thấy, sinh viên trên địa bàn TP.HCM có những hành động khác nhau khi gặp phải một thông tin nóng, giật gân và họ không biết đó có phải là thông tin đúng sự thật, hữu ích không. Trong đó, hành động được nhiều sinh viên lựa chọn nhất là nghi ngờ, đặt câu hỏi, cố gắng tìm cách xác thực thông tin với 137 sinh viên trên tổng số 300 sinh viên (46.1%). Tiếp đến là hành động chia sẻ tính xác thực cho mọi người nếu là tin giả và báo cáo quản trị viên của MXH cũng được đông đảo sinh viên lựa chọn với 119 sinh viên trên tổng số 300 sinh viên (40,1%). Hành động nghi ngờ, đặt câu hỏi nhưng không biết phải làm gì, cứ lướt qua thể hiện sự thờ ơ, vô cảm của sinh viên trước một thông tin chưa biết đúng sai được 105 sinh viên trên tổng số 300 sinh

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

viên lựa chọn (35,4%). Bên cạnh những hành động tích cực hoặc thờ ơ, sinh viên còn có những hành động tiêu cực như chia sẻ để “câu” tương tác, chia sẻ cho nhóm bạn thân, những nhóm chơi chung để mọi người cùng “hóng hót”. Những hành động tiêu cực này làm thông tin đó càng ngày càng phức tạp, nghiêm trọng và những người chia sẻ thông tin ấy có thể đã vô tình thực hiện hành vi vi phạm pháp luật.

Để nghiên cứu về những khó khăn trong việc đưa ra hành động của sinh viên trước những thông tin xấu, độc trên MXH, nhóm nghiên cứu sử dụng câu hỏi “Bạn gặp phải những khó khăn gì trong việc đưa ra hành động khi gặp những thông tin chứa nội dung xấu, độc?” và nhận được kết quả như Bảng 11.

Bảng 11

Kết quả phân tích số liệu về câu hỏi: “Bạn gặp phải những khó khăn gì trong việc đưa ra hành động khi gặp những thông tin chứa nội dung xấu, độc?”

	Phản hồi		Tỷ lệ phần trăm so với cỡ mẫu
	Tần suất	Phần trăm	
Thiếu nguồn tin chính thống, xác thực	152	22.8%	51.0%
Trình độ lý luận chính trị, nhận thức chính trị, kiến thức của bản thân còn hạn chế hạn chế	111	16.7%	37.2%
Sợ tốn nhiều thời gian	80	12.0%	26.8%
Ngại chia sẻ thông tin trên MXH	108	16.2%	36.2%
Ngại dự luận, sợ bị công kích	93	14.0%	31.2%
Sợ bị trả thù	62	9.3%	20.8%
Không thể nhận biết đâu là thông tin độc hại	60	9.0%	20.1%
Tổng	666	100.0%	223.5%

Quan sát Bảng 11 cho thấy, sinh viên trên địa bàn TP.HCM đã có nhiều khó khăn khác nhau trong việc đưa ra hành động khi gặp những thông tin chứa nội dung xấu, độc. Khó khăn lớn nhất được sinh viên đánh giá là thiếu nguồn tin chính thống, xác thực với 152 sinh viên trên tổng số 300 sinh viên (51%). Khó khăn về trình độ lý luận chính trị, nhận thức chính trị, kiến thức của bản thân còn hạn chế cũng được nhiều bạn sinh viên lựa chọn với 111 trên tổng số 300 sinh viên (37,2%). Khó khăn về thời gian cũng là trở ngại lớn để các bạn sinh viên đưa ra hành động khi gặp những thông tin có nội dung xấu, độc với 108 sinh viên lựa chọn (36,2%). MXH là một môi trường hết sức phức tạp vì vậy các bạn sinh viên thường ngại chia sẻ những thông tin xấu, độc, ngại dự luận, sợ bị công kích hoặc sợ bị trả thù cũng chính là những khó khăn đối với các bạn sinh viên trong việc

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

đưa ra các hành động khi gặp những thông tin sai lệch, xấu, độc. Không những thế, tỉ lệ sinh viên không thể nhận biết đâu là thông tin độc hại vẫn có tồn tại với 60 sinh viên trên tổng số 300 sinh viên, chiếm tỉ lệ 20.1%, đây là một con số đáng chú ý.

Cuối cùng, khi khảo sát nhận thức của sinh viên về tác động của thông tin xấu, độc, nghiên cứu nhận được kết quả như Bảng 12.

Bảng 12

Kết quả phân tích số liệu về câu hỏi: “Bạn nghĩ những thông tin xấu, độc sẽ ảnh hưởng thế nào đến bản thân bạn nói riêng cũng như sinh viên tại TP.HCM nói chung?”

	Phản hồi		Tỷ lệ phản
	Tần suất	Phần trăm	trăm so với cỡ mẫu
Không có ảnh hưởng gì, chỉ là một bài viết trên MXH	41	4.7%	13.7%
Gây hoang mang, nghi ngờ	152	17.3%	50.7%
Gây mất niềm tin vào Đảng, Nhà nước, chính quyền	142	16.2%	47.3%
Gây ảnh hưởng xấu đến tinh thần	154	17.5%	51.3%
Có thể dẫn đến các hành vi vi phạm pháp luật	137	15.6%	45.7%
Tốn nhiều thời gian để quan tâm đến những thông tin đó	108	12.3%	36.0%
Ảnh hưởng đến nhận thức về chính trị, tư tưởng, suy nghĩ	144	16.4%	48.0%
Tổng	878	100.0%	292.7%

Quan sát Bảng 12 cho thấy, sinh viên trên địa bàn TP.HCM đã nhận thức được những ảnh hưởng của những thông tin xấu, độc đối với bản thân. Ảnh hưởng được nhiều sinh viên lựa chọn nhất là gây ảnh hưởng xấu đến tinh thần với 154 sinh viên trên tổng số 300 sinh viên (51,3%). Cùng với gây ảnh hưởng xấu đến tinh thần thì gây hoang mang, nghi ngờ cũng chiếm tỉ lệ rất cao, cụ thể là 50,7% với 152 sinh viên lựa chọn. Nhiều sinh viên còn cho rằng những thông tin xấu, độc còn ảnh hưởng đến nhận thức về chính trị, tư tưởng, suy nghĩ và gây mất niềm tin vào Đảng, Nhà nước và chính quyền được cụ thể hóa thông qua có hơn 140 lựa chọn của sinh viên cho mỗi ảnh hưởng (47.3%). Không những thế, sinh viên còn nhận thấy ảnh hưởng không tốt của các thông tin xấu, độc là có thể dẫn đến vi phạm pháp luật với 137 sinh viên lựa chọn (45,7%). Bên cạnh việc nhận thức rõ ảnh hưởng không tốt, một bộ phận sinh viên không nhận thức được tác hại của thông tin xấu, độc hoặc bỏ qua, không quan tâm những thông tin này do tốn nhiều thời gian.

4.2. Thảo luận

MXH ngày càng trở nên phổ biến và có vai trò quan trọng trong các hoạt động xã hội. Sự phát triển ồ ạt của nhiều MXH khiến sinh viên càng có cơ hội tham gia vào thế giới thông tin với kết nối rộng lớn, cùng lúc tiếp cận với nhiều hệ tư tưởng và giá trị sống khác nhau. Tuy nhiên, với khối lượng thông tin lớn chưa qua kiểm duyệt được tung lên MXH mỗi ngày ảnh hưởng thế nào đến lối sống của sinh viên hiện nay. Qua kết quả khảo sát thái độ của sinh viên trên địa bàn TPHCM trước những thông tin có nội dung xấu, độc trên MXH, nhóm nghiên cứu đã nhận thấy sinh viên có những điểm mạnh và điểm yếu nhất định.

** Điểm mạnh:*

Sử dụng MXH là một nhu cầu tất yếu đối với giới trẻ, trong đó có sinh viên. Ngày nay, chỉ với một chiếc điện thoại, một máy tính bảng hay máy tính cá nhân có kết nối Internet là sinh viên có thể tham gia vào MXH. Với nội dung phong phú và cách thức sử dụng dễ dàng, MXH mang lại nhiều tiện ích đối với sinh viên trong học tập cũng như cuộc sống. Kết quả này tương tự với lý thuyết của PGS. TS. Mai Đức Ngọc [6] đã đề cập trong phần 1.

Một là, sinh viên đã khai thác tối đa các tiện ích từ MXH mang lại như: dễ dàng khai thác thông tin, tìm kiếm tài liệu phục vụ hiệu quả cho việc học, mở rộng giao lưu, kết nối không giới hạn về không gian và thời gian, v.v. Với tốc độ nhanh chóng, chỉ cần vài thao tác đơn giản, sinh viên có thể dễ dàng nhận được những thông tin cập nhật về lĩnh vực, vấn đề mà họ quan tâm. Với sự ra đời của Internet và MXH, giao tiếp giữa con người với con người được mở rộng và kết nối nhanh chóng. Từ đó, có thể xem MXH là hình thức giao tiếp tiên tiến, chi phí thấp, hiệu quả cao cho tất cả mọi người, đặc biệt là sinh viên. Và kết quả nghiên cứu này khá tương đồng với kết quả nghiên cứu về các tác động tích cực của MXH đối với sinh viên của đề tài nhóm tác giả Trần Thị Hoan và Nguyễn Thị Nhung [11] đã được đề cập ở mục 2.4 của nghiên cứu này.

Hai là, sinh viên gặp những thông tin xấu độc khá thường xuyên trên MXH và một bộ phận họ có thể nhận biết và thể hiện thái độ bức xúc trước những thông tin đó. Từ kết quả nghiên cứu, nhóm nghiên cứu nhận thấy sinh viên trên địa bàn TP.HCM đã có sự cẩn thận nhất định trước những thông tin trên MXH và trước những thông tin xấu độc, sinh viên đã thể hiện thái độ bức xúc, tuy nhiên số lượng sinh viên thể hiện thái độ trung lập và thờ ơ vẫn còn tồn tại. Đây là điểm mới mà nghiên cứu này đã khảo sát và làm rõ.

Ba là, sinh viên có những cách thức khác nhau để xác minh tính xác thực của thông tin trên MXH và nhận thức được những ảnh hưởng của thông tin xấu độc tác động đến sinh viên. Trước những thông tin xấu độc trên MXH, sinh viên đã có sự xem xét, đánh giá, tìm cách để xác minh tính xác thực của thông tin, tuy nhiên, có những cách

thức chưa phù hợp, chưa đem lại hiệu quả. Những thông tin xấu độc đã có những tác động nhất định đến sinh viên và hầu hết họ đều nhận thức được ảnh hưởng tiêu cực của những thông tin xấu độc mang đến.

**Điểm yếu:*

Một là, khả năng nhận diện thông tin xấu, độc, kỹ năng xác thực thông tin trên MXH của sinh viên còn nhiều hạn chế. MXH là nơi giao lưu, kết bạn dễ dàng và nhanh chóng, giúp sinh viên thuận tiện hơn trong việc liên lạc, trao đổi thông tin, tài liệu. Tuy nhiên, đây chính là thời cơ để các thế lực thù địch lợi dụng MXH để tiếp cận, “tiêm nhiễm” tư tưởng độc hại vào sinh viên, nhằm làm tha hóa đạo đức, lối sống, lý tưởng của sinh viên để dễ bề dụ dỗ, lôi kéo họ tham gia vào các hoạt động chống phá. Thêm vào đó, sinh viên tiếp cận với những thông tin xấu, độc rất thường xuyên. Đứng trước những thông tin giật gân, thông tin nóng, sinh viên còn khá vội vàng khi tiếp cận với nó, một số ít đã nhanh chóng chia sẻ mà không cần thực hiện bất kỳ bước xác minh nào; một số khác thì vẫn cẩn trọng nhưng rất thờ ơ để thông tin tồn tại trên MXH; số khác thì có các cách xác thực chưa đúng, còn nhiều hạn chế.

Hai là, phần lớn sinh viên có thái độ thờ ơ, không quan tâm đến những thông tin xấu, độc trên MXH. Việc thường xuyên tiếp xúc nhưng có thái độ thờ ơ, không quan tâm, không cảnh giác là một mối nguy cơ rất lớn có thể tác động tiêu cực đến bản thân của sinh viên. Sự thờ ơ đó còn làm cho nạn phát tán tin xấu, độc nhắm tới sinh viên ngày càng phát triển mạnh mẽ, tinh vi, nguy hiểm. Cần lắm sự hành động, thái độ tích cực trong việc ngăn chặn, phòng ngừa thông tin xấu, độc và tác động tiêu cực của nó.

Ba là, vẫn còn một bộ phận sinh viên không nhận thức rõ được tác hại, ảnh hưởng tiêu cực của thông tin xấu, độc đối với bản thân mình. Thông tin xấu, độc tác động rất nhiều đến học tập, đời sống, tinh thần, suy nghĩ, tư tưởng và hành động của sinh viên theo chiều hướng tiêu cực. Việc nhận thức rõ ảnh hưởng, tác động đó có vai trò rất quan trọng trong phòng ngừa, cảnh giác trước những thông tin xấu, độc. Thế nhưng, vẫn còn một bộ phận sinh viên chưa nhận thức rõ về tác hại, ảnh hưởng xấu của thông tin xấu, độc đối với bản thân sinh viên cũng như cộng đồng.

Bốn là, có nhiều khó khăn cản trở sinh viên trong việc đưa ra hành động khi gặp những thông tin xấu, độc như trình độ lý luận chính trị, nhận thức chính trị còn hạn chế; ngại chia sẻ trên MXH, ngại dư luận, sợ bị công kích, sợ bị trả thù; thiếu nguồn thông tin chính thống,...

5. Kết luận và gợi ý:

5.1. Kết luận

Từ việc khảo sát thái độ của sinh viên tại TP.HCM về những thông tin xấu, độc trên MXH, nhóm nghiên cứu rút ra một số kết luận sau:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Một là, MXH phát triển rất mạnh mẽ, sinh viên tiếp cận, sử dụng MXH với đa dạng mục đích; thời gian sinh viên dành cho việc sử dụng MXH là khá nhiều; sinh viên đánh giá MXH hữu ích đối với bản thân, công việc và cuộc sống của họ.

Hai là, thái độ của sinh viên tại TP.HCM với những thông tin xấu, độc trên MXH có rất nhiều điểm tích cực: sinh viên đã khai thác tối đa các tiện ích từ MXH mang lại; sinh viên gặp những thông tin xấu độc khá thường xuyên trên MXH và một bộ phận có thể nhận biết và thể hiện thái độ bức xúc trước những thông tin đó; sinh viên có những cách thức khác nhau để xác minh tính xác thực của thông tin trên MXH và nhận thức được những ảnh hưởng của thông tin xấu độc tác động đến sinh viên.

Ba là, tuy nhiên, vẫn còn tồn tại rất nhiều hạn chế trong thái độ của sinh viên tại TP.HCM về những thông tin xấu, độc trên MXH, cụ thể: khả năng nhận diện thông tin xấu, độc, kỹ năng xác thực thông tin trên MXH của sinh viên còn nhiều hạn chế; phần lớn sinh viên có thái độ thờ ơ, không quan tâm đến những thông tin xấu, độc trên MXH; vẫn còn một bộ phận sinh viên không nhận thức rõ được tác hại, ảnh hưởng tiêu cực của thông tin xấu, độc đối với bản thân mình; có nhiều khó khăn cản trở sinh viên trong việc đưa ra hành động khi gặp những thông tin xấu, độc.

5.2. Đề xuất về xây dựng mô hình Câu lạc bộ “phủ xanh thông tin” trong các trường Đại học tại TP.HCM

Thái độ của sinh viên tại TP.HCM về những thông tin xấu, độc trên MXH vẫn còn tồn tại rất nhiều hạn chế. Nhằm nâng cao thái độ của sinh viên TP.HCM về những thông tin xấu, độc trên MXH theo một chiều hướng tích cực, nhóm nghiên cứu đề xuất mô hình Câu lạc bộ “phủ xanh thông tin” để khắc phục, giải quyết những tồn tại còn hạn chế.

5.2.1. Mục tiêu của Câu lạc bộ “phủ xanh thông tin”

- Nâng cao nhận thức, tư tưởng chính trị cho sinh viên.
- Nâng cao nhận thức, kỹ năng nhận diện, xác thực thông tin cho sinh viên.
- Nâng cao nhận thức về tác động tiêu cực của những thông tin xấu, độc trên MXH cho sinh viên.
- Nâng cao hiệu quả học tập những môn lý luận chính trị (Triết học, Kinh tế chính trị, Chủ nghĩa xã hội khoa học, Tư tưởng Hồ Chí Minh, Lịch sử Đảng, v.v.).
- Mỗi sinh viên sẽ là một “ngòi bút sắc bén” trong công cuộc nhận diện, đấu tranh, phản bác, ngăn chặn những thông tin xấu, độc trên MXH; “phủ xanh thông tin”, đưa thông tin chính thống, xác thực đến với tất cả sinh viên nói riêng và người dùng MXH nói chung một cách nhanh chóng, đầy đủ, kịp thời, chính xác, đẩy lùi nạn thông tin xấu, độc.

5.2.2. Những hoạt động trọng tâm

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Phối hợp với các khoa, viện, phòng, đơn vị chức năng tổ chức các buổi sinh hoạt, tuyên truyền, nâng cao nhận thức của sinh viên tại trường; các cuộc thi tìm hiểu, nhận diện, đấu tranh, v.v.

- Nâng cao hiệu quả học tập những môn lý luận chính trị (Triết học, Kinh tế chính trị, Chủ nghĩa xã hội khoa học, Tư tưởng Hồ Chí Minh, Lịch sử Đảng, v.v.) bằng các cuộc thi tìm hiểu, hoạt động hỗ trợ học tập, đổi mới hình thức giáo dục các môn Lý luận chính trị nhằm tạo hứng thú học tập, v.v.

- Phối hợp với các khoa, viện, phòng, đơn vị chức năng tuyên truyền, phổ biến, nâng cao nhận thức của người dùng MXH về thông tin xấu, độc bằng đa dạng các hình thức khác nhau: bằng những bài viết trên MXH, các đoạn phim ngắn trên TikTok, những cuộc thi tìm hiểu, v.v.

- Xây dựng, quản lý các trang MXH dễ tiếp cận đến sinh viên như: Facebook, TikTok, Instagram, v.v. để đăng tải, đưa thông tin chính thống, xác thực đến với tất cả sinh viên nói riêng và người dùng MXH nói chung một cách nhanh chóng, đầy đủ, kịp thời, chính xác, đẩy lùi nạn thông tin xấu, độc. Đồng thời sử dụng những trang MXH này để đấu tranh, phản bác, ngăn chặn, xóa bỏ các thông tin xấu, độc trên MXH; tuyên truyền, nâng cao nhận thức của sinh viên và người dùng MXH.

LỜI CẢM ƠN

Để thực hiện và hoàn thành đề tài nghiên cứu khoa học này, nhóm nghiên cứu đã nhận được sự hỗ trợ, giúp đỡ từ nhiều cơ quan, tổ chức và cá nhân. Nghiên cứu khoa học cũng được hoàn thành dựa trên sự tham khảo, học tập kinh nghiệm từ các kết quả nghiên cứu liên quan, các sách, báo chuyên ngành của nhiều tác giả. Tuy có nhiều cố gắng, nhưng đề tài khó tránh khỏi những thiếu sót, nhóm nghiên cứu mong muốn nhận được sự đóng góp để đề tài hoàn thiện hơn.

TÀI LIỆU THAM KHẢO

- Chính phủ (2013). *Nghị định số 72/2013/NĐCP ngày 15/3/2013 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng*. Hà Nội.
- Gardner, R. C. (1985). *Social Psychology and Second Language Learning: The Role of Attitudes and Motivation*. London: Edward Arnold. Retrieved from <https://doi.org/10.1037/h0083787>
- Garret, P. (2010). *Attitudes to Language*. Cambridge: Cambridge University Press. Retrieved from <http://dx.doi.org/10.1017/CBO9780511844713>
- Hoàng, P. (2019). *Từ điển Tiếng Việt*. Hồng Đức.
- Kara, A. (2009) The Effect of a ‘Learning Theories’ Unit on Students’ Attitudes towards Learning. *Australian Journal of Teacher Education*, 34, 100-113. Retrieved from <https://doi.org/10.14221/ajte.2009v34n3.5>
- Mai, Đ. N. (2021). *Định hướng, giải pháp bảo vệ nền tảng tư tưởng của Đảng, đấu tranh ngăn chặn các quan điểm sai trái, thù địch trên MXH*. Chính trị quốc gia sự thật.
- Masgoret, A. M., Attitudes, motivation and second language learning: A meta-analysis of studies conducted by Gardner and associated. *Language Learning*, 53(1), 123-163.
- Nguyễn, L.N. (2020). *Ảnh hưởng của việc sử dụng mạng xã hội facebook đến học tập và đời sống của sinh viên hiện nay*. Luận án tiến sĩ. Đại học Khoa học xã hội và Nhân văn: Hà Nội.
- Quốc hội (2016). *Luật Tiếp cận thông tin 2016*. Hà Nội.
- Tôn, N. C. H. (2014). *Luận văn thạc sĩ Thái độ của sinh viên một số trường đại học tại TP.HCM về MXH*. Thành phố Hồ Chí Minh.
- Trần, T. H. & Nguyễn, T. N. (2021). Tìm hiểu một số tác động của mạng xã hội đối với sinh viên Việt Nam hiện nay. *Tạp chí giáo dục lý luận – số 322*, 71-76.
- Vũ, N. P., Nguyễn, X. N., Trần, T. T. & Trương, T. L. H. (2023). Ứng dụng mạng xã hội trong việc định hướng dư luận sinh viên tại các trường đại học ở Việt Nam. *Tạp chí Khoa học & Công nghệ tập 5, số 3*.

TỘI KHỦNG BỐ TRÊN KHÔNG GIAN MẠNG THỜI KỲ CÁCH MẠNG CÔNG NGHIỆP 4.0 - NGHIÊN CỨU SO SÁNH PHÁP LUẬT VIỆT NAM VÀ MỘT SỐ QUỐC GIA TRÊN THẾ GIỚI

Nguyễn Văn Tùng, Nguyễn Thị Thùy Trang, Phạm Trung Dũng

Trường Đại học Luật Hà Nội

Email: nguyenvantungtbk45hlu@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> <i>Khủng bố trên không gian mạng, khủng bố mạng, cách mạng công nghiệp 4.0, Bộ luật Hình sự, trách nhiệm hình sự.</i>	Bằng phương pháp phân tích, thống kê so sánh, liệt kê, tổng hợp, phương pháp nghiên cứu dự báo, nhóm nghiên cứu đã đưa ra khái niệm đặc điểm, nguyên nhân và các quy định pháp luật Việt Nam cũng như thực trạng ở nước ta về khủng bố trên không gian mạng trong thời kỳ cách mạng công nghiệp 4.0. Trên cơ sở so sánh, phân tích đánh giá pháp luật quốc tế, pháp luật các quốc gia cụ thể và pháp luật Việt Nam để nắm rõ và thấy được sự tương quan về tội phạm trên, nhằm rút ra các giá trị tham khảo, làm cơ sở đưa ra các giải pháp, kiến nghị hoàn thiện pháp luật hình sự Việt Nam về tội khủng bố trên không gian mạng thời kỳ cách mạng công nghiệp 4.0.

Dẫn đề: Trong thời kỳ cách mạng công nghiệp 4.0, tội phạm khủng bố trên không gian mạng hoạt động ngày càng tinh vi, phức tạp, chúng “luồn lách” vào những kẽ hở của an ninh mạng để hoạt động. Hiện nay, xu hướng quốc tế hóa pháp luật ngày càng được đẩy mạnh, chống khủng bố trên không gian mạng là mối quan tâm và trở thành một trong số những chính sách ưu tiên hàng đầu của không ít các quốc gia. Ở Việt Nam, nguy cơ tiềm ẩn tội phạm này cũng không nhỏ. Trong khi đó, pháp luật về bảo vệ an ninh mạng chưa thực sự hoàn thiện, việc xử lý, phòng ngừa các tội phạm này cũng chưa thực sự đạt được hiệu quả tốt nhất. Vì vậy, vấn đề về tội phạm trên cần phải được nghiên cứu toàn diện về cả lý luận và thực tiễn. Trong phạm vi tham luận, nhóm nghiên cứu trình bày khái quát những vấn đề lý luận về khủng bố trên không gian mạng thời kỳ cách mạng công nghiệp 4.0, thực tiễn về quy định và xử lý tội phạm này ở Việt Nam; so sánh với pháp luật một số quốc gia cụ thể trên thế giới để rút ra bài học kinh nghiệm và đề xuất các kiến nghị nhằm hoàn thiện hơn pháp luật hiện hành cũng như nâng cao hiệu quả chống, phòng ngừa các tội phạm này trong tương lai.

1. Khái quát về tội khủng bố trên không gian mạng trong thời kì cách mạng công nghiệp 4.0

1.1. Khái niệm khủng bố

Thuật ngữ “khủng bố” (Terrorism) được sử dụng đầu tiên vào năm 1798 bởi nhà triết học người Đức Immanuel Kant. Trong giai đoạn 1879-1881 cụm từ kẻ khủng bố được đế quốc Nga dưới thời Aleksandr II và Aleksandr III với ý nghĩa ban đầu là kẻ chống chính quyền và sau được lan rộng ra.

Định nghĩa về khủng bố trên không gian mạng hiện nay còn có những quan điểm khác nhau như:

Theo Bộ Quốc Phòng Hoa Kỳ, Joint Pub 3-07.2, Antiterrorism, (24 tháng 11 năm 2010), khủng bố được định nghĩa là: *“Việc sử dụng hoặc đe dọa sử dụng bạo lực một cách bất hợp pháp nhằm khắc sâu sự sợ hãi, có ý định cưỡng chế hoặc đe dọa chính phủ, xã hội nhằm theo đuổi các mục tiêu là chính trị, tư tưởng hoặc tôn giáo.”*

Theo Luật phòng, chống khủng bố được Việt Nam thông qua năm 2013: *“Khủng bố là một, một số hoặc tất cả hành vi sau đây của tổ chức, cá nhân nhằm chống chính quyền nhân dân, ép buộc chính quyền nhân dân, tổ chức nước ngoài, tổ chức quốc tế, gây khó khăn cho quan hệ quốc tế của nước Cộng hòa xã hội chủ nghĩa Việt Nam hoặc gây ra tình trạng hoảng loạn trong công chúng.”*

Sự khác biệt trong việc định nghĩa khủng bố giữa một số quốc gia có nguyên nhân từ nhiều yếu tố nhưng cũng chính từ sự khác biệt này lại gây ra nhiều khó khăn cho vấn đề hợp tác quốc tế trong việc phòng, chống tội phạm khủng bố.

Tuy có sự khác biệt trong định nghĩa nhưng nhìn chung, các quan niệm về khủng bố đều có một số điểm chung như:

Đối tượng, mục tiêu của khủng bố là: xâm phạm hoạt động ổn định của cơ quan nhà nước, cuộc sống người dân, sự ổn định an ninh chính trị, quốc phòng, ... của các chủ thể trong xã hội, nhằm mục tiêu gây hoảng loạn, lo sợ trong xã hội, đòi hỏi nhượng bộ, thực thi mục đích từ các nhà nước của các đối tượng khủng bố.

Các hình thức hoạt động của khủng bố: từ hoạt động tấn công, bạo lực, đe dọa như đặt bom, đánh bom, sử dụng vũ khí sinh học... cho đến hoạt động tấn công trên không gian mạng, phát tán dữ liệu độc, gây tê liệt hệ thống mạng... và bao gồm cả tài trợ khủng bố, hoạt động phát tán, chiêu mộ,...

Khủng bố thường nảy sinh chủ yếu từ kết quả của chủ nghĩa cực đoan (với hai thành phần chính là chủ nghĩa dân tộc cực đoan và tôn giáo cực đoan mang trong mình tiêu biểu về sự hẹp hòi, quá khích và độc đoán), đói nghèo, xu thế toàn cầu hóa (lợi ích nhiều nhưng rủi ro cũng không hề ít như mất ninh an toàn quốc gia, bản sắc dân tộc và sự tự chủ vốn có).

1.2. Cách mạng công nghiệp 4.0 và những tác động tới tội phạm khủng bố

So với khung bố “truyền thống”, khung bố trên không gian mạng, đặc trưng bởi yếu tố “không gian mạng”. Không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian (khoản 3 Điều 1 Luật An ninh mạng năm 2018).

Sự xuất hiện “không gian mạng” gắn liền với những thành tố của nền cách mạng công nghiệp 4.0. Tại Diễn đàn Kinh tế Thế giới (WEF) lần thứ 46 đã chính thức khai mạc tại thành phố Davos-Klosters của Thụy Sĩ, với chủ đề “Cuộc cách mạng công nghiệp lần thứ 4”, Chủ tịch Diễn đàn Kinh tế Thế giới đã đưa ra một định nghĩa mới, mở rộng hơn khái niệm Công nghiệp 4.0 của Đức. Theo đó, cách mạng công nghiệp lần thứ tư về bản chất là nền công nghiệp dựa trên nền tảng công nghệ số và tích hợp tất cả các công nghệ thông minh để tối ưu hóa quy trình, phương thức sản xuất, nhấn mạnh rằng một số công nghệ đang và sẽ có tác động to lớn tới đời sống con người.

Cách mạng công nghiệp 4.0 tác động không nhỏ tới đời sống của con người. Trong giai đoạn này nó kết hợp các công nghệ lại với nhau, xóa nhòa các ranh giới giữa các lĩnh vực như vật lý, sinh học... Trong cách mạng công nghiệp 4.0 thì sự kết hợp của trí tuệ nhân tạo (AI), kết nối vạn vật (IoT) và dữ liệu lớn (Big Data). Theo ước tính Liên đoàn truyền thông quốc tế (ITU) – cơ quan về công nghệ thông tin và truyền thông của Liên hợp quốc (UN) thì hiện tại thế giới có hơn 4,9 tỷ người (2/3 dân số thế giới) đang sử dụng internet như một phần không thể thiếu trong cuộc sống, Internet đã gần như phủ sóng cả địa cầu. Trong bối cảnh thế giới thời kỳ này, các thành tố trong cách mạng công nghiệp 4.0 còn tạo nên những tiện ích trong nhiều lĩnh vực khác biệt như: trong lĩnh vực chính trị có thể thấy rõ trong các vấn đề tiêu biểu như bỏ phiếu online, họ kêu gọi bỏ phiếu online... hay trong quan hệ hành chính thì cơ quan công quyền chuyển từ lưu trữ văn phòng từ dạng cứng là giấy thông thường sang lưu trữ song hành ở điện toán đám mây, hay tích hợp các công nghệ vào việc quản lý dân cư, hành chính, hộ tịch... đây đều là các ứng dụng tích cực đã và đang được triển khai.

Sự bùng nổ cách mạng công nghiệp 4.0 biến không gian mạng trở thành môi trường mới lý tưởng cho các hoạt động kinh tế - văn hóa - xã hội nhưng đồng thời cũng là miền hứa hẹn của những hoạt động phi pháp. Với đặc tính của không gian mạng trong thời kỳ cách mạng công nghiệp 4.0, nó có thể tác động tới tội phạm không gian:

Với đặc tính là môi trường không gian ảo, nhân tạo, không có sự hiện diện vật lý của con người nhưng lại là cơ sở để con người trao đổi, lưu trữ dữ liệu, thông tin..., không gian mạng trở thành môi trường thuận lợi cho việc liên kết, trao đổi, truyền tin nhưng cũng không dễ quản lý và bắt giữ được những kẻ phạm tội nói chung, không gian nói riêng. Một trường không gian không có thật do con người tạo lập, bằng cách này

hoặc cách kia, bằng lỗ hổng này hoặc lỗ hổng khác với muôn màn cách thức việc làm điều tra, tiếp cận ra đối tượng thực hiện tương đối khó và vất vả vì yếu tố nên quan đến nước ngoài, bảo mật, ẩn danh...

Sự chuyển hướng các các tổ chức, cá nhân khủng bố sang một phương thức tấn công mới. Nếu như phương thức thực hiện truyền thống của tội phạm khủng bố hay được nhắc tới là đánh bom liều chết hay tung vũ khí sinh học. Khủng bố truyền thống đạt được sự thỏa hiệp dựa trên bạo lực vật chất thì sang khủng bố trên không gian mạng thì chuyển hướng sang bạo lực tinh thần như việc lan truyền, live stream các thông điệp nội dung khủng bố, tiêu cực cho mục đích khủng bố hay chiêu mộ. Sẽ tốt hơn việc đánh bom là mất đi một phần tử và hiệu quả mang tính chất tương đối thì việc tấn công vào không gian mạng sẽ đặc biệt hiệu quả hơn cả về quy mô và tính chất.

Chi phí thời gian, tài chính, nhân lực với hình thức khủng bố mới, có thể giảm thiểu đi nhiều so với các phương tiện khủng bố truyền thống. Công cụ những kẻ khủng bố, tổ chức khủng bố cần là có thể đơn giản một chiếc máy tính cá nhân cấu hình đủ mạnh và một kết nối Internet đơn giản với các gói cước ngang với giá một bữa ăn nhanh đúng nghĩa nhưng hiệu quả thì cực kì đáng lưu tâm.

Ở tầm vĩ mô, cách mạng công nghiệp 4.0 nói chung và với không gian mạng nói riêng còn tác động đến chính sách pháp luật của các quốc gia, trong đó, đặt ra những thách thức to lớn với nhiều lĩnh vực chuyển dịch sâu sắc, trong đó phát sinh hành vi nguy hiểm cho xã hội mới và hoạt động sử dụng công nghệ cao để phạm tội, các mối đe dọa đến an ninh, chủ quyền quốc gia, trật tự, an toàn xã hội, cũng như quyền con người cũng như quyền con người, quyền công dân và toàn bộ hệ thống quản lý, điều hành quốc gia. Do đó, xét riêng trong lĩnh vực phòng ngừa và đấu tranh chống tội phạm điều này đòi hỏi trong chính sách hình sự, pháp luật hình sự (và cả hệ thống tư pháp hình sự) của Nhà nước phải có những thay đổi, ứng phó xử lý trước tình hình, xu thế phát triển của tội phạm.

1.3. Khái niệm khủng bố trên không gian mạng

Thuật ngữ "Khủng bố mạng" lần đầu tiên được sử dụng bởi Barry Collin, một thành viên cao cấp tại Viện An ninh và Tình báo California, vào năm 1980.

Bộ Quốc phòng Hoa Kỳ (DOD) định nghĩa: *“Khủng bố mạng là các hành vi phạm tội được thực hiện bằng cách sử dụng công nghệ máy tính và viễn thông để tạo ra bạo lực và phá hoại hoặc phá hủy các cơ sở công cộng để tạo ra sự hoảng loạn và bất ổn xã hội nhằm ảnh hưởng đến nhà nước hoặc xã hội để đạt được các mục tiêu chính trị, tôn giáo hoặc ý thức hệ... ”*.

Tại quy định tại Khoản 9 Điều 2 Luật An ninh mạng 2018 (Có hiệu lực thi hành từ ngày 01/01/2019) thì khái niệm khủng bố trên không gian mạng được quy định:

“Khủng bố mạng là việc sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện hành vi khủng bố, tài trợ khủng bố.”

Tồn tại một sự tương đồng lớn khi định nghĩa về khủng bố mạng với những đặc trưng của việc sử dụng công nghệ thông tin, điện tử, viễn thông cho việc tiến hành các hành vi bạo lực vật chất, phá hoại nhằm tạo nên sự hoảng loạn trong công chúng hoặc phương hại an ninh quốc gia. Nói cách khác tự tương đồng này thể hiện ở việc sử dụng các “công nghệ mới” (nói trên) như một công cụ tân tiến, hữu hiệu để tiến hành những hành vi khủng bố.

Như vậy, khủng bố trên không gian mạng trước hết có những đặc trưng của hành vi khủng bố truyền thông về hành vi và mục đích. Nhưng đó còn là sự phát triển và kết hợp đặc biệt của khủng bố theo thời gian và sự phát triển khoa học kỹ thuật trên thế giới. Khủng bố trên không gian mạng chính là sử dụng nền tảng không gian mạng vào hoạt động khủng bố. Hoạt động khủng bố này thể hiện ở nhiều khía cạnh và khá đặc biệt, từ việc tấn công hệ thống mạng của cơ quan tổ chức, cá nhân nhằm đe dọa gây sợ hãi đến hoạt động chiêu mộ, huấn luyện vũ khí của các tổ chức khủng bố và cả tài trợ khủng bố. Khủng bố trên không gian mạng còn thể hiện ở việc xuyên tạc thông tin hướng tới kích động bạo loạn, nhằm tác động tới chính quyền, mang đậm màu sắc chính trị.

Với quan niệm như vậy, khủng bố trên không gian mạng có những đặc điểm cơ bản sau đây:

Thứ nhất, về khách thể của tội phạm: Các quan hệ xã hội bị xâm hại là sự ổn định an ninh quốc gia, trật tự - an toàn xã hội. Việc xâm hại đến các khách thể này thường kèm theo việc xâm hại đến các quyền được tôn trọng và bảo vệ về tính mạng, sức khỏe; các quyền tự do cơ bản của con người; quyền sở hữu.

Đối tượng tác động của tội phạm thường là cơ sở dữ liệu, hệ thống thông tin của cá nhân, tổ chức mà đa phần là nhà nước vì mục đích của chúng là sự sợ hãi, sự thỏa hiệp của nhóm đối tượng đặc biệt này. Đặc biệt có thể nhắc tới đối tượng là máy tính và hệ thống mạng. Máy tính là đối tượng tấn công của các hành vi độc hại (*tấn công vào tính toàn vẹn của hệ thống máy tính hoặc tội phạm mạng stricto sensu*).

Đối tượng của chúng hướng tới có thể là các đối tượng con người hoặc đối tượng vật chất như chính trị gia, người có sức ảnh hưởng hoặc các cơ sở quân sự, quốc phòng, hệ thống rada, phòng không... Ví dụ: Ngày 23/4/2013, tài khoản Twitter của tờ Associated Press sau khi bị tấn công chiếm quyền đã đưa ra thông tin Nhà Trắng bị tấn công và tổng thống Mỹ Obama bị thương nặng. Trong một thời gian ngắn, thông tin trên đã gây ra sự hoảng loạn cho mọi người, làm chỉ số chứng khoán Dow Jones mất 130 điểm và 136 tỉ USD của chỉ số S&P 500.

Thứ hai, về mặt khách quan của tội phạm:

Hành vi của tội phạm khủng bố nói chung là hành vi mang tính bạo lực, đe dọa bạo lực, gây nguy hiểm cho con người, gây hậu quả và gây thiệt hại nghiêm trọng về sức khỏe, tính mạng của con người, tài sản, an ninh quốc gia và thế giới. Cùng với đó, hành vi khủng bố trên không gian mạng nói riêng còn có thể là những hành vi gây sự rối loạn hoạt động của các hệ thống mạng internet, viễn thông, điện tử.

Cách thức thực hiện: Nếu đối tượng của chúng là hệ thống mạng, cơ sở dữ liệu của cơ quan nhà nước, bằng việc sử dụng các chuyên gia công nghệ, hacker, lợi dụng lỗ hổng của các phần mềm công nghệ, cách thức thực hiện của chúng là nhắm tới lỗ hổng trong hệ thống mạng để từ đó lan truyền mã code độc, virus nhằm gây tắc nghẽn, sập hệ thống mạng hoặc tiến hành chiếm quyền điều khiển. Nếu đối tượng là con người và các đối tượng vật chất, những tên khủng bố trên không gian mạng, có thể sử dụng mạng lưới internet, phương tiện viễn thông, điện tử là phương tiện liên lạc, bàn bạc, tổ chức hành động... Lúc này, “máy tính” có thể không phải là mục tiêu tấn công mà còn là phương tiện để chuẩn bị, tiến hành hành vi khủng bố.

Hậu quả thiệt hại mà loại tội phạm gây ra: Hoạt động khủng bố thường gây ra những thiệt hại to lớn cho con người, xã hội, quốc gia..., cụ thể là sự thiệt hại về dữ liệu, thông tin, sự ổn định đường truyền, ổn định dữ liệu an toàn mạng thông tin, qua đó, gây ra các thiệt hại thực tế cho trật tự xã hội, an toàn của người dân, an ninh quốc gia.

Thứ ba, về chủ thể của tội phạm: Chủ thể của tội phạm thực hiện hoạt động tội phạm của mình với các mục tiêu thường gắn với yếu tố chính trị, dân tộc, tôn giáo, ly khai... mang trong mình kiến thức về tấn công mạng và phá hoại trên không gian mạng. Chỉ cần được trang bị kiến thức, kỹ năng về mạng máy tính, kỹ năng tấn công mạng và quan trọng là tư tưởng kèm mục đích khủng bố thì hoàn toàn có thể thực hiện khủng bố trên không gian mạng. Tính thời sự ở chỗ chủ thể khủng bố là các thành viên của tổ chức khủng bố ngày càng trẻ hóa và nhạy cảm với chiến tranh mạng.

Tuy nhiên, có điều cần lưu tâm đặt ra là chủ thể nhà nước liệu có nên cũng xác định là chủ thể khủng bố, liệu nhà nước cũng nên liệt kê thành chủ thể của đối tượng đề tài này khi rõ ràng loại chủ thể đặc biệt này hoàn toàn có đầy đủ các yếu tố có thể cân nhắc tới khi đề cập. Khoa học pháp lý Liên bang Xô Viết trước kia từng quan điểm quốc gia là chủ thể của hành vi khủng bố, theo đó thì các hành vi khủng bố được tổ chức bởi các quốc gia nước ngoài nhằm gây ảnh hưởng đến chính sách của một quốc gia khác. Quan điểm của một số quốc gia Ả rập trên diễn đàn của ủy ban Adhoc tại Liên Hợp Quốc cũng nhấn mạnh “khủng bố nhà nước” với các hành vi bất hợp pháp bằng vũ lực của nước này lên nước khác, hoặc các trường hợp nhượng bộ, che giấu hay giúp đỡ của quốc gia này với các nhóm, tổ chức khủng bố tiến hành chống lại nước khác.

Thứ tư, về mặt chủ quan của tội phạm: Lỗi cố ý là đặc trưng của tội khủng bố nói chung và khủng bố mạng nói riêng. Người phạm tội nhận thức rõ tính nguy hiểm của

hành vi cũng như hậu quả thiệt hại có thể gây ra. Việc thực hiện hành vi phạm tội hướng tới mục đích là tạo nên sự bất ổn, hoang mang, lo sợ trong dân chúng, sâu sa hơn còn có thể là sự nhượng bộ của chính quyền, nhà nước trong việc đáp ứng yêu sách của những kẻ khủng bố.

1.5. Tác hại khủng bố trên không gian mạng

Một là, tác hại về kinh tế: Những năm qua, các vụ khủng bố trên không gian mạng đã ngày càng gia tăng một cách chóng mặt, làm tiêu tốn biết bao nhiêu công sức, của cải của con người.. Nhiều người bị đày vào cảnh tay trắng chỉ trong giây phút. Một báo cáo được tài trợ của hàng phần mềm McAfee đưa ra vào năm 2014 ước tính tội phạm mạng gây thiệt hại cho nền kinh tế toàn cầu khoảng 445 tỉ USD. Đầu năm 2016, một nghiên cứu khác của trung tâm Juniper Research ước tính thiệt hại do tội phạm mạng gây ra có thể lên tới 2100 tỉ USD vào năm 2019.

Hai là, tác hại về chính trị: Khủng bố trên không gian mạng làm xuất hiện những hậu quả lâu dài cho tương lai loài người. Khủng bố nói chung và khủng bố trên không gian mạng nói riêng còn khiến cho mâu thuẫn, xung đột trên thế giới ngày càng trở nên gay gắt quyết liệt. Khối thống nhất, nền hòa bình mà nhân loại nỗ lực xây dựng đã bị xâm hại và lung lay thực sự gây thiệt hại nghiêm trọng đến hoạt động bình thường của một chính phủ, hệ thống giao thông công cộng, hệ thống liên lạc hay cơ sở hạ tầng, làm mất ổn định nghiêm trọng hoặc hủy hoại cơ cấu xã hội, kinh tế, thể chế và chính trị căn bản của một quốc gia hoặc một tổ chức quốc tế. Khủng bố trên không gian mạng chưa phải là một cuộc chiến tranh công khai trên một phạm vi rộng nhưng tiến hành khủng bố là cách để nuôi dưỡng mầm mống và làm bùng phát chiến tranh trên toàn thế giới.

Ba là, tác hại về xã hội: Nạn khủng bố trên không gian mạng lan tràn khiến tất cả mọi người mất đi cảm giác an toàn, cảm giác yên tâm trong cuộc sống trong cuộc sống. Nỗi ám ảnh về khủng bố trên không gian mạng len lỏi vào cuộc sống bình yên của mọi người và đang mài mòn, thách thức sức chịu đựng của tất cả. Không gian mạng còn có thể gây nguy hại cho cơ quan, tổ chức, trường học, đơn vị, địa phương, doanh nghiệp, gia đình và cá nhân. Khi công tác bảo mật hệ thống mạng không được coi trọng đúng mức, không gian mạng sẽ bị phát tán mã độc, bị tấn công, gây thiệt hại về tài sản, tinh thần, sức khỏe, thậm chí cả tính mạng con người (bắt cóc, tống tiền, sát hại...).

2. Tội khủng bố trên không gian mạng theo pháp luật hình sự Việt Nam

2.1. Quy định về tội khủng bố trên không gian mạng theo pháp luật Việt Nam

Trước khi BLHS năm 2015 ra đời, pháp luật hình sự Việt Nam chỉ có quy định về tội khủng bố nhằm chống chính quyền nhân dân và tội khủng bố nói chung mà không có điều luật về tội khủng bố trên không gian mạng độc lập. Tuy nhiên, so với trước đây, BLHS năm 2015 đã có những điểm tiến bộ hơn khi trong các dấu hiệu pháp lý CTTTP của các tội khủng bố đã thể hiện rõ nét hơn yếu tố “trên không gian mạng”.

2.1.1. Các dấu hiệu pháp lý về tội khủng bố trên không gian mạng theo quy định Bộ luật Hình sự năm 2015

Ngoài những dấu hiệu về khách thể của tội phạm, mặt chủ quan của tội phạm như đã nêu trong phần lý luận, CTTP các tội khủng bố nhằm chống chính quyền nhân dân (Điều 113) và tội khủng bố (Điều 299) trong BLHS năm 2015 có những dấu hiệu đặc trưng cụ thể như sau:

***Về hành vi:**

Thông thường, tội khủng bố nói chung đặc trưng bởi các nhóm hành vi khách quan như: *Thứ nhất*, hành vi đe dọa xâm phạm tính mạng, sức khỏe, quyền tự do thân thể của con người; *thứ hai*, hành vi xâm phạm tài sản; *thứ ba*, hành vi xâm hại hoạt động của máy tính, mạng viễn thông, phương tiện điện tử; *thứ tư*, hành vi thành lập, tham gia tổ chức khủng bố, tài trợ khủng bố; *thứ năm*, hành vi trợ giúp tổ chức khủng bố. Tuy nhiên tùy từng mục đích phạm tội là chống chính quyền nhân dân hay chỉ nhằm gây hoảng loạn trong công chúng mà có thể cấu thành tội phạm tại Điều 113 hoặc 299 BLHS.

Trong các nhóm hành vi đó, nhóm hành vi thứ tư thể hiện rõ nét yếu tố “trên không gian mạng”, cụ thể tại điểm d khoản 2 Điều 113 và điểm d khoản 2 Điều 299 quy định: “*Tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của cơ quan, tổ chức, cá nhân*”. Quy định này mới được bổ sung trong BLHS năm 2015. Sự bổ sung nhóm hành vi ở đây là hoàn toàn hợp lý và đáp ứng được yêu cầu đấu tranh chống các hoạt động khủng bố trong giai đoạn hiện nay. Quy định tại điểm d khoản 2 các Điều 113 và 299 BLHS được hiểu rằng đối tượng tác động của tội phạm là mạng máy tính, mạng viễn thông, phương tiện điện tử cũng như hoạt động bình thường của các đối tượng này. Việc xâm phạm mạng máy tính, mạng viễn thông, phương tiện điện tử nhằm gây ra tình trạng hoảng loạn trong công chúng hoặc gây suy yếu chính quyền nhân dân. Quy định này đưa đến các trường hợp:

- Trường hợp trực tiếp tấn công xâm hại hoạt động mạng máy tính, mạng viễn thông, phương tiện điện tử; coi đó là đối tượng tác động để gây hại thì áp dụng điểm d khoản 2 Điều 113 BLHS năm 2015.

- Trường hợp các đối tượng sử dụng mạng xã hội một công cụ kết nối, giữ liên lạc của các đồng phạm, để trao đổi thông tin, củng cố tổ chức, truyền tin đến đại chúng (*như tự sử dụng các mạng xã hội như Facebook, Youtube, của mình để đăng tải*) nhưng mục đích nhằm tấn công, gây cản trở, rối loạn hoạt động của mạng, hoạt động mạng máy tính, mạng viễn thông thì áp dụng điểm d khoản 2 điều 113 BLHS năm 2015.

Như vậy, đối với các dạng hành vi khách quan thứ nhất, thứ hai, thứ tư và thứ năm kể trên, “không gian mạng” được sử dụng như phương tiện phạm tội chủ yếu để duy trì, liên kết các đối tượng, hoạt động của các đối tượng chứ không phải đối tượng gây hại như trường hợp hành vi thứ năm.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

*Về chủ thể: Chủ thể của tội phạm phải là người có năng lực TNHS. Năng lực có được khi chủ thể đủ tuổi chịu TNHS tại Điều 12 BLHS và không thuộc tình trạng không có năng lực TNHS tại Điều 21 BLHS. Đối với hai tội danh tại hai điều luật độc lập là 113 và 299 BLHS thì, tuổi chịu TNHS cũng có sự khác biệt:

- Đối với tội khủng bố nhằm chống chính quyền nhân dân (Điều 113 BLHS): tuổi chịu TNHS của chủ thể là từ đủ 16 tuổi trở lên;

- Đối với tội khủng bố (Điều 299 BLHS): tuổi chịu TNHS của chủ thể có thể là từ đủ 14 tuổi trở lên (xem khoản 2 Điều 12 BLHS)

2.1.2. Hình phạt của tội khủng bố trên không gian mạng theo quy định Bộ luật Hình sự năm 2015

Hai tội khủng bố tại 2 Điều 113 và 299 BLHS năm 2015 đều quy định các khung hình phạt khác nhau. Nhìn chung, mức phạt cao nhất tại là tử hình và thấp nhất là một năm tù (trong trường hợp chuẩn bị phạm tội). Trong đó, khung hình phạt dành cho trường hợp “*Tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của cơ quan, tổ chức, cá nhân*” có mức phạt cao nhất là 15 năm tù (cụ thể: từ 10 năm đến 15 năm tù nếu thuộc điểm d khoản 2 Điều 113 BLHS; từ 05 năm đến 15 năm tù nếu thuộc điểm d khoản 2 Điều 299 BLHS. Đây không phải là khung hình phạt có mức hình phạt cao nhất đối với các khủng bố trên không gian mạng với quan niệm hành vi xâm hại các hệ thống tin học nói trên có tính nguy hiểm thấp hơn những trường hợp xâm hại đến tính mạng, tài sản của con người.

Ngoài ra, một số hình phạt bổ sung như tước một số quyền công dân, phạt quản chế, cấm cư trú từ 01 năm đến 05 năm hoặc tịch thu một phần tài sản hoặc toàn bộ tài sản cũng có thể được áp dụng với người phạm tội – khoản 5 Điều 299 BLHS.

2.2. Thực trạng khủng bố trên không gian mạng ở Việt Nam hiện nay

Thực tiễn xét xử về các tội khủng bố trên không gian mạng ở Việt Nam không nhiều. Có thể kể đến điển hình như: Vụ án thuộc nhóm xâm phạm an ninh quốc gia, cụ thể là vụ việc thành lập và tài trợ khủng bố của tổ chức “Triều đại Việt”. Tổ chức “Triều đại Việt” do các đối tượng ở nước ngoài gồm: Ngô Văn Hoàng Hùng (Ngô Hùng), Huỳnh Thanh Hoàng, Trần Thanh Đình thành lập từ khoảng tháng 6/2017 với mục đích lôi kéo, tập hợp người Việt ở trong và ngoài nước tham gia, sử dụng bạo động vũ trang, khủng bố để chống phá chế độ và Nhà nước Việt Nam. Các đối tượng trên thường xuyên đăng tải các video livestream trên mạng xã hội facebook, tuyên truyền, nói xấu Đảng, Nhà nước, nhằm lôi kéo nhiều người tham gia tổ chức, chỉ đạo thực hiện các nhiệm vụ như: mua vật liệu nổ, chế tạo trái nổ, gây nổ tại trụ sở Cơ quan Nhà nước; chuẩn bị vũ khí, tập hợp lực lượng tại nhiều tỉnh, thành phố. Ngoài hành vi nói trên, các đối tượng còn có những hành vi cấu thành các tội khác xâm phạm an ninh quốc gia.

Hay vụ việc từ cuối năm 2016, các đối tượng Đào Minh Quân, Phạm Lisa và một số đối tượng phản động trong và ngoài nước là thành viên của tổ chức “Chính phủ quốc gia Việt Nam lâm thời”, thông qua mạng xã hội đã lôi kéo nhiều đối tượng không nghề nghiệp, bất mãn chế độ nhưng có chung một điểm là hám lợi thành lập các “nhóm hành động” để tiến hành khủng bố, phá hoại tại Việt Nam. Trong đó có vụ đặt bom xăng ở sân bay Tân Sơn Nhất năm 2016, vụ ném bom xăng bãi giữ xe vi phạm Công an thành phố Biên Hòa, tỉnh Đồng Nai năm 2017 và gần đây nhất là vụ ném bom tại trụ sở Công an phường 12, quận Tân Bình năm. Qua quá trình điều tra, xét xử, các đối tượng đều thành khẩn khai nhận trong quá trình sử dụng mạng xã hội đã tiếp xúc liên lạc với những đối tượng khủng bố lưu vong ở nước ngoài và nhận hướng dẫn, chỉ đạo và nhận tiền từ các đối tượng bên ngoài để thực hiện các hành vi khủng bố.

Các vụ án xảy ra ở Việt Nam về khủng bố và có yếu tố của không gian mạng, chủ yếu là sử dụng mạng Internet các đối tượng trong và ngoài nước móc nối với nhau để thực hiện điều hành về cách thức khủng bố, đối tượng tấn công, công cụ, thời gian, địa điểm tiến hành hành vi khủng bố. Các vụ khủng bố trên dù chưa gây ra thiệt hại lớn về người nhưng đã đặt ra những thách thức trong công tác đảm bảo an ninh của Việt Nam. Từ những phân tích nêu trên cho thấy, hoạt động truyền bá tư tưởng khủng bố trong thời gian qua đã được các tổ chức khủng bố lưu vong người Việt ở nước ngoài đẩy mạnh trên không gian mạng.

Có thể thấy rằng, việc tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của các cơ quan, tổ chức, cá nhân theo điểm d khoản 2 Điều 113 hay Điều 299 không phải là điển hình cho thực tiễn xảy ra ở Việt Nam. Những vụ việc diễn ra ở nước ta cho đến thời điểm hiện nay, chủ yếu là sử dụng không gian mạng là công cụ, phương tiện phạm tội cho những hành vi khủng bố truyền thống. Ví dụ như thông qua mạng để bàn bạc, lên kế hoạch để tiến hành xâm phạm tính mạng, phá hủy tài sản hoặc thông qua mạng để thành lập tổ chức khủng bố, lôi kéo các đối tượng gia nhập tổ chức khủng bố... Thực tế, việc tấn công vào mạng máy tính, phương tiện điện tử nói chung đã xảy ra ở Việt Nam, nhưng mục đích không nhằm làm hoảng loạn công chúng hay suy yếu chính quyền, chủ yếu nhằm chiếm đoạt tài sản, nhằm chiếm đoạt bí mật kinh doanh hoặc nhằm lấy cắp thông tin để phục vụ cho một số hoạt động bất hợp pháp khác chứ không nhằm mục đích khủng bố. Những hành vi trong các trường hợp trên sẽ xử lý về tội phạm công nghệ cao.

3. Pháp luật một số quốc gia trên thế giới về tội khủng bố trên không gian mạng

Nghiên cứu trong sự so sánh giữa pháp luật Việt Nam và pháp luật một số quốc gia trên thế giới cho thấy tội khủng bố trên không gian mạng được quy định có những đặc trưng giống và khác biệt nhất định:

Thứ nhất, pháp luật Cộng hòa Pháp

Luật hình sự Pháp chưa đưa ra thuật ngữ khủng bố trên không gian mạng rõ ràng, mà quy định thành tội khủng bố liên quan tới máy tính, có thể hiểu theo hướng họ quy định dựa trên công cụ tiến hành chứ không phải môi trường thực hiện. Nhưng lại quy định về tội phạm khủng bố với đặc điểm là khá sát với tình hình thực tế cả ở hiện tại lẫn theo chiều hướng phát triển của tội phạm. Nhận thức tính nghiêm trọng của loại tội phạm này nên Pháp đã dành 1 chương trong luật hình sự để quy định về loại tội phạm này. Tuy nhiên cũng xuất phát từ yếu tố thời sự của vấn đề, quốc gia này chưa xây dựng cụ thể định nghĩa riêng biệt về khủng bố trên không gian mạng như Việt Nam mà mới chỉ dừng lại ở quy định việc sử dụng các hoạt động máy tính, công nghệ cho mục đích khủng bố là tội phạm khủng bố.

Chủ thể trong luật hình sự Pháp cá nhân thì theo Điều 112-8 Bộ luật Hình sự Pháp, việc truy cứu trách nhiệm hình sự đối với một thể nhân chỉ được thực hiện khi người này đó đủ 13 tuổi trở lên khác với Việt Nam độ tuổi là 14 trở lên. Luật Pháp không quy định độ tuổi mà trong đó năng lực trách nhiệm hình sự được coi là hạn chế. Trong thực tế áp dụng, các cơ quan tố tụng Pháp hiếm khi áp dụng hình phạt đối với người chưa thành niên bởi họ xác định: *“xử lý hình sự người chưa thành niên phạm tội chủ yếu nhằm mục đích bảo vệ, trông nom, chăm sóc và giáo dục người đó là chính”*.

Hình phạt cho loại tội phạm này trong pháp luật pháp tương đối nghiêm khắc, đi kèm hình phạt tù là phạt tiền, hình phạt tương đối cứng rắn, nghiêm khắc. Mức án mà tội phạm phải chịu trong hình phạt tù từ ba năm đến chung thân, so với Việt Nam thì cao nhất trong án phạt tù là tử hình, có thể thấy Việt Nam nghiêm khắc hơn trong xử lý tội phạm khủng bố. Hình phạt tiền trong quy định của Cộng Hoà Pháp thì mức phạt tiền dao động từ mức 100.000 euro đến 750.000 euro, hình phạt này song song, một sự khác biệt so với Việt Nam thì không có.

Một điều cần lưu ý là ở Cộng Hoà Pháp không phân chia tội phạm khủng bố ra riêng dựa vào mục đích như cách của Việt Nam. Ở Việt Nam thì phân chia tội phạm khủng bố thành hai điều luật riêng biệt ở 113 và 299 Bộ luật Hình sự 2015 như một đặc trưng riêng với khủng bố chống chính quyền nhân dân và khủng bố. Là một trong những nhà nước xã hội chủ nghĩa hiếm hoi còn lại trên thế giới, nhà nước Việt Nam ta nhận thức rõ và đề cao việc bảo vệ chế độ, phân loại để xử lý các loại tội phạm mang màu sắc chính trị rõ ràng, tách rõ tội phạm khủng bố với điều 299 còn lại có thể xác định khủng bố ở đây xuất phát từ một số nguyên nhân khác như dân tộc, tôn giáo... Và sự so sánh này có thể được lí giải từ yếu tố nội tại đặc thù của từng quốc gia.

Thứ hai, pháp luật Liên bang Nga

Nghiên cứu pháp luật Liên bang Nga cho thấy nhiều sự tương đồng với pháp luật hình sự Việt Nam. Pháp luật cả hai quốc gia đều không được quy định rõ ràng trong Bộ luật Hình sự. Về chủ thể của tội phạm, trong luật định ở cả hai quốc gia đều được xác

định là cá nhân, tổ chức. Về hậu quả thiệt hại, cả hai quốc gia đều trình bày về hậu của tội phạm giống như một yếu tố chính. Về đối tượng tác động, đều được xác định là diễn ra trên không gian mạng, mạng máy tính hay được thực hiện bằng máy tính. Về mục đích phạm tội: là sự hoảng loạn trong quần chúng sau đó tiến tới sự khuất phục, nhượng bộ của chính quyền. Về hình phạt, ở trong tội này, hai quốc gia đều quy định về việc phải chịu hình phạt, hình phạt cho tội này đều là những hình phạt nghiêm khắc.

Bên cạnh nhưng điểm chung, quy định pháp luật của hai quốc gia cũng có những khác biệt, chẳng hạn: về mục đích phạm tội, trong mô tả tội phạm thì mục đích của tội phạm khủng bố Việt Nam lại khá rõ ràng trong việc quy định rõ mục đích của tội phạm này là chống chính quyền, ép buộc chính quyền ở điều 113 và gây hoảng loạn tại điều 299 còn ở Nga thì mục đích của tội phạm khủng bố này là nhằm gây mất ổn định hoạt động của chính quyền hoặc tổ chức quốc tế hoặc ảnh hưởng đến việc ra quyết định của họ, cũng như mối đe dọa thực hiện các hành động này để ảnh hưởng đến việc ra quyết định của chính quyền hoặc tổ chức quốc tế. Về hình phạt, hình phạt cho tội phạm ở hai quốc gia tuy giống nhau ở việc đều là bản án nghiêm khắc nhất cho tội phạm nhưng ở Nga chỉ là mức án chung thân, còn Việt Nam là tử hình.

Thứ ba, pháp luật Cộng Hòa Liên bang Đức

Nhìn chung, nghiên cứu pháp luật Đức có một số điểm tương đồng với pháp luật Việt Nam khi đều không nhận định rõ về hoạt động khủng bố trên không gian mạng. Chủ thể của tội phạm trong luật định ở cả 2 quốc gia đều được xác định là cá nhân, tổ chức. Về đối tượng tác động, đối tượng tác động của tội phạm này đều được xác định là diễn ra trên không gian mạng, mạng máy tính hay được thực hiện bằng máy tính. Về mục đích phạm tội, mục đích tội phạm mà 2 quốc gia miêu tả đều là sự hoảng loạn trong quần chúng sau đó tiến tới sự khuất phục, nhượng bộ của chính quyền

Sự khác biệt tập trung chủ yếu đó là: Về hình phạt, ở trong tội này, hai quốc gia đều quy định về việc phải chịu hình phạt nhưng hình phạt cho tội này ở Đức đều là những hình phạt nhẹ chưa phải nặng nhất như Việt Nam là chung thân và tử hình. Về lỗi của người phạm tội, yếu tố lỗi là yếu tố không có trong cấu thành tội phạm của Pháp, xuất phát từ truyền thống lập pháp của họ trong việc quy định đã phạm tội là đã có lỗi. Còn ở pháp luật Việt Nam thì yếu tố lỗi cố ý hay vô ý còn được bàn luận để xem xét việc phạm tội của chủ thể là do tự thân hay bị lôi kéo hay do vấn đề khác.

4. Một số kiến nghị hoàn thiện pháp luật và nâng cao hiệu quả áp dụng pháp luật về tội khủng bố trên không gian mạng tại Việt Nam

Trên cơ sở nghiên cứu lý luận, quy định thực tiễn pháp luật hình sự Việt Nam về các tội phạm khủng bố cùng với nghiên cứu một số kinh nghiệm quốc tế, nhóm tác giả khái quát một số định hướng hoàn thiện pháp luật Việt Nam như sau:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thứ nhất, cần đưa ra một khái niệm về tội phạm khủng bố cũng như khủng bố mạng có tính tương thích, đồng nhất với quy định các nước trên thế giới về tội phạm khủng bố. Trong khuôn khổ luật quốc tế, khái niệm về tội phạm khủng bố hay khủng bố mạng hiện đều mang tính quốc gia hay phạm vi khu vực tương đối hẹp, chưa có sự thống nhất, từ đây dẫn đến các hoạt động tương trợ tư pháp, dẫn độ tội phạm gặp khó khăn, đôi khi là không thể nếu các quốc gia không có các điều ước song phương với nhau.

Thứ hai, sửa đổi quy định độ tuổi của chủ thể: Quy định về tuổi chịu TNHS trong tội phạm khủng bố tại Điều 113 BLHS là từ đủ 16 trở lên còn Điều 299 BLHS là từ đủ 14 trở lên. Mặc dù quy định riêng biệt thành 2 tội khác nhau nhưng nếu không xem xét đến yếu tố mục đích thì các dấu hiệu CTTP còn lại là tương đồng. Trong khi đó, nếu xét về tính nguy hiểm cho xã hội thì các tội xâm phạm an ninh quốc gia được xếp vào nhóm nguy hiểm nhất, có nghĩa đánh giá một cách tương đối khách quan, tội khủng bố nhằm chống chính quyền nhân dân (Điều 113) được coi là nguy hiểm hơn tội khủng bố (Điều 299). Tuy nhiên, tuổi chịu TNHS trong tội phạm khủng bố nhằm chống chính quyền nhân dân (Đ113) lại cao hơn so với tội khủng bố (Đ299). Điều này có thực sự hợp lý hay không, cần có sự xem xét và thống nhất lại.

Từ Bộ luật Hình sự Cộng hòa Pháp, bộ luật hình sự của Hàn Quốc thì ta có đề xuất hạ mức tuổi chịu trách nhiệm của tội phạm. Tội phạm nói chung và tội phạm khủng bố trên không gian mạng nói riêng đang dần trẻ hóa như sự phát triển của khoa học công nghệ vậy. Việc giới trẻ ngày càng tiếp thu và sử dụng công nghệ nhưng cũng từ xu thế toàn cầu hóa, guồng quay công việc mà cha mẹ bỏ bê con cái dẫn đến những tư tưởng sai lệch là tìm tới khủng bố hay tân phát xít là một điều không còn hiếm gặp, từ đây là tiền đề cho tầng lớp kế cận khủng bố là khủng bố trên không gian mạng. Nhóm nghiên cứu cho rằng nên giảm độ tuổi chịu trách nhiệm hình sự cho tội này từ 14 xuống 13 giống như của Pháp, điều này hoàn toàn khả thi và phù hợp với tình hình thực tế, với tình hình phát triển của tội phạm.

Thứ ba, sửa đổi hình phạt: Quy định về hình phạt bổ sung tại khoản 5 Điều 299 BLHS là phù hợp, tuy nhiên, đối chiếu vào Điều 113 BLHS thì hình phạt bổ sung không được quy định tại đó. Nhóm nghiên cứu cho rằng nên bổ sung quy định hình phạt bổ sung đối với tội khủng bố nhằm chống chính quyền nhân dân tại Điều 113 BLHS để thống nhất với quy định tại Điều 299 BLHS. Tiếp đó, có thể cân nhắc bổ sung chế tài phạt tiền: Như cách xử lý tội phạm khủng bố ở Pháp ngoài việc thực hiện hình phạt tù thì hình phạt bổ sung là việc phạt số tiền lớn như một chế tài song song, điều này nên được Việt Nam áp dụng để xử lý nghiêm, răn đe những cá nhân, tổ chức đang manh nha phạm tội.

Thứ tư, sửa đổi về kỹ thuật lập pháp: Hành vi tấn công, xâm hại, cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử của cơ quan,

tổ chức, cá nhân (điểm d khoản 2 các Điều 113 và 299 BLHS) thực chất được quy định với tinh thần là một dạng hành vi độc lập với hành vi xâm phạm tính mạng con người hoặc phá hủy tài sản của cơ quan, tổ chức, cá nhân (khoản 1 các Điều 113 và Điều 299). Vì vậy, không nên coi hành vi tại điểm d khoản 2 là trường hợp CTTP giảm nhẹ của tội này mà nên xem là một trường hợp CTTP cơ bản khác nhưng ít nguy hiểm hơn trường hợp tại khoản 1. Tuy nhiên, khoản 2 lại được mở đầu “*phạm tội thuộc một trong các trường hợp sau đây...*” (có nghĩa phải thỏa mãn CTTP tại khoản 1 cộng với một số các tình tiết được mô tả sau) – là cấu trúc của các CTTP giảm nhẹ hoặc CTTP tăng nặng. Thiết nghĩ rằng điều này chưa thật sự hợp lý và cần có sự sửa đổi.

Bên cạnh nhưng một số kiến nghị về hoàn thiện pháp luật nêu trên để chống và phòng ngừa thực sự có hiệu quả tội khủng bố trên không gian mạng, cần phải kết hợp với việc làm tốt những giải pháp về nâng cao nhận thức đội ngũ áp dụng pháp luật (đặc biệt nhận thức trong hoạt động quyết định hình phạt, đặc biệt lưu ý đến những trường hợp sử dụng “không gian mạng” làm phương tiện hữu hiệu để phạm tội – cần xác định đúng tính nguy hiểm của hành vi để lượng hình phù hợp); hoàn thiện hệ thống pháp luật về quản lý cũng như gia tăng đầu tư nguồn lực vật chất cho hoàn thiện cơ sở về mạng lưới công nghệ nhằm quản lý, kiểm soát tốt các hoạt động mạng; tuyên truyền, giáo dục ý thức pháp luật cho người dân; tích cực tham gia vào các lực lượng cảnh sát quốc tế, cảnh sát khu vực để học hỏi và hỗ trợ hoạt động tư pháp xử lý và phòng ngừa tội phạm khủng bố trên không gian mạng;...

KẾT LUẬN

Khủng bố trên không gian mạng thời kỳ cách mạng công nghiệp 4.0 đang là mối đe dọa tới an ninh quốc gia, hòa bình thế giới. Chính vì vậy, đấu tranh chống tội phạm này không chỉ là mối quan tâm của các quốc gia riêng lẻ mà đã trở thành mối quan tâm của cả cộng đồng quốc tế. Đề tài nghiên cứu này dựa vào cơ sở nghiên cứu các quan điểm hiện nay trên thế giới về khái niệm khủng bố trên không gian mạng thời kỳ cách mạng công nghiệp 4.0, mục đích làm rõ những vấn đề lý luận về tội phạm trên để trả lời cho các câu hỏi về khái niệm, đặc điểm, sự cần thiết cần thiết của việc phòng chống tội phạm này, tìm hiểu thực trạng khủng bố trên không gian mạng ở Việt Nam hiện nay và so sánh giữa pháp luật Việt Nam với pháp luật quốc tế và pháp luật một số quốc gia cụ thể trên thế giới. Từ đó có thể rút ra giá trị tham khảo, đồng thời đề xuất các kiến nghị về một số giải pháp hoàn thiện pháp luật Việt Nam về vấn đề này góp phần nâng cao hiệu quả hợp tác đấu tranh chống khủng bố trên không gian mạng giữa Việt Nam với các nước trong khu vực cũng như trên thế giới. Hành trình chống khủng bố trên không gian mạng thời kỳ cách mạng 4.0 là một hành trình dài và sẽ có nhiều khó khăn, thách thức. Thiết nghĩ, muốn thành công trên hành trình này các quốc gia cần đặt lợi ích chung của nhân loại, mục tiêu bảo vệ con người lên trên hết.

TÀI LIỆU THAM KHẢO

* Văn bản pháp luật

1. Bộ luật Hình sự 2015
2. Bộ luật Hình sự Cộng Hòa Pháp
3. Bộ luật Hình sự Liên Bang Đức
4. Bộ luật Hình sự Cộng hòa Liên Bang Nga
5. Luật phòng chống khủng bố 2013
6. Luật an ninh mạng 2018
7. Hội đồng Thẩm phán Tòa án nhân dân tối cao Nghị quyết số 07/2019/NQ-HĐTP.

* Tài liệu khác

Luận án tiến sĩ Luật học: "Giải pháp nâng cao hiệu quả phòng chống khủng bố trong tình hình hiện nay của lực lượng Công an" của Tạ Văn Roan, Học viện Cảnh sát.

Đề tài khoa học cấp Bộ: “Khủng bố và giải pháp phòng, chống khủng bố ở nước ta hiện nay” do PGS.TS. Hoàng Công Tư, Phó Tổng cục trưởng Tổng cục I, Bộ Công an làm Chủ nhiệm, nghiệm thu năm 2007.

Khủng bố trên không gian mạng thời cách mạng công nghiệp 4.0 và các biện pháp ứng phó của EU - An Toàn Thông Tin 2022, <http://m.antoanthongtin.vn/gp-atm/khung-bo-mang-thoi-cach-mang-cong-nghiep-40-va-cac-bien-phap-ung-pho-cua-eu-105434>.

Xem Goodman,M.D.,&Brenner,S.W., "Emerging Consensus on Criminal Conduct in Cyberspace", International Journal of Law and Information Technology, no2(2002).

Усилинский Ф. А. Кибертерроризм в России: его свойства и особенности. Право и кибербезопасность, 2014. № 1. С. 6-11.

TRAO ĐỔI VỀ AN NINH SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

Trung tá, ThS. Phạm Văn Tụ

Trường Đại học An ninh nhân dân

Email: phamtu.dhan@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> chuyển đổi số, bảo vệ thông tin cá nhân, năng lực số, rủi ro sinh viên,... <i>Keywords:</i> Digital transformation, personal information protection, digital competency, student risks,...	Sự phát triển ngày càng sâu rộng của khoa học công nghệ đã mở ra kỷ nguyên số Trong tất cả các lĩnh vực, điều đó đặt ra yêu cầu về nhận thức và kỹ năng chuyển đổi số cho con người. Để đào tạo ra nguồn nhân lực chất lượng cao phục vụ cho phát triển đất nước cần có sự đào tạo, phát triển cho sinh viên trong giai đoạn hiện nay có được hành trang phục vụ cho quá trình chuyển đổi số của quốc gia. Nâng cao năng lực số là nhu cầu tất yếu trong đào tạo nguồn nhân lực. Năng lực số là phát triển các kỹ năng để sinh viên thích ứng với môi trường chuyển đổi số và có kỹ năng lao động trong thời đại cách mạng công nghệ 4.0. Trong thời đại kỹ thuật số phồn thịnh ngày nay, đảm bảo an toàn và bảo vệ thông tin cá nhân trở thành một thách thức không thể phớt lờ. Cùng với sự phát triển nhanh chóng của công nghệ và mạng internet, các mối đe dọa an ninh số cũng ngày càng tinh vi và phức tạp hơn: thông tin bị đánh cắp, bị đọc lén hay bị thay đổi; thiết bị học tập bị hư hỏng, sự cố làm gián đoạn quá trình học tập; rủi ro bị chiếm đoạt tài sản, trục lợi trên mạng;... ABSTRACT The increasingly extensive development of science and technology has opened up the digital era. In all fields, it requires awareness and digital transformation skills for people. To train high-quality human resources to serve the country's development, it is necessary to have training and development for students in the current period to be

equipped to serve the country's digital transformation process. Improving digital capacity is an indispensable need in human resource training. Digital competency is to develop skills for students to adapt to the digital transformation environment and have labor skills in the era of the 4.0 technology revolution. In today's prosperous digital age, ensuring the safety and protection of personal information has become a challenge that cannot be ignored. Along with the rapid development of technology and the internet, digital security threats are also becoming more sophisticated and complex: information is stolen, read or changed; Learning equipment is damaged or incidents disrupt the learning process; risk of property appropriation, online profiteering;...

Sự phát triển ngày càng sâu rộng của khoa học công nghệ đã mở ra kỷ nguyên số. Trong tất cả các lĩnh vực, điều đó đặt ra yêu cầu về nhận thức và kỹ năng chuyển đổi số cho con người. Để đào tạo ra nguồn nhân lực chất lượng cao phục vụ cho phát triển đất nước cần có sự đào tạo, phát triển cho sinh viên trong giai đoạn hiện nay có được hành trang phục vụ cho quá trình chuyển đổi số của quốc gia. Nhìn nhận vấn đề này thể hiện ở việc sinh viên phải có khả năng thích ứng và làm chủ công nghệ, tham gia tích cực vào quá trình chuyển đổi số và linh hoạt trước mọi biến đổi của công nghệ. Chuyển đổi số là bước phát triển tiếp theo của tin học hóa, có được nhờ sự tiến bộ vượt bậc của những công nghệ mới mang tính đột phá, nhất là công nghệ số. Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số. Chuyển đổi số là một trong những mục tiêu được quan tâm hàng đầu của chính phủ cũng như các Bộ, ban ngành. Chuyển đổi số đang ngày một thay đổi nhận thức của những nhà lãnh đạo, những người có khả năng quyết định hướng đi và khả năng chuyển đổi thành công của Chính phủ, cơ quan, đơn vị, doanh nghiệp, tổ chức. Bộ máy chính quyền của nhiều quốc gia sau khi nhận ra tầm quan trọng của chuyển đổi số trong việc gia tăng hiệu quả hoạt động và đảm bảo an ninh quốc gia, đã lập tức bước vào một “cuộc đua” mới trong việc áp dụng chuyển đổi số.

Nâng cao năng lực số cho sinh viên trong thời kỳ chuyển đổi số:

Năng lực số vẫn còn là 1 khái niệm tương đối mới mẻ và chưa được nhiều người biết đến ở Việt Nam. Tuy nhiên, nâng cao năng lực số là nhu cầu tất yếu trong đào tạo nguồn nhân lực. Năng lực số là phát triển các kỹ năng để sinh viên thích ứng với môi trường chuyển đổi số và có kỹ năng lao động trong thời đại cách mạng công nghệ 4.0. Khung năng lực số có thể dựa trên 1 số tiêu chí sau:

- Vận hành thiết bị và phần mềm;
- Khai thác thông tin và dữ liệu;
- Giao tiếp và hợp tác trong môi trường số;
- An toàn và an ninh số;
- Sáng tạo nội dung số;
- Sáng tạo nội dung số;
- Học tập và phát triển kỹ năng số;
- Sử dụng năng lực số cho nghề nghiệp.

Sinh viên cần có nhận thức và sự chủ động tận dụng các cơ hội học tập, trao đổi cũng như tự hoàn thiện bản thân để có được năng lực số tốt hơn. Đó có thể là sự thông thạo, nhanh nhạy hơn trong việc sử lý các công cụ số như: máy tính cá nhân, điện thoại thông minh, mạng xã hội và các nền tảng ứng dụng. Tư duy phản biện để đánh giá lượng thông tin không lồ, đó cũng thể là năng lực duy trì những tương tác an toàn và tích cực, tham gia vào các cộng đồng số để hướng đến sự cân bằng cho cá nhân và toàn xã hội trên nền tảng của cái nhìn đa chiều và năng lực thấu cảm tôn trọng người khác. Quan trọng hơn là phục vụ cho việc học tập và phát triển sự nghiệp của mình trong tương lai.

Sinh viên hòa nhập vào hệ sinh thái chuyển đổi số của nhà trường. Sinh viên với việc ứng dụng công nghệ số vào mọi mặt đời sống, tích cực hòa nhập trải nghiệm, xây dựng thói quen, hành vi liên quan đến các công nghệ số từ cuộc sống hàng ngày vào quá trình học tập, nghiên cứu cũng như làm việc; hòa nhập một cách thoải mái vào các hệ sinh thái chuyển đổi số mà nhà trường hay các cơ quan, doanh nghiệp, các đơn vị công tác sau này.

Sinh viên trong quá trình nâng cao năng lực số cần có sự cá nhân hóa, có lộ trình: Công nghệ số là lĩnh vực mới, phát triển nhanh và đầy thách thức, khó khăn. Vì vậy, mỗi sinh viên phải tự có lộ lực phát triển năng lực số theo từng bước. Từ cơ bản đến nâng cao để có thể hoàn thiện bản thân. Phát triển năng lực số không chỉ dựa trên kỹ năng công nghệ mà còn là nhận thức về giá trị số trong đời sống xã hội, đồng nghĩa là phải hiểu và tự biết chăm sóc sức khỏe thể chất cũng như tinh thần của mình trong quá trình sử dụng các nền tảng này. Hạn chế sự lạm dụng, cân nhắc các yếu tố an toàn, quyền riêng tư và lợi ích của xã hội, quốc gia.

An ninh sinh viên trong thời kỳ chuyển đổi số và giáo dục an ninh số:

Trong thời đại kỹ thuật số phồn thịnh ngày nay, đảm bảo an toàn và bảo vệ thông tin cá nhân trở thành một thách thức không thể phớt lờ. Cùng với sự phát triển nhanh chóng của công nghệ và mạng internet, các mối đe dọa an ninh số cũng ngày càng tinh vi và phức tạp hơn. Các cuộc tấn công mạng và việc xâm nhập vào hệ thống thông tin cá nhân, doanh nghiệp và tổ chức đã trở thành mối đe dọa ngày càng tinh vi. Giáo dục an ninh số giúp chúng ta hiểu và ứng phó với những mối đe dọa này, từ việc bảo vệ thông tin cá nhân cho đến việc đảm bảo an toàn của hệ thống mạng. Đó là lý do tại sao giáo dục an ninh số trở thành một yếu tố quan trọng không thể thiếu trong thế giới kỹ thuật số ngày nay.

Giáo dục An ninh số trong thời kỳ chuyển đổi số không chỉ đơn thuần là việc hướng dẫn cách tạo mật khẩu mạnh hay cài đặt phần mềm chống virus mà đó là một quá trình liên tục, cung cấp kiến thức và kỹ năng cần thiết để nhận biết, đối phó và phòng ngừa các mối đe dọa an ninh trong không gian số. Giáo dục An ninh số giúp chúng ta hiểu rõ về các loại tấn công mạng, xâm nhập hệ thống, lừa đảo trực tuyến và vi phạm quyền riêng tư. Giáo dục an ninh số trong thời kỳ chuyển đổi số cũng đóng vai trò quan trọng trong việc phát triển tư duy an ninh và khả năng phản biện. Chúng ta học cách suy nghĩ một cách phản xạ và đánh giá các tình huống an ninh số, từ việc phân tích email độc hại đến nhận diện các trang web giả mạo, giúp sinh viên trở nên tự tin hơn trong việc sử dụng công nghệ mà không gặp nguy hiểm và đồng thời, có khả năng bảo vệ thông tin cá nhân và dữ liệu quan trọng của mình.

Một số rủi ro sinh viên có thể gặp phải trong quá trình chuyển đổi số và những vấn đề cần lưu ý:

Việc áp dụng công nghệ vào giáo dục là điều tất yếu vì có rất nhiều lợi ích từ nó, nhưng nếu quá lạm dụng hoặc sử dụng sai mục đích có thể gây ra những rủi ro:

- Thông tin bị đánh cắp, bị đọc lén hay bị thay đổi: tin tặc có thể thâm nhập vào các ứng dụng trao đổi thông tin để đánh cắp các thông tin quan trọng, tài liệu mật mà sinh viên không hề biết;
- Thiết bị học tập bị hư hỏng, sự cố làm gián đoạn quá trình học tập: trong quá trình sử dụng đồ điện tử có tỉ lệ lỗi nhất định hoặc không hoạt động khiến cho việc học tập trở nên khó khăn;
- Rủi ro bị chiếm đoạt tài sản, trục lợi trên mạng: việc áp dụng công nghệ vào giáo dục cũng có liên quan đến các khía cạnh tài chính, như cần mua tài liệu để học nhưng bị lừa đảo, chiếm đoạt tài sản.

An ninh sinh viên trong thời kỳ chuyển đổi số cần lưu ý:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

+ Đảm bảo an toàn và bảo mật thông tin trong giáo dục số là một vấn đề quan trọng, đặc biệt khi ngày càng có nhiều dữ liệu quan trọng được chia sẻ và lưu trữ trực tuyến.

+ Chính sách và quy định bảo mật: Các tổ chức giáo dục nên có chính sách và quy định rõ ràng về bảo mật thông tin, bao gồm việc xác định trách nhiệm và quy trình xử lý sự cố liên quan đến bảo mật.

+ Giáo dục và tập huấn về an ninh mạng: Đào tạo giáo viên, học sinh và nhân viên về các nguy cơ an ninh mạng, cách phòng chống và khắc phục khi xảy ra sự cố, giúp nâng cao ý thức và kỹ năng bảo vệ thông tin cá nhân và tổ chức.

+ Cập nhật và bảo trì phần mềm: Đảm bảo rằng tất cả các phần mềm, ứng dụng và hệ điều hành được cập nhật định kỳ và có các bản vá bảo mật để giảm thiểu nguy cơ bị tấn công.

+ Sử dụng mã hóa dữ liệu: Mã hóa dữ liệu quan trọng khi lưu trữ và truyền tải giúp ngăn chặn việc truy cập trái phép và đảm bảo tính bảo mật của thông tin.

+ Quản lý truy cập: Hạn chế và kiểm soát quyền truy cập vào dữ liệu nhạy cảm, chỉ cho phép những người có liên quan và được ủy quyền mới có thể truy cập.

+ Xác thực đa yếu tố: Sử dụng xác thực đa yếu tố (MFA) để đảm bảo rằng chỉ những người dùng hợp lệ mới có thể truy cập vào hệ thống và dữ liệu.

+ Sao lưu dữ liệu: Thường xuyên sao lưu dữ liệu quan trọng và lưu trữ ở nhiều nơi khác nhau để đảm bảo an toàn và phục hồi dữ liệu khi cần thiết.

+ Đánh giá và kiểm tra an ninh thông tin: Thực hiện đánh giá và kiểm tra an ninh hệ thống thông tin định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật, cũng như đảm bảo việc tuân thủ các chính sách và quy định bảo mật.

+ Hợp tác với các tổ chức chuyên nghiệp: Cộng tác với các tổ chức chuyên nghiệp về an ninh mạng để nhận được hỗ trợ, tư vấn và giải pháp phù hợp với nhu cầu và nguồn lực của tổ chức giáo dục.

+ Bằng cách thực hiện các biện pháp trên, các tổ chức giáo dục có thể bảo vệ thông tin và dữ liệu quan trọng của mình, đồng thời tạo ra một môi trường học tập trực tuyến an toàn và tin cậy cho giáo viên và học sinh.

+ An ninh sinh viên trong thời kỳ chuyển đổi số là một vấn đề quan trọng. Để bảo vệ thông tin cá nhân và dữ liệu của sinh viên trong môi trường số hóa, sinh viên cần: đặt mật khẩu mạnh mẽ (Sử dụng mật khẩu mạnh cho tài khoản của bạn và đảm bảo thay đổi chúng định kỳ, không nên sử dụng mật khẩu dễ đoán như ngày sinh hoặc số điện thoại); cập nhật phần mềm (đảm bảo rằng máy tính và thiết bị luôn được cập nhật phiên mới nhất); cài đặt và duy trì phần mềm diệt virus và phần mềm chống malware để bảo vệ khỏi các mối đe dọa trực tuyến; cẩn thận với email (hãy cẩn trọng khi mở email hoặc tệp đính kèm từ nguồn không rõ); sử dụng kết nối an toàn (sử dụng mạng Wi-Fi

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

được bảo vệ hoặc ứng dụng VPN khi kết nối với các dịch vụ trực tuyến); lưu trữ dữ liệu an toàn (đảm bảo dữ liệu quan trọng được lưu trữ an toàn trên các dịch vụ đám mây hoặc thiết bị lưu trữ riêng); giới hạn chia sẻ thông tin cá nhân (hạn chế việc chia sẻ thông tin cá nhân trên mạng xã hội và trang web công cộng); giám sát tài khoản (phát hiện hoạt động bất thường và sử dụng cơ chế bảo mật hai yếu tố nếu có sẵn); tư duy cảnh giác (hãy luôn tư duy cảnh giác trước khi chia sẻ thông tin cá nhân hoặc tiến hành các giao dịch trực tuyến quan trọng).

+ Đào tạo về an ninh số: Tìm hiểu về các nguy cơ và biện pháp bảo vệ an toàn trực tuyến thông qua các khóa học hoặc tài liệu hướng dẫn.

Trong quá trình sử dụng nền tảng số để học tập, sinh viên cần thực hiện tốt một số nội dung sau:

- Biết cách bảo mật thông tin, đặc biệt là các thông tin quan trọng như mật khẩu, tài khoản ngân hàng; sử dụng các kênh trao đổi thông tin có độ bảo mật cao; kiểm tra, bảo dưỡng định kỳ các thiết bị học tập, sửa chữa các công cụ nếu cần thiết; sử dụng các kênh mua bán, trao đổi tài liệu học tập chính thống, có bản quyền, được xác thực đầy đủ.

Trên đây là một số ý kiến đóng góp trao đổi về chủ đề hội thảo “An ninh sinh viên trong thời kỳ chuyển đổi số” tại Trường Đại học An ninh nhân dân.

PVT

ỨNG DỤNG NHẬN DẠNG KHUÔN MẶT TRONG QUẢN LÝ ĐIỂM DANH SINH VIÊN FACE RECOGNITION APPLICATION IN STUDENT ATTENDANCE MANAGEMENT

Phạm Mai Mẫn Nhi*

Trường Đại học Sư phạm Kỹ thuật TP. HCM

*Tác giả liên hệ: phammaimannhi@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa: nhận dạng khuôn mặt, điểm danh, so sánh khuôn mặt, phần mềm điểm danh, faceid</i>	Nhận dạng khuôn mặt người là một công nghệ được ứng dụng rộng rãi trong đời sống hằng ngày của con người như các hệ thống giám sát, quản lý vào ra, tìm kiếm thông tin người nổi tiếng,... có rất nhiều phương pháp nhận dạng khuôn mặt để nâng cao hiệu suất tuy nhiên dù ít hay nhiều những phương pháp này đang vấp phải những thử thách về độ sáng, hướng nghiêng, kích thước ảnh, hay ảnh hưởng của tham số môi trường. Một số tính năng mà Phần mềm điểm danh học sinh qua nhận diện khuôn mặt – AI đã đạt được: Xây dựng giao diện Menu, giao diện điểm danh, thiết kế giao diện cho phép xử lý các chức năng chính, thiết kế giao diện chương trình chính thực hiện các công việc, nhận diện khuôn mặt qua camera (tính hợp với camera an ninh, giám sát lớp học), quản lý buổi học, quản lý lớp học, quản lý thông tin và hình ảnh của học sinh, nhận diện chính xác, bằng phương pháp lưu hình ảnh của học sinh vào database và đối chiếu với khuôn mặt của học sinh tại thời điểm điểm danh, quản lý người dùng - giáo viên thực hiện thao tác điểm danh theo từng lớp học, xuất file CSV kết nối API với các phần mềm, ứng dụng khác, thống kê báo cáo theo buổi học, lớp học. ABSTRACT Human face recognition is a technology widely used in people's daily lives such as surveillance systems, access management, celebrity information search, etc. There are many recognition methods. face to improve performance, but to a greater or lesser extent, these methods are facing challenges in terms of brightness, orientation, image size, or the influence of environmental parameters. Some features of “Student Attendance Software via facial recognition

Keywords: facial recognition, attendance, face comparison, attendance software, faceid

– AI.” achieved: Building a Menu interface, attendance interface, designing an interface that allows handling main functions, designing the main program interface to perform tasks, recognizing faces via cameras (compatibility). with security cameras, classroom monitoring), lesson management, classroom management, student information and image management, accurate identification, by saving student images in the database and projecting students' faces at the time of attendance, user management - teachers perform attendance operations for each class, export CSV files to connect API with other software and applications, and report statistics by session or class.

1. Giới thiệu

Những năm gần đây, với sự bùng nổ về công nghệ nhằm phục vụ nhu cầu về học tập cũng như đời sống. Đồng hành với đó là công cuộc chuyển đổi số trong tất cả ngành nghề nói chung và trong giáo dục nói riêng. Chuyển đổi số ngành giáo dục đã tạo ra kỷ nguyên mới, thời đại mà người dạy và người học được trao quyền để sử dụng công nghệ. Các thành tựu công nghệ như Big data giúp lưu trữ mọi kiến thức lên không gian mạng, IoT (Internet vạn vật) giúp theo dõi hành vi của học sinh, quản lý, giám sát học sinh; hay Blockchain giúp xây dựng hệ thống quản lý thông tin và hồ sơ giáo dục của học sinh, cho phép hợp nhất, quản lý và chia sẻ dữ liệu từ nhiều trường học, ghi chép lại lịch sử học tập, bảng điểm của học sinh để đảm bảo thông tin dữ liệu được đồng nhất, minh bạch.

Với lý do đó nhóm tác giả đã tìm hiểu và thực hiện giải pháp: Phần mềm Điểm danh học sinh bằng nhận diện khuôn mặt sử dụng ngôn ngữ lập trình Python.

Khuôn mặt đóng vai trò quan trọng trong quá trình giao tiếp giữa người với người, và cũng mang một lượng thông tin giàu có, chẳng hạn có thể xác định giới tính, tuổi tác, trạng thái cảm xúc của người đó,... hơn nữa khảo sát chuyển động của các đường nét trên khuôn mặt có thể biết được người đó đang muốn nói gì.

Trong hệ thống nhận dạng người thì quá trình nhận dạng khuôn mặt được đánh giá là bước khó khăn và quan trọng nhất so với các bước còn lại của hệ thống. Do đó, nhận dạng khuôn mặt là điều quan trọng và cần thiết.

2. Cơ sở lý thuyết

2.1. Ngôn ngữ lập trình và thư viện

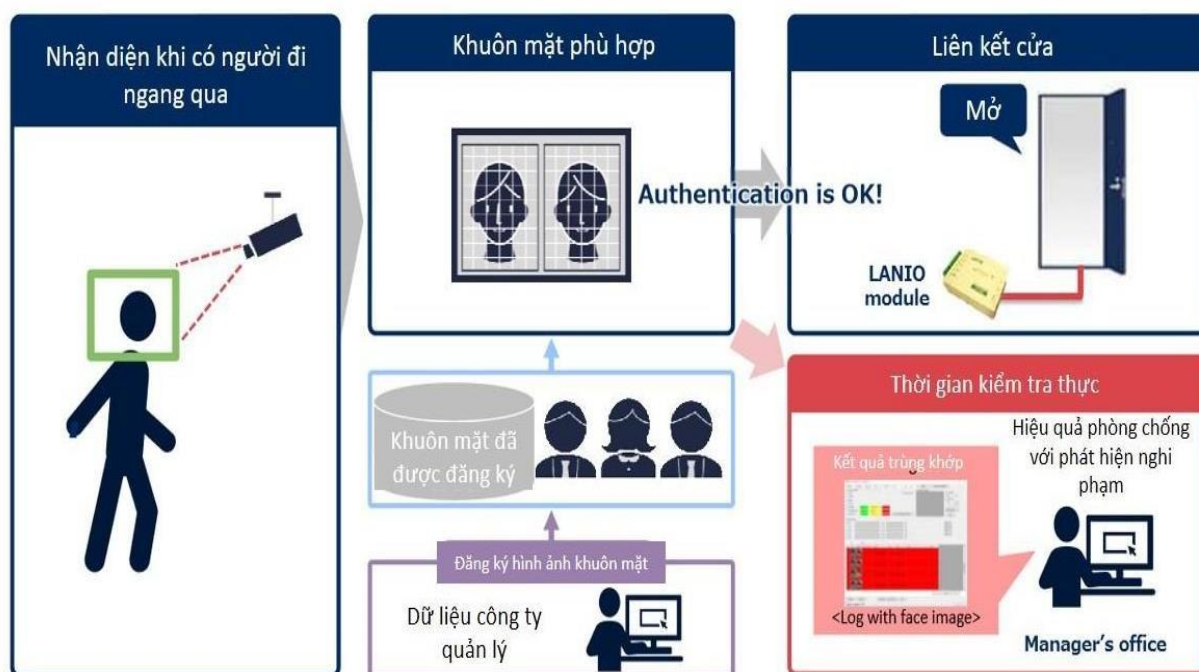
Python là ngôn ngữ lập trình hướng đối tượng, cấp cao, mạnh mẽ, được tạo ra bởi Guido van Rossum. Python có cú pháp đơn giản và dễ sử dụng, do đó nó trở thành một trong những ngôn ngữ lập trình nhập môn tốt nhất cho người mới bắt đầu.

Python có cấu trúc dữ liệu cao cấp mạnh mẽ và cách tiếp cận đơn giản nhưng hiệu quả đối với lập trình hướng đối tượng. Cú pháp lệnh của Python là điểm cộng vô cùng lớn vì sự rõ ràng, dễ hiểu và linh động, làm cho nó nhanh chóng trở thành một ngôn ngữ lý tưởng để viết script và phát triển ứng dụng trong nhiều lĩnh vực, ở hầu hết các nền tảng.

Project OpenCV được bắt đầu từ Intel năm 1999 bởi Gary Bradsky. OpenCV viết tắt cho Open Source Computer Vision Library. OpenCV là thư viện nguồn mở hàng đầu cho Computer Vision và Machine Learning, và hiện có thêm tính năng tăng tốc GPU cho các hoạt động theo real- time.

2.2. Nguyên lý hoạt động

Theo tính năng và ứng dụng của OpenCV, có thể chia thư viện này thành các nhóm tính năng và module tương ứng như sau.



Hình 1: Xử lý và hiển thị Hình ảnh / Video/ I/O (core, imgproc, highgui)

Bước 1: Nhận diện khuôn mặt

Máy ảnh phát hiện và định vị hình ảnh của một khuôn mặt khi đối tượng đang ở một mình hoặc trong một đám đông. Từ đó ghi nhận hình ảnh của đối tượng.

Bước 2: Phân tích khuôn mặt

Tiếp theo, hình ảnh khuôn mặt đối tượng được chụp lại và tiến hành phân tích. Hầu hết công nghệ nhận diện khuôn mặt dựa trên hình ảnh 2D thay vì 3D vì nó có thể khớp hình ảnh 2D với ảnh công khai trong cơ sở dữ liệu một cách thuận tiện và chính xác hơn. Sau đó đưa vào phần mềm để tiến hành đọc hình dạng khuôn mặt của đối tượng. Các yếu tố chính cần xử lý bao gồm khoảng cách giữa hai mắt, độ sâu của hốc

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

mắt, khoảng cách từ trán đến cằm, hình dạng của gò má và đường viền của môi, tai và cằm. Mục đích là để xác định các điểm mốc chính trên khuôn mặt nhằm phân biệt nhiều người khác nhau.

Bước 3: Chuyển đổi hình ảnh thành dữ liệu

Chuyển đổi ảnh chụp khuôn mặt thành một tập hợp thông tin kỹ thuật số (dữ liệu) dựa trên các đặc điểm khuôn mặt của người đó. Những thuộc tính khuôn mặt sẽ được xử lý dưới dạng các thuật toán và công thức, và mỗi người sẽ sở hữu một dữ liệu khuôn mặt riêng biệt.

Bước 4: Tìm kết quả nhận diện khuôn mặt phù hợp

Bước tiếp theo tiến hành so sánh với cơ sở dữ liệu khuôn mặt sẵn có. Nếu khuôn mặt được ghi lại khớp với một hình ảnh trong cơ sở dữ liệu, thì việc xác định sẽ hoàn tất.

3. Phương pháp nghiên cứu

3.1. Thiết kế phần mềm



Hình 2: Giao diện quản lý của phần mềm



Hình 3: Giao diện chức năng của hệ thống

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

The screenshot shows a web application titled "Quản lý thông tin Học sinh". It features a sidebar with a clock showing 17:00:46 PM on 27-11-2022. The main content area is divided into two sections. The left section, "Thông tin Học sinh", contains a "Thông tin khóa học" (Course Information) form with dropdowns for "Khóa học" and "Cơ sở", and a "Thông tin lớp học" (Class Information) form with fields for "ID Học sinh", "Tên Học sinh", "Lớp học", "CMND", "Giới tính", "Ngày sinh", "Email", "SDT", and "Địa chỉ". Below these are buttons for "Lưu", "Sửa", "Xóa", "Lấy ảnh học sinh", "Training Data", and "Xem ảnh". The right section, "Hệ Thống Tìm kiếm", includes a search bar with "Tìm kiếm theo: ID Học sinh" and buttons for "Tìm kiếm" and "Xem tất cả". Below this is a table listing students with columns for ID, Course, Base, Name, Class, and CMND. A "Quản lý lớp học" (Class Management) section is also visible, with a "Lớp học" dropdown, a "Tìm kiếm" button, and a "Xem tất cả" button. Below these are fields for "Lớp học" and "Tên lớp học", and buttons for "Thêm", "Xóa", "Cập nhật", and "Lấy ảnh".

Hình 4: Giao diện quản lý học sinh

The screenshot shows a web application titled "Hệ thống điểm danh khuôn mặt". It features a sidebar with a clock showing 17:18:19 PM on 27-11-2022. The main content area is divided into two sections. The left section, "Màn hình nhận diện", contains a "Chọn Lớp/Buổi học" dropdown and a "Chọn loại Điểm Danh" dropdown. Below these is a large gray area for the face recognition interface. At the bottom are buttons for "Mở Camera" and "Đóng Camera". The right section, "Điểm danh thành công", shows a silhouette of a person with a question mark. Below this are fields for "ID Học sinh", "Tên Học sinh", and "Thời gian". Below these are fields for "Lớp học", "ID Buổi học", and "Thời gian".

Hình 5: Giao diện điểm danh khuôn mặt

The screenshot shows a web application titled "Quản lý thông tin lịch học". It features a sidebar with a clock showing 17:18:19 PM on 27-11-2022. The main content area is divided into two sections. The left section, "Thông tin buổi học" (Class Session Information), contains fields for "ID Buổi học", "Giờ bắt đầu", "Giờ kết thúc", "Ngày", and "Lớp học". Below these are buttons for "Thêm mới", "Xóa", "Cập nhật", and "Lấy ảnh". The right section, "Hệ Thống Tìm kiếm", includes a search bar with "Tìm kiếm theo: ID Buổi học" and buttons for "Tìm kiếm" and "Xem tất cả". Below this is a table listing class sessions with columns for ID, Start Time, End Time, Date, and Class. Below the table are buttons for "Thêm", "Xóa", "Cập nhật", and "Lấy ảnh".

Hình 6: Giao diện quản lý lớp học

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Hệ thống quản lý điểm danh học sinh

Quản lý điểm danh

17:19:32 PM
27-11-2022

Quản lý thông tin điểm danh

Cập Nhật điểm danh

ID Điểm Danh:

ID Học sinh:

Tên Học sinh:

Lớp học:

Giờ vào:

Giờ ra:

Ngày:

Điểm danh:

ID Bài học:

Tìm kiếm theo: ID Điểm Danh

AttendanceID	ID Học sinh	Tên Học sinh	Lớp học	Giờ vào	Giờ ra	Ngày	ID Bài học	Điểm

Hình 7: Giao diện quản lý thông tin điểm danh

Hệ thống nhân diện khuôn mặt

Thông kê hệ thống

Số Học sinh
12

Số bản điểm danh
0

Số lần đi muộn
0

Số lần vắng
92

Học sinh đi muộn

ID Học sinh:

ID SV	Tên Học sinh	Lớp học	Ngày	ID Buổi học	Trạng thái

Học sinh vắng

ID Học sinh:

ID SV	Tên Học sinh	Lớp	Ngày	ID Buổi học	Trạng thái

Học sinh không điểm danh

ID Học sinh:

ID SV	Tên Học sinh	Lớp	Ngày	ID Buổi học	Trạng thái
7	Nguyễn Việt Hoa	SA	05/10/2022	SA	13
1	Le Quang Anh	SA	06/10/2022	SA	14
2	Do Mạnh Dũng	SA	06/10/2022	SA	14
3	Mai Quốc Khánh	SA	06/10/2022	SA	14
6	Trương Việt Hoàn	SA	06/10/2022	SA	14
7	Nguyễn Việt Hoa	SA	06/10/2022	SA	14
1	Le Quang Anh	SA	27/10/2022	SA	15
2	Do Mạnh Dũng	SA	27/10/2022	SA	15
3	Mai Quốc Khánh	SA	27/10/2022	SA	15
6	Trương Việt Hoàn	SA	27/10/2022	SA	15
7	Nguyễn Việt Hoa	SA	27/10/2022	SA	15
1	Le Quang Anh	SA	27/11/2022	SA	16
2	Do Mạnh Dũng	SA	27/11/2022	SA	16
3	Mai Quốc Khánh	SA	27/11/2022	SA	16
6	Trương Việt Hoàn	SA	27/11/2022	SA	16
7	Nguyễn Việt Hoa	SA	27/11/2022	SA	16

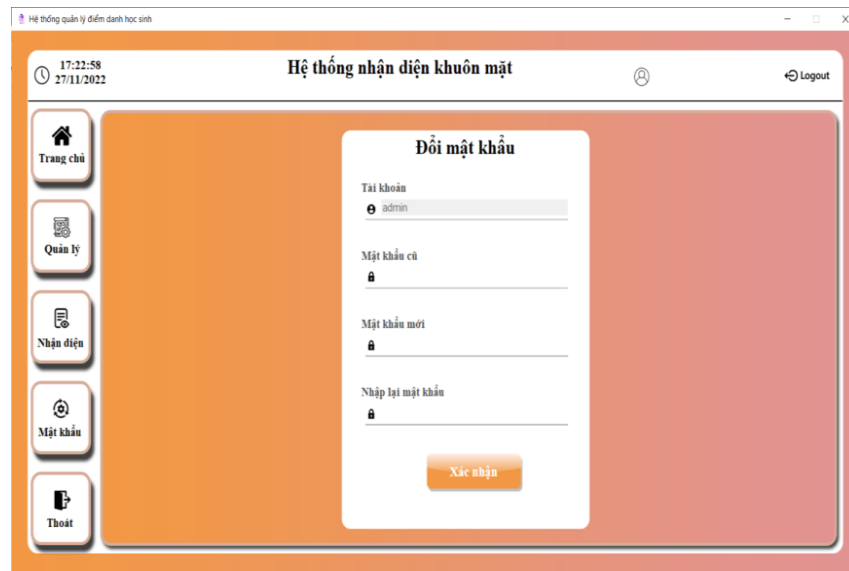
Hình 8: Giao diện thống kê

Quản lý thông tin

Thêm danh sách học sinh:

Thêm danh sách buổi học:

Hình 9: Giao diện xuất file báo cáo

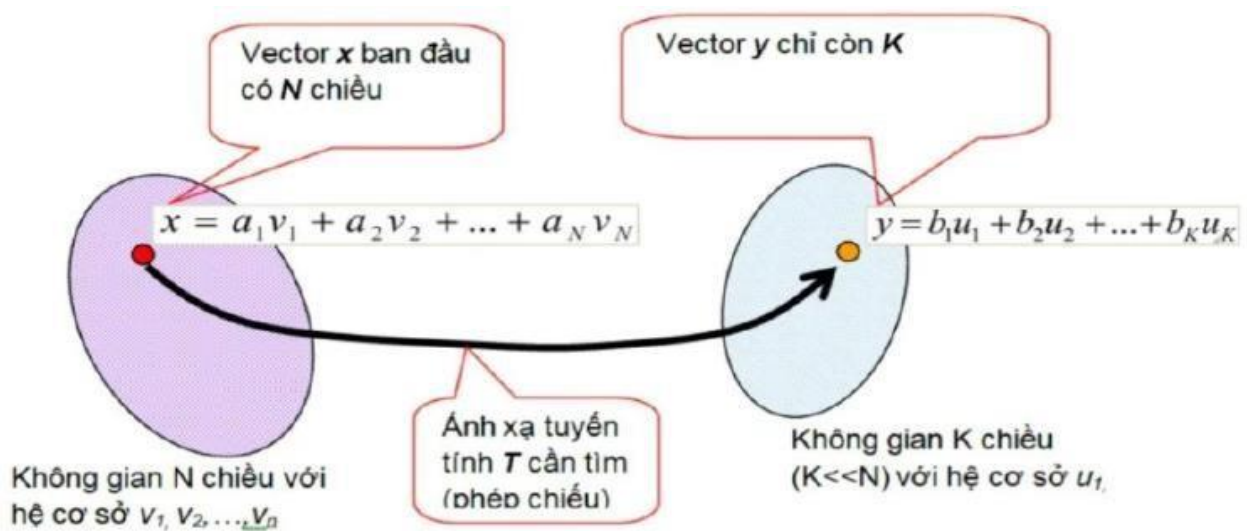


Hình 10: Giao diện cập nhật thông tin, thay đổi mật khẩu

3.2. Thuật toán nhận dạng khuôn mặt

Sử dụng thuật toán PCA để giảm số chiều của 1 tập vector sao cho vẫn đảm bảo được tối đa những thông tin quan trọng nhất. Sử dụng Feature Extraction giữ k thuộc tính “mới”.

Ứng dụng của PCA trong nhận diện khuôn mặt theo các bước sau: Tiền xử lý chuẩn hoá kích cỡ giữa ảnh trong cơ sở dữ liệu, tách khuôn mặt: khuôn mặt trên ảnh chụp được tách ra phần mặt, nó sẽ là các khuôn mặt cần tìm và chức năng trích chọn đặc trưng sẽ sử dụng các ảnh được tách ra này, trích chọn đặc trưng, tìm ra các đặc trưng chính của ảnh mặt, từ các đặc trưng này hình thành các vector đặc trưng, các vector này sẽ được sử dụng để đối sánh sự giống nhau giữa ảnh mặt cần tìm và ảnh mặt, so sánh giữa các vector đặc trưng để chọn ra độ tương tự giữa ảnh cần tìm và ảnh trong cơ sở dữ liệu.



Hình 11: Thuật toán PCA nhận dạng khuôn mặt

Ưu điểm của PCA khi nhận dạng khuôn mặt là giúp giảm số chiều của dữ liệu. Thay vì giữ lại các trục tọa độ của không gian cũ, PCA xây dựng một không gian mới ít chiều hơn, nhưng lại có khả năng biểu diễn dữ liệu tốt tương đương không gian cũ, nghĩa là đảm bảo độ biến thiên trên mỗi chiều mới. Các trục tọa độ trong không gian mới là tổ hợp tuyến tính của không gian cũ, do đó về mặt ngữ nghĩa, PCA xây dựng đặc trưng mới dựa trên quan sát được. Điểm hay là những đặc trưng này vẫn biểu diễn tốt dữ liệu ban đầu. Trong không gian mới, các liên kết tiềm ẩn của dữ liệu có thể được khám phá, mà nếu đặt trong không gian cũ thì khó phát hiện hơn, hoặc những liên kết như thế không thể hiện rõ.

4. Kết quả nghiên cứu và thảo luận

4.1. Thử nghiệm phần mềm

Thử nghiệm được kiểm tra trên nhiều sinh viên với các ảnh khuôn mặt và trang phục cùng điều kiện chụp hình ngoại cảnh sáng tối khác nhau.

Dữ liệu khuôn mặt được thực hiện tại Trường Đại học Sư phạm kỹ thuật TP. HCM với sinh viên Khoa Kế Toán. Tổng cơ sở dữ liệu bao gồm 52 khuôn mặt, mỗi khuôn mặt chụp 3 ảnh. Kết quả thử nghiệm được công bố như bảng sau.

Bảng 1

Thông kê kết quả tỷ lệ chính xác khi ứng dụng vào thực tế

Thử nghiệm lần thứ	Tổng số lượng sinh viên ghi vào cơ sở dữ liệu	Tổng số lượng khuôn mặt ghi vào cơ sở dữ liệu	Số lượng sinh viên quay lại để kiểm tra độ chính xác	Độ chính xác
1	18	54	9	100%
2	12	36	10	100%
3	22	66	22	100%

Ghi chú: Thực hiện tại Khoa Kế Toán, Trường Đại học Sư phạm kỹ thuật TP. HCM

Sau 3 lần thử nghiệm với tổng cộng 52 khuôn mặt và chọn các sinh viên bất kỳ quay lại để kiểm tra độ chính xác, tỷ lệ chính xác là tuyệt đối 100%. Như vậy phần mềm có độ chính xác cao trong quy mô một lớp học để điểm danh các sinh viên.

4.2. Thảo luận

Khả năng áp dụng của sản phẩm: Chương trình hoàn toàn có khả năng nhân rộng vào tất cả các trường học phổ thông, và cả giáo viên chủ nhiệm lớp. Từ tiểu học, đến cấp THPT và cả đại học đều có thể ứng dụng chương trình để quản lý và điểm danh học sinh trong nhà trường, giúp tiết kiệm thời gian, công sức của người quản lý nề nếp, giúp giáo viên có cái nhìn trực quan, tổng thể về tình hình vi phạm của học sinh, sinh viên toàn trường. Ở các phiên bản sau, chương trình sẽ được bổ sung chức năng phân quyền người dùng, mã hóa dữ liệu, nhập liệu qua mạng nội bộ, kiểm tra toàn vẹn dữ liệu, nhằm tăng cường tính năng bảo mật và thân thiện với người dùng.

4.3. Kết luận và gợi ý

Kết quả sau khi thử nghiệm phần mềm và thuật toán: Đáp ứng nhu cầu chuyển đổi số và ứng dụng công nghệ thông tin vào môi trường giáo dục, phần mềm đã cơ bản hoạt động hoàn chỉnh, kết nối với camera giám sát có sẵn tại lớp học, kiểm tra và đối chiếu hình ảnh khớp với cơ sở dữ liệu, thông tin học sinh và dữ liệu hình ảnh được nạp vào phần mềm khá hoàn chỉnh, tạo hứng khởi cho các bạn trong lớp khi áp dụng phần mềm, giúp giáo viên chủ nhiệm có thể kiểm tra quá trình điểm danh, vào, ra lớp học.

LỜI CẢM ƠN

Xin chân thành cảm ơn Trường Đại học Sư phạm Kỹ thuật TP. HCM đã tạo điều kiện để thử nghiệm phần mềm và kiểm tra độ chính xác trước khi chia sẻ thuật toán và mã nguồn phần mềm cho cộng đồng sử dụng.

TÀI LIỆU THAM KHẢO

- F. Faghri, D. J. Fleet, J. R. Kiros, and S. Fidler, “*Vse++: Improving visual-semantic embeddings with hard negatives*” arXiv preprint arXiv:1707.05612, 2017.15.
- P. Anderson, X. He, C. Buehler, D. Teney, M. Johnson, S. Gould, and L. Zhang, “*Bottom-up and top-down attention for image captioning and visual question answering*” in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 6077–6086, 2018.16.
- Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, “*Roberta: A robustly optimized bert pretraining approach*” arXiv preprint arXiv: 1907.11692, 2019.

TIỂU BAN 2: PHÁP LUẬT VÀ NHỮNG GIẢI PHÁP ĐẢM BẢO AN NINH SINH VIÊN

BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA SINH VIÊN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

Trần Thị Minh An

Hà Quang Bách

Trường Đại học Luật Hà Nội

Email: tranminhan3103@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> an ninh sinh viên; bảo vệ dữ liệu cá nhân của sinh viên; nhận thức pháp luật về bảo vệ dữ liệu cá nhân của sinh viên; thực hiện pháp luật trong bảo vệ dữ liệu cá nhân.	Nhận thấy, trong thời kỳ chuyển đổi số, sinh viên là một bộ phận lớn thường xuyên tham gia vào môi trường mạng nên các dữ liệu cá nhân của sinh viên có thể được coi là “mỏ vàng” dữ liệu để các đối tượng tội phạm mạng đánh cắp nhằm mục đích thu lợi bất chính. Vì vậy, an ninh sinh viên, bảo đảm an toàn thông tin cá nhân của sinh viên là vấn đề cần nghiên cứu nhằm hạn chế tối đa các nguy cơ đe dọa, ảnh hưởng xấu đến đời sống riêng tư của sinh viên. Trong khuôn khổ bài viết này, nhóm tác giả tập trung nghiên cứu cơ sở pháp lý hiện hành về bảo vệ dữ liệu cá nhân; thực trạng nhận thức pháp luật và thực hiện pháp luật trong hoạt động bảo vệ dữ liệu cá nhân của sinh viên hiện nay, đánh giá ưu điểm, hạn chế đối với vấn đề này; trên cơ sở đó, đề xuất một số kiến nghị, giải pháp góp phần nâng cao hiệu quả trong việc bảo vệ dữ liệu cá nhân của sinh viên.
<i>Keywords:</i> student security, student personal data protection, legal awareness of student personal data protection, legal compliance in safeguarding student personal data.	ABSTRACT We understand that during the digital transformation era, students, who are a significant part of the population, frequently engage in online environments. Therefore, students' personal data can be considered a "goldmine" of information for cybercriminals aiming to unlawfully profit. Consequently, ensuring the security of students and safeguarding their personal information has become a crucial issue that requires research to minimize potential threats and negative impacts on students' privacy. In this article, the authors focus on researching the current legal framework for personal data protection. They investigate the current legal awareness and compliance with data

protection laws in safeguarding students' personal data. The authors evaluate the advantages and limitations of the current situation and, based on this assessment, propose some recommendations and solutions to enhance the effectiveness of protecting students' personal data.

1. Giới thiệu

Bảo vệ an toàn dữ liệu cá nhân luôn là vấn đề thu hút sự quan tâm của tất cả mọi người, bởi những hệ lụy khôn lường có thể xảy ra bất cứ lúc nào khi các chủ thể mất kiểm soát hoặc vô tình để lộ thông tin cá nhân. Trong thời đại công nghệ ngày càng phát triển, cùng với đó là sự ra đời của Nghị định số 13/2023/NĐ-CP – bản pháp luật đầu tiên ghi nhận một cách đầy đủ và hệ thống các nội dung về dữ liệu cá nhân tại Việt Nam thì việc quan tâm tìm hiểu và thực hiện nghiêm chỉnh pháp luật đối với vấn đề này càng phải được nâng cao, đặc biệt đối với đối tượng là học sinh, sinh viên – những người thường xuyên truy cập và sử dụng mạng xã hội. Vì vậy, bài viết đã nghiên cứu các quy định của pháp luật Việt Nam hiện hành về bảo vệ dữ liệu cá nhân; vấn đề nhận thức pháp luật và thực hiện pháp luật của sinh viên hiện nay trong hoạt động bảo vệ dữ liệu cá nhân thông qua thực hiện khảo sát. Trên cơ sở kết quả khảo sát, nhóm tác giả đánh giá về thực trạng vấn đề này và đề xuất một số kiến nghị nhằm góp phần nâng cao hiệu quả hoạt động bảo vệ dữ liệu cá nhân của sinh viên trong thời kỳ chuyển đổi số.

2. Cơ sở lý thuyết

Để thực hiện việc nghiên cứu này, nhóm tác giả đã tham khảo, tìm hiểu một số bài viết, công trình nghiên cứu liên quan đến an toàn thông tin cá nhân như:

Luận văn thạc sĩ: “*Quản trị an ninh thông tin mạng xã hội trong sinh viên ở Việt Nam hiện nay*” năm 2021 của tác giả Nguyễn Khắc Vĩnh Lộc. Đây là công trình có liên quan gần gũi đến đề tài mà nhóm tác giả nghiên cứu. Ở công trình này, tác giả Nguyễn Khắc Vĩnh Lộc đã tìm hiểu các quy định pháp luật về an toàn thông tin mạng, đánh giá thực tế sử dụng mạng xã hội của sinh viên. Tuy nhiên, thời điểm này Nghị định 13/2023/NĐ-CP chưa được ban hành nên chưa có sự so sánh, đối chiếu những điểm mới trong các quy định. Đồng thời, chưa hình thành và sử dụng thống nhất thuật ngữ “dữ liệu cá nhân”. Bên cạnh đó, công trình chưa nghiên cứu và đánh giá sâu về nhận thức pháp luật của sinh viên đối với hoạt động bảo vệ dữ liệu cá nhân.

Bài viết: “*An toàn thông tin trong các trường đại học, cao đẳng*” được đăng trên Tạp chí CNTT&TT kỳ 2 (11.2015) của tác giả Đỗ Hữu Tuyền. Trong bài viết này, tác giả tập trung nghiên cứu những mối đe dọa về an toàn thông tin trong các trường đại học, cao đẳng và đưa ra ý kiến về xây dựng chiến lược đảm bảo an toàn thông tin trong

các trường cao đẳng, đại học. Vấn đề bảo vệ dữ liệu cá nhân của sinh viên không được nghiên cứu chuyên sâu trong bài viết.

Tài liệu: “*Hội nghị phổ biến hướng dẫn Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân*” trong Chương trình “Hội nghị phổ biến hướng dẫn Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân” do Bộ Công an tổ chức và Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an chủ trì vào ngày 07/6/2023 tại Hà Nội.

Ngoài ra, để có cơ sở và cái nhìn tổng quan các nội dung cần nghiên cứu, nhóm tác giả đã tìm hiểu một số bài viết, báo cáo thực tế và thực hiện khảo sát một số sinh viên liên quan đến quy định về bảo vệ dữ liệu cá nhân, thực tế thực hiện của các bạn về hoạt động này. Qua đó, nêu lên đánh giá và đề xuất kiến nghị.

3. Phương pháp nghiên cứu

Đối với phương pháp nghiên cứu, nhóm tác giả đã sử dụng kết hợp những phương pháp nghiên cứu, thu thập dữ liệu và xử lý thông tin khác nhau, cụ thể:

Phương pháp phân tích, tổng hợp về mặt lý thuyết để làm rõ vấn đề lý luận, quy định pháp luật hiện hành liên quan đến dữ liệu cá nhân và bảo vệ dữ liệu cá nhân.

Phương pháp chứng minh nhằm đưa ra các dẫn chứng về quy định, tài liệu... làm rõ nội dung lý luận.

Phương pháp xã hội học:

+ *Phương pháp phân tích tài liệu* dựa trên quy định pháp luật hiện hành về bảo vệ dữ liệu cá nhân; các công trình nghiên cứu; bài viết tạp chí; báo cáo của Bộ Giáo dục và Đào tạo; báo cáo của Bộ Công an.

+ *Phương pháp phỏng vấn*: Nhóm tác giả đã phỏng vấn sâu một số sinh viên theo học chuyên ngành luật trong các trường đại học, cao đẳng trên địa bàn Hà Nội để đánh giá về vấn đề nhận thức pháp luật của sinh viên đối với hoạt động bảo vệ dữ liệu cá nhân. Ngoài ra, nhóm tác giả cũng thực hiện phỏng vấn thông thường đối với các sinh viên để tìm hiểu thực tế thực hiện việc bảo đảm an toàn thông tin cá nhân của các bạn.

4. Kết quả nghiên cứu và thảo luận

4.1. Kết quả nghiên cứu

4.1.1. Quy định của pháp luật Việt Nam hiện hành về bảo vệ dữ liệu cá nhân

Trước đây, khái niệm về dữ liệu cá nhân chưa được quy định cụ thể tại bất kỳ văn bản pháp luật nào, trong mỗi văn bản pháp luật lại sử dụng thuật ngữ khác nhau khi muốn nói đến dữ liệu cá nhân như “thông tin cá nhân”, “thông tin riêng tư”, “thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình”. Vì vậy, chưa có cách hiểu thống nhất về khái niệm và nội hàm dữ liệu cá nhân, bảo vệ dữ liệu cá nhân. Tuy nhiên, hiện nay, sau khi Nghị định 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân được ban hành và có hiệu lực pháp luật đã tạo ra hành lang pháp lý rõ ràng về nội hàm thuật

ngữ dữ liệu cá nhân. Theo đó, “*Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm*” (khoản 1 Điều 2). Theo quy định này có thể hiểu dữ liệu cá nhân chính là thông tin, dấu hiệu giúp có thể xác định hoặc xác định chính xác một người cụ thể; các thông tin, dấu hiệu này có thể được nhận biết dưới nhiều dạng khác nhau như ký hiệu, chữ viết, chữ số, âm thanh, hình ảnh...

Do đó, bảo vệ dữ liệu cá nhân được hiểu là cách thức, phương thức mỗi cá nhân thực hiện, áp dụng để bảo vệ thông tin riêng tư của mình, từ đó nhằm ngăn chặn, phòng ngừa, xử lý vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật.

Về cơ bản, pháp luật Việt Nam quy định về phòng ngừa và bảo vệ dữ liệu cá nhân trong hầu hết các lĩnh vực cụ thể và được thể hiện tại nhiều văn bản khác nhau như Hiến pháp năm 2013, Bộ luật Dân sự năm 2015, Bộ luật Hình sự 2015 (sửa đổi, bổ sung 2017), Luật An toàn thông tin năm 2015, Luật Công nghệ thông tin năm 2006, Luật An ninh mạng 2018, Luật Bảo vệ người tiêu dùng năm 2010... Các văn bản này đều ghi nhận những phương thức bảo vệ dữ liệu cá nhân của chủ thể.

Trong Hiến pháp năm 2013 – văn bản có giá trị pháp lý cao nhất, tại Chương II về quyền con người quy định:

“1. Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình.

Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn.

2. Mọi người có quyền bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác.

Không ai được bóc mở, kiểm soát, thu giữ trái luật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư của người khác”.

Như vậy, Hiến pháp đã ghi nhận bảo vệ thông tin cá nhân dưới góc độ quyền cơ bản của con người. Đây là quyền được bảo vệ tuyệt đối và bất khả xâm phạm.

Tiếp tục tiếp cận dưới góc độ quyền con người, Bộ luật Dân sự năm 2015 ghi nhận bảo vệ thông tin cá nhân là một quyền dân sự. Theo đó, khoản 1 Điều 38 Bộ luật này quy định quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình như sau: “*Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ*”. Đồng thời, chế tài dân sự cũng đã được đặt ra để ngăn chặn hành vi xâm phạm dữ liệu cá nhân. Điều 11 Bộ luật này quy định 07 hình thức chế tài dân sự khi quyền dân sự bị xâm phạm.

Pháp luật hình sự bảo vệ thông tin cá nhân thông qua việc quy định các chế tài hình sự đối với những hành vi xâm phạm dữ liệu cá nhân, trong đó Điều 288 quy định bảo vệ quyền riêng tư, bí mật cá nhân trong môi trường mạng; Điều 159 quy định về tội

xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác; Điều 291 về tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng.

Bên cạnh đó, trong một số lĩnh vực chuyên ngành cụ thể có khả năng tiềm ẩn nhiều nguy cơ bị đánh cắp thông tin, dữ liệu cá nhân cũng dự liệu những quy định cụ thể nhằm phòng ngừa các hành vi xâm phạm đến quyền riêng tư của con người. Cụ thể, Luật Công nghệ thông tin năm 2006 quy định về thu thập, xử lý và sử dụng thông tin cá nhân trên môi trường mạng (Điều 21); Luật An ninh mạng năm 2018 quy định về phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng (Điều 17); Luật Bảo vệ người tiêu dùng năm 2010 quy định về bảo vệ thông tin người tiêu dùng (Điều 6); Luật Khám, chữa bệnh năm 2009 quy định quyền được tôn trọng bí mật riêng tư (Điều 8); Luật An toàn thông tin mạng năm 2015 quy định về nguyên tắc bảo đảm an toàn thông tin mạng (Điều 4)... Đồng thời, hiện nay, Nghị định 13/2023/NĐ-CP đã hệ thống lại quy định về bảo vệ dữ liệu cá nhân trong các ngành, lĩnh vực bằng việc quy định các chế định cụ thể trong hoạt động bảo vệ dữ liệu cá nhân nhằm tạo sự thống nhất trong việc kiểm soát, điều chỉnh các vấn đề phát sinh liên quan đến hành vi xâm phạm đời tư, bí mật cá nhân.

Tóm lại, có thể thấy rằng, các thông tin liên quan đến đời sống riêng tư của mỗi người là vấn đề quan trọng đã được nhận thức và quan tâm kịp thời bởi cơ quan nhà nước. Pháp luật bảo vệ dữ liệu cá nhân được ban hành đã tạo ra khung pháp lý chuẩn để mỗi cá nhân tự nhận thức được tầm quan trọng trong việc giữ gìn bí mật đời tư, đồng thời là cơ sở để các cơ quan có thẩm quyền dễ dàng kiểm soát, xử lý kịp thời khi phát hiện các hành vi xâm phạm đến dữ liệu cá nhân, hướng đến bảo đảm sự an toàn trong thời đại công nghệ thông tin phát triển mạnh mẽ như hiện nay.

4.1.2. Thực trạng bảo vệ dữ liệu cá nhân của sinh viên trong thời kỳ chuyển đổi số hiện nay

(i) Thực trạng nhận thức của sinh viên về các quy định pháp luật liên quan đến bảo vệ dữ liệu cá nhân

Trong thời đại công nghệ 4.0 hiện nay, sinh viên thuộc nhóm người sử dụng và tiếp xúc rất nhiều với Internet. Đặc biệt, khi đại dịch COVID-19 xuất hiện, do yêu cầu giãn cách xã hội, việc học tập tập trung của nhiều trường đại học, cao đẳng chuyển sang hình thức trực tuyến thì việc tham gia môi trường mạng của sinh viên càng lớn. Các Website, ứng dụng mạng xã hội phổ biến mà giới trẻ thường xuyên truy cập hiện nay có thể kể đến như Facebook, Zalo, Telegram, Tiktok, Instagram, Twitter, Youtube, các ứng dụng game, ứng dụng hẹn hò ... Tuy nhiên, đây chính là nơi tiềm ẩn rất nhiều rủi ro trên không gian mạng, là cơ hội cho tội phạm mạng tấn công và đánh cắp dữ liệu cá nhân

của chính các bạn sinh viên. Sở dĩ vậy là do khi sử dụng các ứng dụng mạng xã hội trên, người dùng thường khai báo thông tin đăng ký ở chế độ mở như thông tin ngày tháng năm sinh, trường học, nơi làm việc, nơi ở, số điện thoại ... Bên cạnh đó, trong quá trình sử dụng mạng xã hội, các bạn trẻ thường có thói quen cập nhật mọi hoạt động hàng ngày của họ một cách công khai.

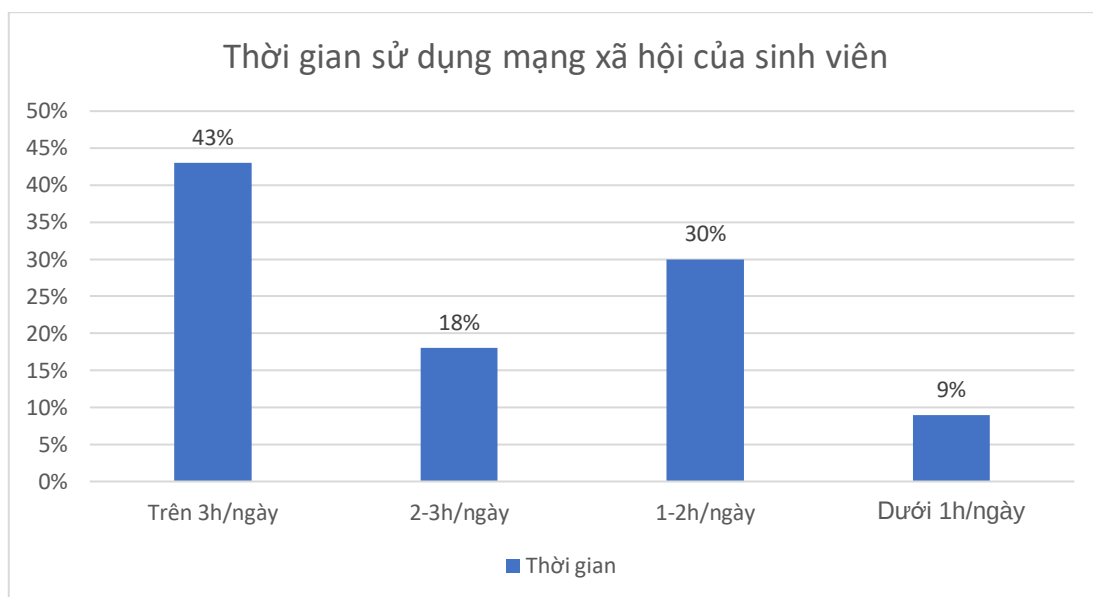
Tuy vậy, vẫn không thể phủ nhận, mạng xã hội chiếm một phần quan trọng trong đời sống tinh thần của sinh viên Việt Nam. ¹⁶Theo một nghiên cứu thống kê, mục đích tham gia mạng xã hội lớn nhất ở sinh viên đó là liên lạc và cập nhật thông tin về cuộc sống của gia đình, bạn bè (chiếm 41%). Bên cạnh đó, mục đích sử dụng mạng xã hội của sinh viên còn được thể hiện ở các nhu cầu khác như cập nhật tin tức xã hội (chiếm 23%), thể hiện bản thân (chiếm 15%), bày tỏ các ý kiến (chiếm 15%), giải trí (chiếm 12%), kinh doanh trên mạng (chiếm 6%).

Cũng theo khảo sát này, có đến 43% số sinh viên tham gia phỏng vấn trả lời thời gian sử dụng mạng xã hội trong ngày là trên 3h/ngày. Số sinh viên sử dụng mạng xã hội từ 2-3h/ngày chiếm 18%; 30% sử dụng mạng xã hội 1-2h/ngày và chỉ có 9% sinh viên được khảo sát sử dụng mạng xã hội dưới 1h/ngày.



Hình 1: Mục đích tham gia mạng xã hội của sinh viên

¹⁶ Nguyễn Khắc Vĩnh Lộc: *Quản trị an ninh thông tin mạng xã hội trong sinh viên ở Việt Nam hiện nay*, Luận văn Thạc sĩ, Đại học Quốc gia Hà Nội. Hà Nội, 2021



Hình 2: Thời gian sử dụng mạng xã hội của sinh viên

Ngoài ra, theo kết quả tại một khảo sát của Bộ GD&ĐT năm 2018, có 92.5% sinh viên và 84.5% học sinh cấp trung học thường xuyên sử dụng mạng xã hội Facebook. Trong đó, có 26% học sinh sinh viên sử dụng dưới 1h/ngày; 40% học sinh sinh viên sử dụng từ 1-3h/ngày và 34% học sinh sinh viên sử dụng hơn 3h/ngày. Bên cạnh đó, 45% học sinh sinh viên thường truy cập mạng xã hội Facebook bất kỳ lúc nào và có thiết bị truy cập trong tay (điện thoại, laptop); 12% học sinh sinh viên truy cập mạng xã hội Facebook bất cứ lúc nào nhận được thông báo mới¹⁷.

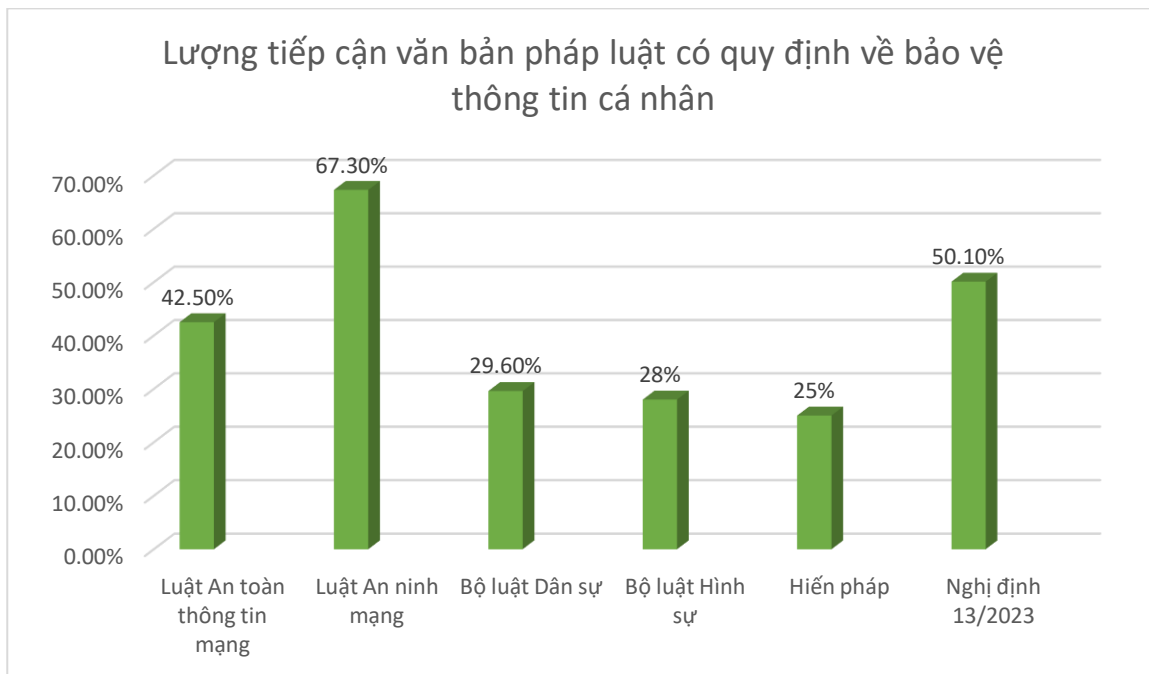
Như vậy, có thể thấy số lượng và thời lượng sinh viên tham gia vào mạng xã hội tương đối lớn. Từ đó cho thấy, đa số sinh viên đều tiếp cận thường xuyên, liên tục với môi trường mạng trong thời kỳ chuyển đổi số hiện nay.

Mặc khác, trong quá trình khảo sát, bên cạnh đa số sinh viên yêu thích và thường xuyên dùng mạng xã hội thì không ít người cho rằng hiện nay mạng xã hội xuất hiện khá nhiều kẻ lừa gạt và sử dụng mạng xã hội nhiều có thể gây ảnh hưởng không tốt đến đời sống riêng tư. Bởi khi công nghệ thông tin ngày càng phát triển mạnh mẽ thì sẽ xuất hiện càng nhiều lỗ hổng, nhiều kẻ cơ hội lợi dụng mạng xã hội để trục lợi. Phần đông sinh viên đều cảm nhận được rằng tính năng bảo mật của mạng xã hội không cao và không được đảm bảo. Tuy nhiên, các sinh viên này chỉ thể hiện ở thái độ băn khoăn vì biết mạng xã hội không thực sự an toàn nhưng vẫn không có động thái phòng tránh rủi ro này mà hầu hết khi tham gia sinh viên vẫn cung cấp đầy đủ thông tin cá nhân lên mạng xã hội, để chế độ công khai.

Trong số những sinh viên được khảo sát, đa số đều biết và quan tâm đến vấn đề an toàn thông tin khi sử dụng mạng xã hội nhưng lại chưa tìm hiểu sâu đến các cơ chế

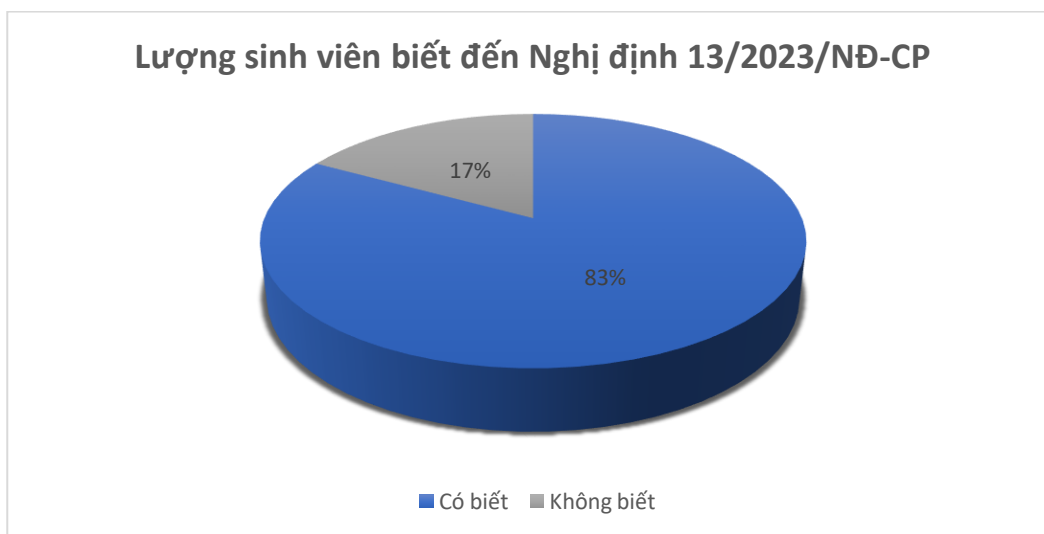
¹⁷ Thu An, *Giúp học sinh, sinh viên ứng xử lành mạnh trên môi trường mạng*, Báo Quân đội nhân dân, 19/7/2020.

bảo vệ cũng như chế tài phải chịu khi có hành vi xâm phạm dữ liệu cá nhân. Khi được hỏi đến lượng văn bản pháp luật hiện nay quy định nội dung liên quan đến bảo đảm an toàn thông tin cá nhân, bí mật đời sống riêng tư phần lớn sinh viên chỉ biết đến Luật An ninh mạng năm 2018. Ngoài ra, vấn đề này quy định trong các văn bản pháp luật chuyên ngành cụ thể hầu như không được sinh viên tiếp cận.



Hình 3: Lượng tiếp cận văn bản pháp luật có quy định về bảo vệ thông tin cá nhân

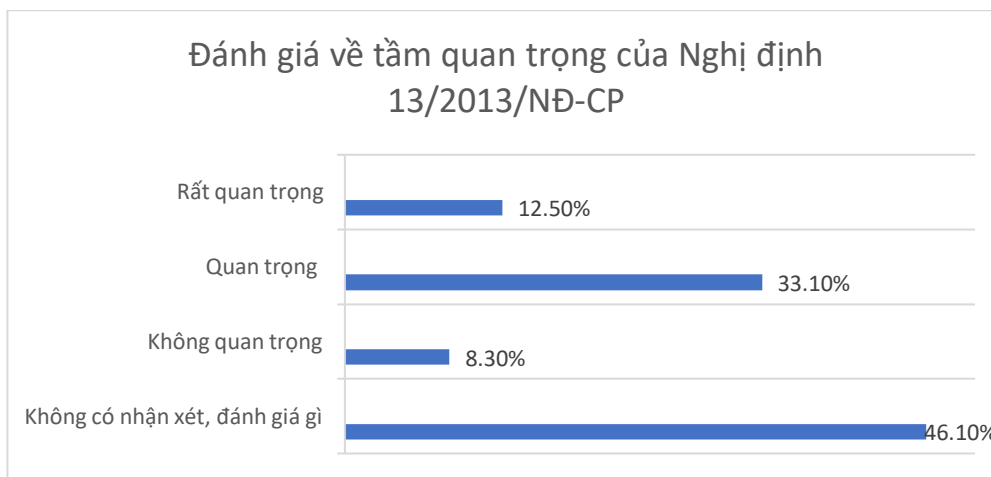
Đặc biệt hơn, trong quá trình nghiên cứu nội dung này, nhóm tác giả đã phỏng vấn sâu một số sinh viên theo học chuyên ngành luật của một số trường Cao đẳng, Đại học trên địa bàn thành phố Hà Nội về sự ra đời của Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Kết quả nhận được cho thấy, hầu hết sinh viên (chiếm 83%) biết đến Nghị định 13/2023/NĐ-CP. Phần còn lại cho rằng họ không biết đến nghị định mới quy định về bảo vệ dữ liệu cá nhân hiện nay (chiếm 17%).



Hình 4: Lượng sinh viên biết đến Nghị định 13/2013/NĐ-CP

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Trong số các sinh viên biết đến sự ra đời của Nghị định 13/2013/NĐ-CP, phần lớn các bạn chưa tiếp cận và tìm hiểu sâu về nội dung Nghị định này; chưa đánh giá và nhận thấy được tầm quan trọng, sự cần thiết của Nghị định 13 trong việc bảo vệ dữ liệu cá nhân, phòng ngừa, ngăn chặn và xử lý các hành vi xâm phạm liên quan đến dữ liệu cá nhân. Cụ thể, 46.1% số sinh viên được khảo sát biết đến Nghị định 13/2013/NĐ-CP đều không có nhận xét hay ý kiến gì về mức độ quan trọng của Nghị định này.



Hình 5: Đánh giá về tầm quan trọng của Nghị định 13/2013/NĐ-CP

Có thể thấy, nhận thức quy định pháp luật về bảo vệ dữ liệu cá nhân của sinh viên hiện nay còn ở mức sơ sài. Các bạn sinh viên mới chỉ dừng lại ở việc biết đến các quy định này nhưng chưa có ý thức tiếp cận và tìm hiểu sâu. Điều này dẫn đến sinh viên không thể nắm kỹ quy định về các quyền liên quan đến dữ liệu cá nhân mà mình được pháp luật bảo vệ, đồng thời không hiểu rõ các chế tài đối với hành vi xâm phạm dữ liệu cá nhân hiện nay. Việc không trang bị tốt những kiến thức về bảo vệ dữ liệu cá nhân cho bản thân nên thực tế nhiều bạn sinh viên bị đánh cắp thông tin riêng tư nhưng không xác định được nguyên nhân do đâu. Điển hình, ¹⁸theo thông tin chia sẻ từ một bạn sinh viên đang theo học tại một trường đại học ở thành phố Hồ Chí Minh cho biết, thông tin cá nhân của bạn đã bị đánh cắp nhưng không xác định được là từ nguồn nào. Theo đó, sinh viên này cùng người nhà liên tục bị đòi nợ tín dụng đe dọa yêu cầu trả nợ cho dù chưa từng sử dụng dịch vụ này. Đầu dây bên kia thông báo số tiền sinh viên này vay nợ không lớn nhưng lãi suất cao và có thể lên tới hàng chục triệu đồng nếu không trả sớm. Khi phủ nhận đây là thông tin không đúng, sinh viên này đã được phía đòi nợ đưa ra bằng chứng với hợp đồng có ghi chính xác số căn cước công dân và điện thoại, email, thậm chí có cả thông tin cá nhân của người thân. Cũng chính sinh viên này cho hay, các thông tin bên tín dụng có được đã được anh chia sẻ cho nhiều dịch vụ khác khi đăng ký nhưng chưa bao giờ dùng đến dịch vụ tín dụng nói trên.

¹⁸ <https://vnexpress.net/du-lieu-nguoi-viet-bi-thu-thap-va-loi-dung-the-nao-4498747.html>

(i) Thực trạng thực hiện bảo vệ dữ liệu cá nhân trong môi trường mạng của sinh viên hiện nay

Tiến hành khảo sát trên sinh viên tại các trường đại học cho thấy: Trong số những sinh viên được khảo sát, về cơ bản các sinh viên đều đã ý thức được đến vấn đề bảo vệ dữ liệu cá nhân của mình trên không gian mạng. Phần lớn sinh viên đều đã tiến hành bảo mật thông tin của mình trên các mạng xã hội như facebook, instagram hay Tiktok. Giới hạn những người có thể xem được thông tin về mình trên các nền tảng mạng xã hội này. Thêm vào đó, như trước đây nỡ rộ phong trào chụp ảnh check in những thông tin cá nhân như thẻ lên máy bay (Boarding Pass) thì hiện nay các bạn sinh viên cũng đã hạn chế hơn trong việc chia sẻ những thông tin này lên mạng.

Với tình trạng những đoạn link lạ, link chứa mã độc xuất hiện tràn lan trên các nền tảng mạng xã hội như hiện nay, các bạn sinh viên cũng đã cẩn trọng hơn trước khi click chuột vào một đường link nào đó. Sinh viên cũng đã có ý thức đăng xuất các tài khoản mạng xã hội sau khi dùng máy tính công cộng. Cá biệt, có những sinh viên có ý thức rất tốt trong việc bảo vệ dữ liệu cá nhân, các bạn luôn cập nhật phần mềm một cách thường xuyên nhằm đảm bảo hệ thống bảo mật của phần mềm luôn trong trạng thái hoạt động tốt nhất. Bên cạnh đó, sinh viên hiện nay cũng đã thường xuyên đổi mật khẩu các tài khoản của mình và áp dụng những mật khẩu khó đoán để tăng tính bảo mật.

Ngoài đa số sinh viên có ý thức bảo vệ dữ liệu cá nhân của mình khi tham gia môi trường mạng thì vẫn còn tồn tại một bộ phận sinh viên còn khá cởi mở khi thường xuyên chia sẻ thông tin đời tư một cách công khai; xem nhẹ tầm quan trọng của bí mật đời tư, thậm chí có những hành vi xâm phạm thông tin cá nhân của người khác. Số lượng sinh viên này tuy không nhiều nhưng cũng là hồi chuông cảnh tỉnh trong việc mất cảnh giác, mất an toàn khi bảo vệ dữ liệu cá nhân của sinh viên, có thể gây ra nhiều hệ lụy không lường cho chính các bạn và gia đình.

(i) Thực trạng về mức độ an toàn trong việc bảo vệ dữ liệu cá nhân của sinh viên hiện nay

Có thể thấy rằng, hiện nay hầu hết sinh viên đều biết và sử dụng thường xuyên mạng xã hội nhưng phần lớn sinh viên khi tham gia mạng xã hội chưa được trang bị đầy đủ kiến thức pháp luật, kỹ năng bảo mật thông tin riêng tư; chưa nhận thức sâu sắc các tác hại của việc “rò rỉ” thông tin cá nhân trên mạng xã hội và chưa có ý thức trong việc phòng ngừa, bảo mật dữ liệu cá nhân trong thời kỳ chuyển đổi số hiện nay. Đây chính là vấn đề quan trọng cần nghiên cứu, đánh giá và phải có giải pháp kịp thời bởi chỉ khi nào sinh viên nhận thức được tầm quan trọng của việc bảo vệ dữ liệu cá nhân, hiểu được những nguy hại có thể xảy ra khi tham gia mạng xã hội thì mới có thái độ cảnh giác, hành động phòng ngừa rủi ro do mặt trái của công nghệ thông tin mang lại.

Hiện nay, tội phạm mạng còn tấn công vào các nhà trường, cơ sở giáo dục để tiếp cận nguồn thông tin dữ liệu cá nhân của sinh viên nhằm mục đích trục lợi, mua bán dữ

liệu cá nhân. Các thông tin cá nhân của sinh viên được lưu trữ trong các nhà trường có thể coi là “mỏ vàng” dữ liệu cá nhân, là “miếng mồi ngon” cho các đối tượng nhòm ngó lấy cắp. Theo thống kê, 36% số trường đại học bị một đợt tấn công trên mạng mỗi giờ¹⁹. Năm 2016, theo báo cáo về Đạo luật Clery: 78% tội phạm hướng đến sinh viên và nhân viên trong trường đại học²⁰. Giáo dục bậc cao là khu vực chiếm 17% các vụ xâm nhập dữ liệu với thông tin cá nhân bị đánh cắp, chỉ đứng sau ngành y tế²¹.

Tiếp đến, trong báo cáo được công bố ngày 02/8/2022 của Proofpoint cũng đã chỉ ra rằng, 97% trong số các trường đại học được khảo sát của Hoa Kỳ, Anh và Úc đang khiến sinh viên, nhân viên và ban quản lý nhà trường phải chịu rủi ro cao trong việc gặp phải những cuộc tấn công mạo danh email và các cuộc tấn công khác thông qua email vì hệ thống an ninh thiếu hụt bảo mật cơ bản. Đặc biệt trong số đó có cấp độ bảo vệ an toàn thông tin kém nhất là các trường đại học của Hoa Kỳ²².

Nhóm dữ liệu có được do liên kết của các trường đại học với các tổ chức bên ngoài như tổ chức y tế, chính trị, các viện nghiên cứu hoặc doanh nghiệp cũng là một trong những mối đe dọa chính về an toàn thông tin trong các trường đại học, cao đẳng.



Hình 6: Nguy cơ mất an toàn dữ liệu cá nhân của sinh viên và nhân viên trong các trường đại học theo Đạo luật Clery

Ngoài ra, theo báo cáo của Cục An toàn thông tin, Bộ Thông tin và truyền thông, thời gian qua thế giới cũng như Việt Nam đã xảy ra nhiều trường hợp lộ lọt dữ liệu cá

¹⁹ VMWare, Thách thức học đường: Tấn công mạng trong trường đại học, 2016

²⁰ Bộ Giáo dục Hoa Kỳ, Công cụ phân tích dữ liệu an toàn và bảo mật trong trường học, 2018

²¹ HUB, Trường Đại học – Một mỏ vàng dữ liệu cá nhân cho tin tặc, 2017

²² Dương Trường: Các trường đại học hàng đầu Châu Âu khiến người dùng email gặp rủi ro an ninh mạng, đường link: <https://antoanthongtin.vn/an-toan-thong-tin/cac-truong-dai-hoc-hang-dau-o-chau-au-khien-nguoi-dung-email-gap-rui-ro-an-ninh-mang-108264>, truy cập ngày 12/9/2023

nhân. Tại Việt Nam, ngoài vụ lộ thông tin 400.000 khách hàng của một hãng hàng không (năm 2017) thì thời gian sau đó xuất hiện không ít vụ rao bán hàng triệu thông tin cá nhân (được cho là thông tin khách hàng) trên mạng... Thực trạng này là hồi chuông cảnh báo về vấn đề bảo mật dữ liệu cá nhân tại Việt Nam, vì có thể gây ảnh hưởng không nhỏ đến quyền riêng tư, bí mật cá nhân, có thể dẫn đến tình trạng lừa đảo công nghệ cao, cũng như các hành vi phạm pháp khác...

Thêm vào đó, việc rò rỉ dữ liệu cá nhân đang là mối lo chung của nhiều cơ quan chức năng khi những thông tin, dữ liệu cá nhân của người dùng, thường được khai báo khi đăng ký những ứng dụng như Facebook, zalo,... tưởng chừng vô hại nhưng lại bị các đối tượng xấu lợi dụng thủ đoạn để thu thập. Đỉnh điểm vào năm 2021, khoảng 17 GB dữ liệu cá nhân của người Việt gồm chứng minh thư nhân dân (CMTND), căn cước công dân (CCCD), sổ hộ khẩu, ảnh và video selfie... trở thành món hàng trị giá 9.000 USD đối với hacker. Dù chưa thể truy ra nguồn gốc số liệu đó và kẻ rao bán hiện đã xóa bài đăng, song vụ việc vẫn cho thấy đã có lỗ hổng trong quản lý những dữ liệu quan trọng này.

Mặt khác, không thể không nhắc đến những hình thức thu thập dữ liệu cá nhân một cách trái phép đang ngày càng trở nên phổ biến, có thể kể đến như việc các công ty cung cấp dịch vụ, ứng dụng bán cho khách hàng những ứng dụng có đính kèm phần mềm thu thập thông tin trái phép. Khi người dùng sử dụng ứng dụng, doanh nghiệp hoặc nhà phát hành sẽ nhận được các thông tin cá nhân về địa chỉ IP, địa điểm, thậm chí cả số điện thoại của người sử dụng ứng dụng trong khi đó, chỉ nhà cung cấp dịch vụ là các công ty viễn thông mới có thể biết những thông tin này²³.

Từ những dẫn chứng thực tế về mức độ nguy hiểm của việc rò rỉ thông tin cá nhân hiện nay có thể thấy rằng, học sinh, sinh viên không thuộc vùng ngoại lệ trong các vụ mua bán, xâm nhập dữ liệu cá nhân; các thông tin riêng tư của các bạn sinh viên đều có thể bị các đối tượng tội phạm mạng đánh cắp bất cứ lúc nào khi chúng tiếp cận được với dữ liệu cá nhân trên các ứng dụng mạng xã hội, tài khoản ngân hàng cũng như hệ thống lưu trữ thông tin cá nhân trong các trường học. Mức độ đe dọa sự an toàn trong bảo vệ dữ liệu cá nhân của sinh viên là tương đối lớn và tiềm ẩn nhiều nguy cơ đe dọa đến đời sống riêng tư của chính các bạn và gia đình.

Việc mất an toàn trong bảo vệ dữ liệu cá nhân, bí mật đời tư xuất phát từ nhiều nguyên nhân khác nhau. Qua tìm hiểu, nhóm tác giả nhận thấy, việc lộ, lọt dữ liệu cá nhân ở Việt Nam chủ yếu do hai nhóm nguyên nhân chính là yếu tố kỹ thuật (các lỗ hổng trong việc quản lý an toàn hệ thống mạng như lỗ hổng trong chính sách cung cấp dịch vụ hoặc lỗ hổng về mặt lập trình) và yếu tố phi kỹ thuật (xuất phát từ nhận thức và kinh nghiệm thực tế của các bạn

²³Thành Luân-Anh Quân: Vụ rò rỉ 17 GB dữ liệu người dùng Việt: Cách bảo vệ thông tin cá nhân, đường link: <https://thanhluan.vn/vu-ro-ri-17-gb-du-lieu-nguoi-dung-viet-cach-bao-ve-thong-tin-ca-nhan-1851069078.htm>, truy cập ngày 12/9/2023

sinh viên; thông qua các thủ đoạn tinh xảo của tội phạm mạng; các chế tài xử phạt hành vi xâm phạm dữ liệu cá nhân chưa đủ tính răn đe; công tác tuyên truyền, phổ biến quy định pháp luật về bảo vệ dữ liệu cá nhân chưa được đề cao).

Tuy nhiên, trong khuôn khổ bài viết, nhóm tác giả tập trung làm rõ một số nguyên nhân do yếu tố phi kỹ thuật gây ra như nhận thức và kinh nghiệm thực tế của sinh viên trong việc bảo vệ dữ liệu cá nhân còn sơ sài; vấn đề đảm bảo dữ liệu cá nhân trong các nhà trường chưa được quan tâm đúng mức; các chế tài xử phạt hành vi xâm phạm dữ liệu cá nhân chưa đủ tính răn đe; công tác tuyên truyền, phổ biến quy định pháp luật về bảo vệ dữ liệu cá nhân chưa được đề cao.

Về nhận thức và kinh nghiệm thực tế của sinh viên trong việc bảo vệ dữ liệu cá nhân: Qua nghiên cứu cho thấy, hầu hết sinh viên hiện nay chưa trang bị cho mình những kiến thức pháp luật về bảo vệ dữ liệu cá nhân; chưa nắm rõ quyền được đảm bảo an toàn thông tin cá nhân; chưa quan tâm đến các chế tài phải chịu khi làm lộ thông tin cá nhân của người khác. Đồng thời, các bạn sinh viên đang thiếu sự phòng ngừa khi tham gia môi trường mạng; còn khá cởi mở trong việc chia sẻ thông tin đời tư một cách công khai.

Bên cạnh đó, *vấn đề kiểm soát an toàn thông tin trong các trường đại học, cao đẳng* chưa được siết chặt cũng là nguyên nhân khiến dữ liệu cá nhân của sinh viên thậm chí của cả giáo viên và phụ huynh học sinh bị lấy cắp. Thực tế, nhiều nhà trường còn yếu về kiến thức, thiếu về kinh nghiệm và lúng túng khi có sự cố về vấn đề đảm bảo an toàn thông tin xảy ra. Trong các báo cáo về những lỗ hổng bảo mật hoặc các website bị tấn công hoặc có nguy cơ bị tấn công của Công ty an ninh mạng Bkav tại Việt Nam, website của các trường đại học luôn chiếm một tỉ lệ lớn.

Các chế tài xử phạt hành vi xâm phạm dữ liệu cá nhân còn nhẹ, chưa đủ tính răn đe. Về chế tài hình sự, mức hình phạt cao nhất dành cho hành vi xâm phạm dữ liệu cá nhân nói chung là 07 năm tù. Về chế tài hành chính, mức phạt tiền cao nhất được quy định tại Nghị định 15/2020/NĐ-CP là 70.000.000 đồng đối với cá nhân và 140.000.000 đồng đối với tổ chức. Trong khi đó, lợi nhuận thu được từ việc xâm chiếm, đánh cắp dữ liệu cá nhân lớn hơn rất nhiều so với mức phạt phải gánh chịu.

Công tác tuyên truyền, phổ biến pháp luật liên quan đến bảo vệ dữ liệu cá nhân hiện nay chưa được chú trọng. Sinh viên chưa được tuyên truyền đầy đủ các quy định/văn bản pháp luật mới, điều chỉnh trực tiếp đến quyền được bảo đảm an toàn dữ liệu cá nhân. Vì vậy, hiện nay hầu hết sinh viên chưa ý thức được mức độ quan trọng của dữ liệu cá nhân, chưa có những biện pháp phù hợp, đúng đắn để tự bảo vệ một cách tốt nhất thông tin cá nhân của mình.

4.2. Thảo luận

Nhận thấy tầm quan trọng trong việc bảo vệ dữ liệu cá nhân nói chung và an toàn sinh viên nói riêng, nhóm tác giả nghiên cứu và tìm hiểu vấn đề này với mong muốn có

được cái nhìn thực tế, khách quan trong việc nhận thức và thực hiện pháp luật về bảo vệ dữ liệu cá nhân của sinh viên tại các trường cao đẳng, đại học. Đặc biệt, trong tình hình bối cảnh chuyển đổi số ngày một phát triển, cùng với sự ra đời của Nghị định 13/2023/NĐ-CP – văn bản đầu tiên ghi nhận một cách đầy đủ và hệ thống các nội dung về dữ liệu cá nhân tại Việt Nam thì việc quan tâm tìm hiểu và thực hiện nghiêm chỉnh pháp luật đối với vấn đề này càng phải được nâng cao. Mặc khác, đến nay chưa có nhiều nghiên cứu về an ninh sinh viên trong thời kỳ chuyển đổi số; chưa có sự đánh giá chi tiết về mức độ nhận thức pháp luật và thực hiện pháp luật của các bạn sinh viên trong hoạt động bảo vệ dữ liệu cá nhân ở giai đoạn hiện nay. Vì vậy, bài viết đã đi sâu vào nghiên cứu vấn đề này nhằm góp phần hoàn thiện những thiếu hụt trên. Đồng thời, thông qua kết quả nghiên cứu có thể mang đến những góc nhìn chân thực để các nhà làm luật, các cơ quan có thẩm quyền xem xét, đánh giá toàn diện vấn đề về bảo vệ dữ liệu cá nhân của sinh viên; từ đó sẽ có những biện pháp phù hợp nhằm nâng cao ý thức pháp luật của sinh viên, cũng như giúp các nhà trường thực hiện tốt việc bảo mật an toàn thông tin sinh viên, hạn chế tối đa các cuộc tấn công vào hệ thống an ninh trong các nhà trường làm “rò rỉ” khối lượng lớn dữ liệu cá nhân của sinh viên và giáo viên trong các trường cao đẳng, đại học.

5. Kết luận và gợi ý

Qua việc nghiên cứu và khảo sát, nhóm tác giả nhận thấy, hoạt động bảo vệ dữ liệu cá nhân nói chung và của sinh viên nói riêng hiện nay còn đang tồn tại nhiều nguy cơ mất an toàn. Vấn đề này xuất phát từ nhiều nguyên nhân khác nhau như sinh viên chưa được trang bị tốt kiến thức pháp luật về bảo vệ dữ liệu cá nhân, chưa có ý thức tiếp cận, tìm hiểu sâu các quyền được bảo đảm đối với bí mật đời tư mà pháp luật quy định cùng các chế tài xử phạt phải gánh chịu khi có hành vi vi phạm, dẫn đến hầu hết sinh viên chưa chủ động phòng ngừa, ngăn chặn các hành vi xâm phạm dữ liệu cá nhân trên không gian mạng. Bên cạnh đó, hiện nay hệ thống lưu trữ dữ liệu thông tin sinh viên trong các trường đại học, cao đẳng có cấp độ bảo vệ kém; cùng với đó công tác tuyên truyền, giáo dục cho sinh viên về tầm quan trọng của dữ liệu cá nhân và các văn bản pháp luật đang dự liệu về vấn đề này chưa được chú trọng. Ngoài ra, chế tài của pháp luật đối với hoạt động xâm chiếm dữ liệu cá nhân còn nhẹ, chưa đủ sức răn đe cũng là vấn đề cần nghiên cứu. Từ kết quả nghiên cứu trên, nhóm tác giả đưa ra một số giải pháp sau giúp nâng cao hiệu quả hoạt động bảo vệ dữ liệu cá nhân của sinh viên:

Thứ nhất, hoàn thiện pháp luật bảo vệ dữ liệu cá nhân: Hiện nay, Nghị định 13/2023/NĐ-CP được ban hành đã lấp đầy lỗ hổng pháp luật, tạo ra khung pháp lý chuẩn và thống nhất trong cách hiểu và phân loại dữ liệu cá nhân; quy định chi tiết các hoạt động bảo vệ dữ liệu cá nhân cho các chủ thể. Tuy nhiên, với việc biến động không ngừng của đời sống xã hội, trong tương lai sẽ xuất hiện những loại dữ liệu mới mà không nằm trong nghị định

khiến việc áp dụng pháp luật gặp nhiều vướng mắc. Ví dụ, Nghị định 13/2013/NĐ-CP quy định rằng “Số chứng minh nhân dân, số hộ chiếu, số căn cước công dân, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội” là những dữ liệu cơ bản tuy nhiên lại để ngỏ giấy chứng nhận quyền sở hữu nhà là dữ liệu cá nhân.

Vì vậy, cần nghiên cứu để có hướng dẫn phân loại rõ ràng, bao quát và có tính dự liệu hơn đối với dữ liệu cá nhân; xác định rõ chế tài và tạo căn cứ pháp lý để phòng ngừa, đấu tranh với các hành vi xâm phạm việc bảo vệ dữ liệu cá nhân hiện nay như tăng mức chế tài hình sự và hành chính đối với hành vi xâm phạm dữ liệu cá nhân. Ngoài ra, việc xem xét thành lập cơ quan chuyên trách các vấn đề liên quan đến giám sát, bảo đảm thực hiện bảo vệ dữ liệu cá nhân cũng là điều cần thiết giúp nâng cao nhận thức của người dân nói chung và sinh viên nói riêng đối với vấn đề này.

Đồng thời, cần tăng cường mức chế tài hình sự cũng như hành chính và quy định các hành vi xâm phạm dữ liệu cá nhân trong các văn bản luật. Vì lý do các chế tài về xử lý xâm phạm dữ liệu cá nhân còn quá nhẹ, không đủ sức giáo dục và răn đe. So sánh với chế tài ở các nước trên thế giới cho thấy mức chế tài của Việt Nam là chưa tương xứng với mức độ nghiêm trọng của hành vi vi phạm cũng như chưa đảm bảo tính răn đe. Cùng với nâng cao chế tài, nước ta còn cần nghiên cứu tội phạm hóa đối với hành vi thu thập, sử dụng, khai thác, chuyển nhượng trái phép dữ liệu cá nhân gây hậu quả nghiêm trọng, từ đó bổ sung các quy định về tội phạm hình sự có liên quan trong Bộ luật hình sự hiện hành với biện pháp chế tài áp dụng cho cá nhân cũng như pháp nhân.

Thứ hai, cần tiến hành đẩy mạnh tuyên truyền, giáo dục, nâng cao ý thức xã hội và xây dựng văn hóa bảo vệ dữ liệu cá nhân trong sinh viên. Để làm tốt vấn đề này, các trường đại học có thể tổ chức các buổi Hội thảo, tọa đàm cho sinh viên nhằm cung cấp thêm kiến thức, góc nhìn về pháp luật liên quan đến hoạt động bảo vệ dữ liệu cá nhân. Bên cạnh đó, việc thiết lập phòng ban chuyên thực hiện công tác nghiên cứu, cập nhật và phổ biến pháp luật đến sinh viên cũng là điều cần thiết.

Thứ ba, cần xây dựng chiến lược đảm bảo an toàn thông tin trong các trường cao đẳng, đại học. Đứng trên góc độ quản lý, các trường đại học, cao đẳng cần xác định 3 bước phải làm để xây dựng và phát triển một chiến lược an ninh mạng ổn định nhằm thiết lập tuyến phòng vệ chuyên sâu giúp bảo đảm an toàn dữ liệu cá nhân của sinh viên, đó là²⁴:

- Đánh giá rủi ro bằng cách xác định các nhóm dữ liệu, phát hiện lỗ hổng và thiết lập các ưu tiên quản lý;
- Xây dựng và thực hiện nghiêm túc các giải pháp, chính sách như quản trị doanh nghiệp, quản trị dữ liệu, thiết lập các lớp an ninh mạng;

²⁴ Đỗ Hữu Tuyển: An toàn thông tin trong các trường đại học, cao đẳng; bài đăng trên Tạp chí CNTT&TT kỳ 2 (11.2015)

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Giám sát và báo cáo định kỳ dựa trên đặc thù của từng đơn vị như thay đổi hành vi, nhận thức người dùng; đồng thời chia sẻ và cập nhật kiến thức thường xuyên.

Thứ tư, cần đề cao trách nhiệm và tăng cường phối hợp giữa các cơ quan nhà nước liên quan đến dữ liệu cá nhân. Bảo vệ dữ liệu cá nhân liên quan đến nhiều cơ quan quản lý trong các lĩnh vực chuyên ngành, các cơ quan này đóng vai trò tổ chức thực hiện pháp luật như bộ tư pháp, bộ tài chính, bộ thông tin và truyền thông. Chính phủ cần quy định chặt chẽ sẽ phân công, phối hợp giữa các cơ quan có liên quan đến bảo vệ dữ liệu cá nhân để không dẫn đến tình trạng đùn đẩy trách nhiệm giữa các cơ quan khi có vi phạm xảy ra. Đồng thời chính phủ là chủ thể đóng vai trò quan trọng trong việc phát triển các doanh nghiệp công nghệ như FPT, BKAV,... góp phần bảo vệ dữ liệu cá nhân.

LỜI CẢM ƠN

Để hoàn thành bài nghiên cứu này, nhóm tác giả xin gửi lời cảm ơn chân thành đến:

Ban Giám hiệu trường Đại Học Luật Hà Nội vì đã tạo điều kiện về cơ sở vật chất với hệ thống thư viện hiện đại, đa dạng các loại sách, tài liệu thuận lợi cho việc tìm kiếm, nghiên cứu thông tin.

Xin cảm ơn các giảng viên bộ môn đã giảng dạy tận tình, chi tiết để nhóm tác giả có đủ kiến thức và vận dụng chúng vào bài nghiên cứu này.

Do chưa có nhiều kinh nghiệm làm đề tài cũng như những hạn chế về kiến thức trong nghiên cứu chắc chắn sẽ không tránh khỏi những thiếu sót. Rất mong nhận được sự nhận xét, ý kiến đóng góp, phê bình từ phía Ban Giám khảo để bài tham luận được hoàn thiện hơn.

Lời cuối cùng, nhóm tác giả xin kính chúc Ban tổ chức Hội thảo nhiều sức khỏe, thành công và hạnh phúc.

TÀI LIỆU THAM KHẢO

Nguyễn Khắc Vĩnh Lộc. (2021). *Quản trị an ninh thông tin mạng xã hội trong sinh viên ở Việt Nam hiện nay*. Luận văn Thạc sĩ, Đại học Quốc gia Hà Nội. Hà Nội.

Đỗ Hữu Tuyển. (2015). *An toàn thông tin trong các trường đại học, cao đẳng*. Bài đăng trên Tạp chí CNTT&TT kỳ 2 (11.2015), 27.

Thu An. (2020). *Giúp học sinh, sinh viên ứng xử lành mạnh trên môi trường mạng*, Báo Quân đội nhân dân.

<https://vnexpress.net/du-lieu-nguoi-viet-bi-thu-thap-va-loi-dung-the-nao-4498747.html>

VMWare. (2016). *Thách thức học đường: Tấn công mạng trong trường đại học*.

Bộ Giáo dục Hoa kỳ. (2018). *Công cụ phân tích dữ liệu an toàn và bảo mật trong trường học*.

HUB. (2017). *Trường Đại học – Một mỏ vàng dữ liệu cá nhân cho tin tặc*.

Dương Trường: *Các trường đại học hàng đầu Châu Âu khiến người dùng email gặp rủi ro an ninh mạng*, đường link: <https://antoanthongtin.vn/an-toan-thong-tin/cac->

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

truong-dai-hoc-hang-dau-o-chau-au-khien-nguoi-dung-email-gap-rui-ro-an-ninh-mang-108264, truy cập ngày 12/9/2023.

Thành Luân-Anh Quân: *Vụ rò rỉ 17 GB dữ liệu người dùng Việt: Cách bảo vệ thông tin cá nhân*, đường link: <https://thanhnien.vn/vu-ro-ri-17-gb-du-lieu-nguoi-dung-viet-cach-bao-ve-thong-tin-ca-nhan-1851069078.htm>, truy cập ngày 12/9/2023.

**BẮT NẠT TRỰC TUYẾN TRONG SINH VIÊN –
THỰC TRẠNG VÀ GIẢI PHÁP PHÒNG NGỪA
CYBERBULLYING AMONG STUDENTS – CURRENT SITUATION AND
PREVENTION SOLUTIONS**

Trần Linh Huân^{1*}, Lê Thị Châu Giang²

¹ Câu lạc bộ các Nhà khoa học trẻ TP. Hồ Chí Minh, Việt Nam

² Trường Đại học Luật TP. Hồ Chí Minh, Việt Nam

*Tác giả liên hệ, Email: linhhuantran@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Bắt nạt trực tuyến, sinh viên, thực trạng, giải pháp, phòng ngừa. <i>Keywords:</i> Cyberbullying, students, situation, solutions, prevention.	Bắt nạt trực tuyến trong sinh viên (Cyberbullying) là một trong những vấn nạn đang ngày càng đáng báo động, nhất là trong thời đại công nghệ số hiện nay. Sự phát triển mạnh mẽ của công nghệ thông tin đã mang lại cho sinh viên rất nhiều lợi ích trong việc học tập, nghiên cứu, giải trí,... Tuy nhiên, bên cạnh những giá trị tốt đẹp mà công nghệ thông tin mang lại thì vẫn còn tồn tại những hạn chế nhất định, tiêu biểu trong số đó là vấn đề bắt nạt trực tuyến, đây là một mối đe dọa an ninh trong môi trường số, ảnh hưởng đến cuộc sống của sinh viên và gây ra nhiều hệ lụy vô cùng lớn. Do đó, chúng ta cần phải nhận thức rõ về vấn đề này để kịp thời đưa ra các biện pháp giải quyết, hạn chế rủi ro, tạo lập và duy trì an toàn trực tuyến trong cộng đồng. Bài viết này tập trung nghiên cứu, đánh giá tầm quan trọng của việc phòng ngừa bắt nạt trực tuyến, đồng thời nêu lên thực trạng hành vi bắt nạt trực tuyến trong sinh viên và từ đó đề xuất một số giải pháp phòng ngừa. ABSTRACT Cyberbullying among students is one of the increasingly alarming problems, especially in the current digital age. The strong development of information technology has brought students a lot of benefits in studying, researching and entertainment,... However, in addition to the good values that information technology

brings, there are still certain limitations, typical of which is the problem of cyberbullying, this is a security threat in the digital environment, affecting the lives of students and causing many great consequences. Therefore, we need to be aware of this issue to promptly put measures in place, limit risks, create and maintain online safety in the community. This article focuses on researching and assessing the importance of cyberbullying prevention, while highlighting the situation of cyberbullying behavior among students and thereby proposing some prevention solutions.

1. Đặt vấn đề

Chuyển đổi số - xu hướng tất yếu hiện nay đang phát triển mạnh mẽ ở đa số các quốc gia trên thế giới. Đây là một chặng đường với sự đột phá của các công nghệ số dẫn đến sự thông minh hóa mọi mặt của đời sống xã hội²⁵, tác động lớn đến cuộc sống của con người và thúc đẩy sự phát triển của kỷ nguyên công nghệ hiện đại. Cách mạng 4.0 đã làm thay đổi cách chúng ta sống, làm việc và giao tiếp. Trong khoảng thời gian dịch bệnh Covid-19 bùng phát, khi phải thực hiện giãn cách xã hội, các biện pháp học tập, làm việc và sinh hoạt đều phải thực hiện bằng phương thức trực tuyến. Có thể thấy, việc sử dụng internet mang lại cho chúng ta rất nhiều lợi ích, tuy nhiên, đây cũng là “cơ hội” để các hành vi vi phạm pháp luật như lừa đảo, bắt nạt, ... được thực hiện. Trong môi trường học đường, hiện tượng bắt nạt trực tuyến đang ngày càng gia tăng và trở thành vấn nạn đáng báo động. Bằng các hành vi như gửi tin nhắn xúc phạm, chia sẻ thông tin cá nhân nhạy cảm mà không có sự chấp thuận, tạo nhóm trên mạng xã hội để công khai xúc phạm người khác, hoặc lan truyền tin đồn, hình ảnh xấu, ... bắt nạt trực tuyến có thể gây ra tác động tâm lý nghiêm trọng đối với sinh viên, nạn nhân có thể trở nên căng thẳng, lo lắng, mất tự tin và mất niềm tin vào bản thân. Điều này có thể ảnh hưởng đến sức khỏe, bao gồm tăng nguy cơ mắc trầm cảm, lo âu, tự tử và giảm chất lượng cuộc sống, trong học tập và quan hệ xã hội của họ. Việt Nam mặc dù đã ban hành Luật An ninh mạng năm 2018 và Bộ quy tắc ứng xử trên mạng xã hội nhưng việc thi hành trên thực tế vẫn chưa thực sự mang lại hiệu quả cao, những hành vi bắt nạt trực tuyến ngày càng diễn ra thường xuyên hơn và gây ra nhiều hậu quả khó lường. Để khắc phục được tình trạng này, ý thức cá nhân của cá nhân đóng vai trò quan trọng nhất, cùng với đó là

²⁵ Ban tuyên giáo Tỉnh ủy Hà Giang (2022), “Hỏi – đáp về chuyển đổi số (Tập 1)”, https://s3.khaothi.online/xcbt-files/P3/BTGHAGIANG/documents/HOI-DAP-CHUYEN-DOI-SO-TP-10X14.5_12.pdf, truy cập ngày 29/8/2023.

sự đồng lòng của cả xã hội và sự giúp đỡ từ phía cơ quan nhà nước có thẩm quyền. Internet là một công cụ không thể thiếu trong cuộc sống hiện đại, nhưng sử dụng internet như thế nào cho văn minh, phù hợp là điều mà tất cả chúng ta cần phải chú ý. Nhận thức rõ về bản chất của bắt nạt trực tuyến sẽ giúp chúng ta kịp thời đề ra các biện pháp phòng ngừa, đồng thời biết cách xử lý khi có hiện tượng bắt nạt trực tuyến xảy ra để bảo vệ sự an toàn cho mọi người trong không gian số, góp phần xây dựng một xã hội lành mạnh, không còn tồn tại vấn nạn bắt nạt trực tuyến.

2. Tầm quan trọng của việc phòng ngừa bắt nạt trực tuyến trong sinh viên

Theo cuốn Từ điển Tiếng Việt (2003), “bắt nạt” là *cậy thế, cậy quyền dọa dẫm để làm cho phải sợ*²⁶. Tổ chức National Centre Against Bullying tại Úc định nghĩa: “*bắt nạt là hành vi lạm dụng quyền lực liên tục và có chủ ý trong các mối quan hệ thông qua hành vi lặp đi lặp lại bằng lời nói, thể chất và/hoặc xã hội nhằm mục đích gây tổn hại về thể chất, xã hội và/hoặc tâm lý*”²⁷. Chúng ta thường bắt nạt là việc cố ý thực hiện hành vi như dùng vũ lực, lời nói tác động trực tiếp lên nạn nhân. Tuy nhiên, trong thời kỳ công nghệ số có tồn tại hành động bắt nạt mới mà không thông qua hình thức sử dụng vũ lực bằng hành vi hoặc lời nói trực tiếp mà bằng các hành động khác có sự hỗ trợ của khoa học kỹ thuật, khoa học gọi đây là “bắt nạt trực tuyến” (Cyberbullying). Theo định nghĩa từ Unicef²⁸, “*bắt nạt trực tuyến là việc sử dụng các công nghệ kỹ thuật số, có thể diễn ra trên phương tiện truyền thông xã hội, các nền tảng nhắn tin, nền tảng game và điện thoại di động. Đó là hành vi lặp lại nhằm mục đích gây sợ hãi, tức giận hoặc xấu hổ đối với những người được nhắm là mục tiêu*”²⁹. Cambridge Dictionary đưa ra định nghĩa “bắt nạt trực tuyến” là “*hoạt động sử dụng Internet để gây hại hoặc khiến cho người khác sợ hãi, đặc biệt là bằng cách gửi cho họ những tin nhắn khó chịu*”³⁰. Như vậy, bắt nạt trực tuyến là hành vi được thực hiện một cách cố ý gián tiếp bằng từ ngữ, hình ảnh hoặc âm thanh thông qua việc sử dụng công nghệ thông tin để đưa thông tin sai sự thật, xúc phạm người khác nhằm mục đích gây tổn thương tinh thần và danh dự của nạn nhân. Hành vi này được lặp đi lặp lại nhiều lần và có thể xảy ra ở bất kỳ nơi nào, bất kỳ lúc nào khi kẻ bắt nạt có cơ hội tiếp cận với các phương tiện điện tử. Cụ thể, người bắt nạt sẽ gửi những tin nhắn với lời lẽ xúc phạm người khác qua nhóm chat, diễn đàn trên mạng xã hội, lan truyền những thông tin sai lệch hoặc tin đồn không có căn cứ

²⁶ Hoàng Phê (2003), “Từ điển Tiếng Việt”, <https://archive.org/details/tu-dien-tieng-viet-vien-ngon-ngu-hoc/page/46/mode/2up>, truy cập ngày 29/8/2023.

²⁷ National Centre Against Bullying (n.d), “Definition of bullying”, <https://www.ncab.org.au/bullying-advice/bullying-for-parents/definition-of-bullying/>, truy cập ngày 29/8/2023.

²⁸ United Nations International Children's Emergency Fund (Quỹ Nhi đồng Liên hợp quốc)

²⁹ Unicef (n.d), “Cyberbullying: What is it and how to stop it”, <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>, truy cập ngày 29/8/2023.

³⁰ Cambridge Dictionary, <https://dictionary.cambridge.org/vi/dictionary/english/cyberbullying>, truy cập ngày 29/8/2023.

về người khác, gây tổn hại đến danh dự của họ, đăng tải những hình ảnh hoặc video nhạy cảm, xấu hổ của người khác mà không được sự cho phép của nạn nhân, ... Tuy không thực hiện hành vi nhưng những người bình luận (comment) vào những bài viết đó, hòa theo cổ vũ dù chưa biết rõ sự việc đúng hay sai cũng được xem là người bắt nạt. Khi trở thành nạn nhân của bắt nạt trực tuyến, tinh thần, tâm lý của sinh viên sẽ ảnh hưởng rất nhiều. Họ cảm thấy xấu hổ, lo lắng về những gì mọi người bàn tán về mình, điều này có thể dẫn đến việc rút lui khỏi bạn bè gia đình và xã hội, những suy nghĩ tiêu cực, cảm thấy tội lỗi về những điều họ đã làm hoặc không làm, từ đó gây ra căng thẳng, lo âu, trầm cảm và tự ti, khó khăn trong việc học tập và tham gia vào các hoạt động giáo dục. Trốn học hoặc bỏ học là một tác động phổ biến khác của bắt nạt trực tuyến và có thể ảnh hưởng đến sức khỏe tâm thần của sinh viên, nguy cơ cao họ sẽ sử dụng các chất kích thích như rượu và ma túy hoặc hành vi bạo lực để đối phó với nỗi đau tâm lý và thể chất của họ. Từ những hậu quả nêu trên, có thể thấy, việc phòng ngừa bạo lực trực tuyến trong sinh viên hiện nay là vô cùng quan trọng, cụ thể:

Thứ nhất, đối với sinh viên. Phòng ngừa bạo lực trực tuyến giúp bảo vệ tâm lý và sức khỏe của sinh viên, chúng ta có thể giảm thiểu căng thẳng, trầm cảm, lo âu và các vấn đề tâm lý khác mà sinh viên có thể gặp phải. Bên cạnh đó, chúng ta tạo ra một môi trường học tập an toàn và khuyến khích sự tương tác xã hội tích cực, sinh viên có thể tập trung vào việc học, tham gia vào hoạt động giáo dục và phát triển bản thân một cách tốt nhất. Môi quan hệ tốt đẹp giữa sinh viên với nhau cũng được xây dựng và duy trì, khuyến khích sự tôn trọng, đồng cảm và hỗ trợ lẫn nhau trong cộng đồng sinh viên. Ngoài ra, việc phòng ngừa còn góp phần bảo vệ quyền và tự do cá nhân của sinh viên, đảm bảo rằng sinh viên có quyền được tự do, an toàn và tôn trọng trong môi trường trực tuyến.

Thứ hai, đối với xã hội. Phòng ngừa bạo lực trực tuyến trong sinh viên sẽ góp phần xây dựng một xã hội văn minh và an toàn, giáo dục một thế hệ trẻ lành mạnh, ứng xử văn minh trên không gian số và giảm thiểu hậu quả xã hội của bạo lực trực tuyến. Bên cạnh đó, vấn đề đạo đức trong thời đại thông tin cũng được cải thiện đáng kể, nâng cao ý thức sử dụng mạng an toàn cho sinh viên. Chúng ta sẽ tạo nên một môi trường số an toàn, lành mạnh, nơi mà các sinh viên có thể học tập, làm việc, tự tin thể hiện mình mà không gặp bất kỳ một mối đe dọa nào.

3. Thực trạng hành vi bắt nạt trực tuyến trong sinh viên hiện nay

Tại Việt Nam, số lượng sinh viên bị bắt nạt ngày càng gia tăng. Theo một khảo sát sinh viên của 3 trường Đại học trên địa bàn TP. Hồ Chí Minh, kết quả cho thấy có tới 56% sinh viên bị đánh cắp thông tin, mật khẩu, 69% trường hợp từng là nạn nhân của bạo lực trên không gian mạng bằng nhiều hình thức.³¹ Các hành vi bắt nạt trực tuyến

³¹ Hà Ánh (2023), “69% sinh viên từng là nạn nhân của bạo lực trên mạng”, <https://thanhnien.vn/69-sinh-vien-tung-la-nan-nhan-cua-bao-luc-tren-mang-185230516162921705.htm>, truy cập ngày 30/8/2023.

trong sinh viên hầu như diễn ra mỗi ngày. Khi giải trí trên mạng xã hội như Facebook, Messenger, Tiktok, Instagram, ... chúng ta sẽ thường xuyên bắt gặp các bài viết có nội dung kèm theo hình ảnh công khai nạn nhân với mục đích chỉ trích, xúc phạm hoặc đưa ra những thông tin cá nhân nhạy cảm về một cá nhân mà không có căn cứ chính xác (thường gọi là các bài viết “bóc phốt”) cùng với lượt bình luận và chia sẻ rất cao. Nội dung bài viết chủ yếu là về một hành động sai trái của nạn nhân là sinh viên của một trường đại học nào đó, đôi khi nạn nhân không làm gì sai nhưng bị ghét nên thủ phạm mới thêm dệt nên một câu chuyện không có thật để bôi nhọ, làm xấu đi hình ảnh của nạn nhân để thỏa mãn ý xấu của mình, hả hê khi nạn nhân bị chỉ trích, lên án. Hiện nay, bắt nạt trực tuyến thường được thực hiện bằng những hành vi như viết những bình luận ác ý hoặc sử dụng từ ngữ xúc phạm trong tin nhắn để công kích cá nhân; tự ý chỉnh sửa, cắt ghép ảnh của nạn nhân để bôi nhọ họ; tung tin đồn trên mạng internet hay sử dụng tài khoản mạo danh để chế giễu, quấy rối người khác, ... Hiện nay, hành vi thường bắt nạt trực tuyến mà sinh viên thường gặp nhất là kẻ bắt nạt sẽ tạo một tài khoản ẩn danh trên mạng xã hội hoặc lập một hội nhóm tẩy chay (group anti) nạn nhân. Số lượng thành viên của các hội nhóm này liên tục tăng rất nhanh, những con số này không thể hiện rằng cá nhân đó bị nhiều người ghét mà nhiều người tham gia chỉ vì tính hiếu kỳ, muốn vào để “hóng” xem trong nhóm này có gì, hùa theo và lan truyền tin xấu đó ra bên ngoài làm dậy sóng dư luận. Chẳng hạn như một sinh viên tham gia cuộc thi hoa hậu và đạt giải, khi trở thành hoa hậu, lập tức các hình ảnh ngày xưa, hành động, cử chỉ, phát ngôn của họ sẽ được đào bới lại bị bàn tán và soi mói, thậm chí, kết quả học tập hay các hoạt động riêng tư khác cũng sẽ được công khai dù không có sự đồng ý của nạn nhân. Gần đây, các bạn trẻ thường lựa chọn trở thành người sáng tạo nội dung trên các trang mạng xã hội như Tiktok, Youtube. Với hình thức này, các bạn sẽ đăng video lên nền tảng, video càng thu hút thì càng có nhiều lượt xem và có nhiều cơ hội kiếm thêm thu nhập. Do đó, không ít các bạn sinh viên đăng video với nội dung là “phốt” của người khác để “câu like”, lợi dụng các lượt “share” (chia sẻ) để nổi tiếng. Như vậy, các bài viết có nội dung bắt nạt cứ thế lan truyền, không bao giờ được gỡ bỏ hoàn toàn khỏi mạng xã hội.

Ngoài câu chuyện lập “group anti” để bôi nhọ, chỉ trích, các trang confession (tạm dịch là “lời thú tội” mang ý nghĩa bày tỏ lời muốn nói) trên mạng xã hội của các trường Đại học cũng là vấn đề đáng bàn đến. Confession được xem là cách thể hiện những điều mà người viết muốn nói nhưng không muốn ai biết là mình nói, tức là bạn sẽ gửi những câu chuyện của mình ở trang confession với tư cách ẩn danh. Cụ thể hơn, trang confession của các trường đại học thông thường sẽ mang tên của trường, ví dụ như ULAW Confession (trường ĐH Luật TP.HCM), HCMUTE Confession (trường ĐH Sư phạm kỹ thuật TP.HCM), ... Trang confession có một đội ngũ quản trị viên, người tham gia sẽ gửi tâm thư của mình thông qua trung gian (thường là google form), quản trị viên

sẽ kiểm duyệt trước khi đăng lên trang chính thức. Ban đầu, đa số những câu chuyện được đăng lên các trang confession đều là những câu chuyện mang tính hài hước, giải trí cao; những câu chuyện thâm kín không thể chia sẻ được với ai hay những lời tâm tình khó nói với bạn bè, ... Đồng thời, đây cũng là nơi kết nối sinh viên với nhà trường, bày tỏ những ý kiến mà sinh viên không thể nói trực tiếp với thầy cô và các phòng ban phụ trách chính. Khởi đầu với mục đích chính đáng, tuy nhiên, bên cạnh những giá trị tốt đẹp mà nó mang lại thì cũng còn tồn tại những hiểm họa về văn hóa, càng phổ biến thì các trang confession ngày càng biến tướng, “là một con dao hai lưỡi”, trở thành một “ổ bắt nạt trực tuyến” đối với sinh viên. Khi bất bình với một cá nhân hay một tập thể, sinh viên không lựa chọn phương án gặp mặt trực tiếp để góp ý hay giải quyết vấn đề mà họ lại gửi bài ẩn danh lên trang confession với những lời lẽ rất khó nghe, có ý xúc phạm, làm xấu hình ảnh của nạn nhân. Confession lúc này được sử dụng như một công cụ để nói xấu và bóc phốt, nhiều sinh viên dù không quen biết nạn nhân, không hiểu rõ vấn đề nhưng vẫn tham gia vào để gây hoang mang trong dư luận. Hơn nữa, không chỉ là sinh viên trong trường biết đến sự việc mà sinh viên từ các trường khác cũng có thể tiếp cận và bàn tán về nó. Do đó, nạn nhân không chỉ bị chỉ trích trong trường, mà tin tức còn lan truyền ra ngoài với tốc độ rất nhanh, tác động tiêu cực đến tinh thần, tâm lý của sinh viên, đồng thời tác động xấu đến hình ảnh của nhà trường. Vì có tính chất ẩn danh, thông tin cứ thế được tung ra mà chúng ta không biết người là ai, nội dung của các confession hầu như được diễn đạt bằng những từ ngữ rất khiếm nhã. Những hành động thường ngày như ăn, uống, sinh hoạt tại trường, thái độ học tập trong lớp, cách ăn mặc, phát ngôn, ... bất cứ hành động nào chỉ cần không vừa mắt người khác thì sẽ bị “lên án” ngay trên confession, dù những vấn đề này chúng ta có thể góp ý với nhau một cách kín đáo và tế nhị. Đáng lo ngại hơn, không chỉ sinh viên là nạn nhân mà cả thầy cô cũng trở thành đối tượng của hành vi bắt nạt trực tuyến. Khi gặp vấn đề với giảng viên, các bạn sinh viên không chọn cách nói chuyện trực tiếp với thầy cô hay gửi ý kiến phản hồi đến các phòng ban của nhà trường mà lại mang câu chuyện ấy lên các trang confession, làm ảnh hưởng xấu đến hình ảnh người thầy trong nền giáo dục. Người kiểm duyệt nội dung của các confession (admin) cũng đóng vai trò rất quan trọng. Các admin cần chọn lọc những bài đăng nào có giá trị để công khai, việc duyệt đăng các confession có nội dung bắt nạt thì chẳng khác nào tiếp tay cho hành vi sai trái đó, trực tiếp làm ảnh hưởng đến cuộc đời của một con người. Vừa qua, một quản trị viên của trang fanpage UEH Confession đã chỉnh sửa bài viết do người không rõ lai lịch gửi đến. Nội dung bài viết bịa đặt về việc tại Trường Quân sự Quân khu 7 xảy ra vụ hiếp dâm nữ sinh viên học giáo dục quốc phòng, an ninh vào lúc 22 giờ 30 đêm 10-1-2023 tại Đại đội 6, Tiểu đoàn 3, Trung tâm giáo dục Quốc phòng và An ninh (Trường Quân sự Quân khu 7) và nhiều

vụ việc hiếp dâm trước đây.³² Ngay khi bài viết vừa được đăng trên mạng xã hội, dư luận rúng động ngay lập tức, rất nhiều bình luận tiêu cực trực tiếp tác động đến nhà nước, ảnh hưởng xấu đến hình ảnh của quân đội. Ngoài ra, một số bộ phận là phản động cũng lợi dụng tình hình rối ren để tung tin giả về nhà nước Việt Nam, tác động đến tâm lý, gây hoang mang, chia rẽ nhân dân, đặc biệt là thế hệ trẻ.

Có thể thấy, sinh viên hiện nay đang quá lệ thuộc vào các trang mạng xã hội, dần dần đánh mất đi khả năng hòa nhập với cuộc sống, gắn kết, hòa đồng với bạn bè và xã hội. Sinh viên là đối tượng nhạy bén về công nghệ, có tần suất sử dụng các thiết bị điện tử cao, thời gian hoạt động trên mạng xã hội rất nhiều, dẫn đến việc họ “chìm đắm” trong thế giới ảo và quên đi thế giới thực. Vì thế, sinh viên có thể trở thành nạn nhân của bắt nạt trực tuyến, thậm chí trở thành chủ thể vi phạm mà không hề hay biết. Hệ quả của bắt nạt trực tuyến là vô cùng nghiêm trọng. Những nạn nhân của bắt nạt trực tuyến thường không thể và không biết làm cách nào để đối mặt dẫn đến trầm cảm, phải tự làm đau bản thân để giải tỏa sức ép để rồi dẫn đến một vòng luẩn quẩn giữa sự sống và cái chết mà chính họ cũng không biết phải lựa chọn thế nào. Sinh viên thông thường đều là những người đi học xa nhà, xa quê hương, nhiều bạn trẻ lại không thể hòa nhập được với môi trường mới. Do vậy, khi gặp tình trạng bắt nạt, họ thường không biết chia sẻ với ai, ngại chia sẻ với gia đình và người thân vì xấu hổ và tự ti. Theo nhóm tác giả, sự ảm danh của kẻ bắt nạt là nguyên nhân quan trọng của hành vi bắt nạt trực tuyến. Việc gia tăng sử dụng Internet, sự xuất hiện ngày càng nhiều các nền tảng mạng xã hội và lượng người dùng không giới hạn đã tạo điều kiện cho những kẻ ảm danh thực hành vi bắt nạt trực tuyến của mình.³³ Nhiều người nghĩ rằng, chỉ cần sử dụng mạng xã hội với tư cách ảm danh thì chúng ta có thể tự do phát ngôn, tự do nói những điều mình nghĩ mà không cần phải kiêng nể hay sợ mất lòng ai, vì dù gì cũng không có ai phát hiện ra mình. Mạng xã hội là thế giới ảo, là nơi mà bất kỳ ai cũng có thể tạo hàng trăm tài khoản giả mạo để tấn công một cá nhân mà không sợ bị phát hiện. Con người đã lạm dụng quyền tự do ngôn luận và tự do thể hiện quyền ngôn luận của mình để gây tổn thương đến người khác. Số lượng các tài khoản ảo ngày càng nhiều kéo theo vấn đề bắt nạt trực tuyến trở nên trầm trọng hơn. Không chỉ gây tác động xấu đến nạn nhân, thủ phạm và người tham gia bắt nạt trực tuyến cũng bị ảnh hưởng đến tâm lý, tư tưởng sai lệch, thái độ ngạo mạn, không coi trọng người khác, lâu ngày sẽ hình thành nên lối sống ích kỷ, chỉ quan tâm đến bản thân mình, thiếu sự cảm thông, chia sẻ với con người.

³² Ý Linh (2023), “Đưa tin giả “nữ sinh trường HUFLIT bị xâm hại”, cựu admin UEH Confessions hầu tòa”, <https://nld.com.vn/phap-luat/dua-tin-gia-nu-sinh-truong-huflit-bi-xam-hai-cuu-admin-ueh-confessions-hau-toa-20230726150422162.htm>, truy cập ngày 31/8/2023.

³³ Nguyễn Thị Ngọc Ánh, Nguyễn Thị Thùy Duyên, Nguyễn Lương Thị Thúy Hân (2022), “Phòng ngừa hành vi bắt nạt trực tuyến”, Công trình Nghiên cứu khoa học sinh viên cấp trường, Trường Đại học Luật Thành phố Hồ Chí Minh, tr.45.

Bắt nạt trực tuyến không phải là một vấn đề mới mẻ. Từ khi internet bắt đầu phát triển, vấn đề này cũng trở nên phổ biến hơn. Tuy nhiên, mặc dù nhiều sự can thiệp nhưng thực trạng về hành vi này vẫn chưa giảm đi mà ngày càng tăng mạnh. Sự đau khổ được tạo ra từ những vở bọc vô danh trên mạng, thủ phạm núp mình trong không gian ảo khiến cho nạn nhân rơi vào bế tắc, dù muốn tố cáo thủ phạm thì cũng khó biết chính xác danh tính là ai. Chính vì thế, chúng ta nên đề ra các biện pháp phòng ngừa kịp thời để bảo vệ sinh viên nói riêng và con người trong xã hội nói chung. Công dân hạnh phúc thì đất nước mới hạnh phúc và phát triển. Việc xử lý triệt để các hành vi bắt nạt trực tuyến nói riêng và bạo lực mạng nói chung là điều cần thiết để xây dựng một môi trường mạng văn minh, lành mạnh.

4. Một số giải pháp phòng ngừa hành vi bắt nạt trực tuyến trong sinh viên

Hành vi bắt nạt trực tuyến là một khía cạnh của bạo lực mạng, là một trong những mối đe dọa mà sinh viên gặp phải trong môi trường số. Hành vi bạo lực này xuất hiện đã từ lâu, chúng ta cũng đã đề ra nhiều biện pháp phòng ngừa và xử lý khi có sự việc xảy ra, tuy nhiên hiện tượng bắt nạt trên mạng vẫn ngày càng gia tăng mà chưa có xu hướng suy giảm, số lượng nạn nhân ngày càng nhiều, ảnh hưởng không nhỏ đến tinh thần, tâm lý của sinh viên và cuộc sống của họ sau này. Liệu rằng các biện pháp của chúng ta đề ra chưa đúng hay việc thi hành các biện pháp đó trên thực tế chưa thực sự mang lại hiệu quả. Để góp phần phòng ngừa tình trạng bắt nạt trực tuyến trong sinh viên, nhóm tác giả đề xuất một số biện pháp như sau:

Một là, xuất phát từ ý thức cá nhân của mỗi người. Theo nhóm tác giả, đây là giải pháp cơ bản và quan trọng nhất. Mỗi chúng ta đều phải tự ý thức được chúng ta nên làm gì cho đúng đắn, hành xử văn minh trong đời sống hằng ngày lẫn trên mạng xã hội. Với tư cách là người sử dụng mạng, khi gặp các bài viết về có nội dung bắt nạt, chúng ta phải có sự đồng cảm, chia sẻ với nạn nhân, không được hùa theo, không cổ vũ, tiếp tay cho thủ phạm thực hiện các hành vi xấu, tiến hành báo cáo bài viết cho cơ quan quản lý trang web/mạng xã hội, yêu cầu chấm dứt nhanh chóng hành vi bắt nạt. Chúng ta không nên vô tâm lướt qua bài viết bởi đôi khi vì sự vô tâm của mình, một cuộc đời con người sẽ bị phá hoại. Tích cực lên án việc làm sai trái của nạn nhân không hẳn là làm cho họ thay đổi mà khi bị tấn công quá dữ dội, nạn nhân sẽ bế tắc, từ đó dẫn đến nhiều hậu quả đáng tiếc khác. Khi chính bản thân gặp phải tình trạng bắt nạt, hãy cố gắng mở lòng mình, chia sẻ với một người khác để cùng tìm ra cách giải quyết đúng đắn và kịp thời, đừng im lặng một mình để rồi suy nghĩ không được thấu đáo, vấn đề sẽ không được giải quyết một cách hiệu quả. Ngoài ra, khi sử dụng mạng xã hội, chúng ta nên tìm hiểu kỹ càng về các loại tấn công mạng và cách phòng ngừa, bảo mật thông tin cá nhân, cảnh giác và cẩn trọng khi sử dụng mạng. Chúng ta nên tự bảo vệ chính mình trước khi bảo vệ người khác an toàn trên không gian số.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Hai là, xuất phát từ gia đình. Đa phần sinh viên đại học đều là những bạn trẻ đến từ các tỉnh thành khác nhau trên cả nước, hoàn cảnh xa nhà khiến các bạn sinh viên trở nên sống khép kín với gia đình, ít chia sẻ, bộc lộ tâm tư, tình cảm của mình. Chính vì thế, bố mẹ và những người thân trong gia đình cần phải quan tâm đến con cái mình nhiều hơn, thường xuyên gần gũi, tâm sự với con để con có thể chia sẻ với mình những khó khăn đang gặp phải, không nên phản ứng theo kiểu đổ lỗi cho con. Nếu phát hiện con đang bị bắt nạt, bố mẹ hãy đứng về phía con, tìm hiểu xem nguyên nhân vì sao con bị bắt nạt và cùng con tìm ra giải pháp khắc phục vấn đề này. Nỗi đau về mặt cảm xúc khi bị bắt nạt có thể tác động lâu dài, ảnh hưởng đến cuộc sống của các bạn sinh viên sau này. Sự quan tâm, chăm sóc của gia đình sẽ khiến cho các bạn sinh viên yên tâm hơn, tự tin hơn trong cuộc sống, nhất là khi trở thành nạn nhân của một vụ bắt nạt trên mạng.

Ba là, xuất phát từ nhà trường và các cơ sở giáo dục. Nhà trường đóng vai trò quan trọng trong việc bảo vệ sinh viên khỏi bắt nạt trực tuyến. Chính vì thế, nhà trường cần ban hành bộ quy tắc ứng xử trên mạng xã hội trong phạm vi trường đại học, tích cực trong công tác kiểm soát hoạt động phát ngôn của sinh viên do trường quản lý. Ngoài ra, các trang mạng giải trí (chẳng hạn như confession hay các group của sinh viên trong trường) nên do nhà trường trực tiếp quản lý hoặc có thể để sinh viên tự do nhưng phải tuân theo quy tắc của trường đề ra. Bên cạnh đó, nhà trường cần tạo ra một môi trường giao tiếp tích cực giữa sinh viên, giáo viên và cán bộ nhà trường. Giảng viên phải là người luôn lắng nghe, gần gũi với sinh viên, đồng hành cùng sinh viên giải quyết các vấn đề chứ không nên vô tâm bỏ qua những khó khăn mà sinh viên đang gặp phải. Ngoài ra, các trường đại học nên phát triển và triển khai chương trình giáo dục an toàn trực tuyến, thường xuyên tổ chức các buổi nói chuyện, ngoại khóa, sinh hoạt chuyên đề nhằm cung cấp thông tin về các dạng bạo lực trực tuyến, giúp sinh viên nhận biết và phản ứng đúng cách khi gặp phải tình huống bắt nạt, hiểu rõ về quyền riêng tư, an ninh mạng và kỹ năng phòng ngừa bạo lực trực tuyến. Nhìn chung, đa phần các vụ việc bắt nạt trực tuyến đều khởi nguồn từ trong môi trường học đường, do đó, nhà trường cần phải trở thành một nơi an toàn, nơi mà sinh viên có thể yên tâm chia sẻ, gửi gắm tương lai của mình.

Cuối cùng, xuất phát từ phía Nhà nước. Hiện nay, các quy định pháp luật điều chỉnh hành vi bắt nạt trực tuyến vẫn còn chung chung, chưa có một quy định cụ thể để bảo vệ cá nhân trước các hành vi bắt nạt, chưa bao quát hết các dạng hành vi xảy ra trên thực tiễn, nhất là trong bối cảnh công nghệ số trong thời điểm hiện tại. Chính vì thế, Nhà nước cần tiếp tục hoàn thiện pháp luật về bắt nạt trực tuyến nói riêng và bạo lực mạng nói chung. Các chế tài xử lý hành vi bắt nạt trực tuyến phải đủ tính nghiêm khắc, răn đe, ghi nhận cả trách nhiệm hình sự và trách nhiệm hành chính tùy theo hậu quả, quy định phải đủ sức ngăn chặn hiệu quả hành vi bắt nạt trực tuyến trên thực tế. Bên

cạnh đó, cơ quan nhà nước có thẩm quyền cần phải nâng cao công tác quản lý, tích cực đồng hành cùng các cơ sở giáo dục và sinh viên trong công tác phòng ngừa bắt nạt trực tuyến, góp phần loại bỏ các mối đe dọa an ninh mạng, tạo ra một môi trường an toàn, lành mạnh và văn minh.

5. Kết luận

Với sự phát triển mạnh mẽ của công nghệ thông tin, bắt nạt trực tuyến đã trở thành một vấn đề đáng lo ngại trong môi trường học đường. Nó có thể gây ra tác hại về mặt tâm lý, ảnh hưởng đến sự tự tin, gây cảm giác bất an, hoảng sợ và lo lắng, gây ra sự cô lập và kém hiệu quả trong học tập của sinh viên. Để loại bỏ hoàn toàn hiện tượng bắt nạt trực tuyến trong sinh viên là một quá trình khó khăn, cần nhiều thời gian và cần có sự chung tay của cả xã hội. Nhận thức rõ thực trạng của hành vi bắt nạt trực tuyến trong thời điểm hiện nay là cơ sở để chúng ta kịp thời đưa ra các biện pháp phòng ngừa, xây dựng một không gian mạng an toàn với lối ứng xử lịch sự, góp phần tạo ra một xã hội văn minh, an toàn, một xã hội mà ở đó mọi người ai cũng tự tin thể hiện mình, cống hiến hết sức mình cho đất nước.

Tài liệu tham khảo

- Ban tuyên giáo Tỉnh ủy Hà Giang (2022), “Hỏi – đáp về chuyển đổi số (Tập 1)”, https://s3.khaothi.online/xcbt-files/P3/BTGHAGIANG/documents/HOI-DAP-CHUYEN-DOI-SO-TP-10X14.5_l2.pdf, truy cập ngày 29/8/2023.
- CambridgeDictionary, <https://dictionary.cambridge.org/vi/dictionary/english/cyberbullying>, truy cập ngày 29/8/2023.
- Hà Ánh (2023), “69% sinh viên từng là nạn nhân của bạo lực trên mạng”, <https://thanhnien.vn/69-sinh-vien-tung-la-nan-nhan-cua-bao-luc-tren-mang-185230516162921705.htm>, truy cập ngày 30/8/2023.
- Hoàng Phê (2003), “Từ điển Tiếng Việt”, <https://archive.org/details/tu-dien-tieng-viet-vien-ngon-ngu-hoc/page/46/mode/2up>, truy cập ngày 29/8/2023.
- National Centre Against Bullying (n.d), “Definition of bullying”, <https://www.ncab.org.au/bullying-advice/bullying-for-parents/definition-of-bullying/>, truy cập ngày 29/8/2023.
- Nguyễn Thị Ngọc Ánh, Nguyễn Thị Thùy Duyên, Nguyễn Lương Thị Thúy Hân (2022), “Phòng ngừa hành vi bắt nạt trực tuyến”, Công trình Nghiên cứu khoa học sinh viên cấp trường, Trường Đại học Luật Thành phố Hồ Chí Minh, tr.45.
- United Nations International Children's Emergency Fund (Quỹ Nhi đồng Liên hợp quốc)

Unicef (n.d), “Cyberbullying: What is it and how to stop it”, <https://www.unicef.org/end-violence/how-to-stop-cyberbullying>, truy cập ngày 29/8/2023.

Ý Linh (2023), “Đưa tin giả “nữ sinh trường HUFLIT bị xâm hại”, cựu admin UEH Confessions hầu tòa”, <https://nld.com.vn/phap-luat/dua-tin-gia-nu-sinh-truong-huflit-bi-xam-hai-cuu-admin-ueh-confessions-hau-toa-20230726150422162.htm>, truy cập ngày 31/8/2023.

CÁC GIẢI PHÁP GIẢM THIỂU TỆ NẠN XÃ HỘI TRONG SINH VIÊN

Phạm Thị Khánh Ly

Trường Đại học Luật Hà Nội

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Giải pháp. tệ nạn xã hội, giảm thiểu tệ nạn xã hội, sinh viên.	Tệ nạn xã hội là một trong những căn bệnh xã hội nguy hiểm, nó ảnh hưởng xấu đến sự phát triển nhân cách của nhân, sự ổn định của xã hội và bước tiến của nhân loại. Hiện nay, thực trạng về tệ nạn xã hội trong sinh viên đang diễn biến hết sức phức tạp với tỉ lệ ngày một tăng cao. Do vậy, bài viết tập trung nghiên cứu các giải pháp giảm thiểu tệ nạn xã hội cho sinh viên hiện nay, làm cơ sở đề xuất biện pháp quản lý hoạt động giáo dục phòng ngừa tệ nạn xã hội cho sinh viên, góp phần nâng cao chất lượng đào tạo nguồn nhân lực ở các đơn vị đào tạo sinh viên hiện nay.
<i>Keywords:</i> Solution. social evils, reduce social evils, student.	ABSTRACT Social evils are one of the dangerous social diseases, it negatively affects the personality development of people, the stability of society and the advancement of humanity. Currently, the situation of social evils among students is becoming extremely complicated with an increasing rate. Therefore, the article focuses on researching solutions to reduce social evils for students today, as a basis for proposing measures to manage educational activities to prevent social evils for students, contributing to improving education. quality of human resource training in current student training units.

I. ĐẶT VẤN ĐỀ

Tệ nạn xã hội, mà những loại hình cụ thể của nó như nghiện hút ma túy, mại dâm, cờ bạc, say rượu, các loại bệnh xã hội, quấy phá do quá khích, đua đòi ăn chơi thái quá..., về bản chất, là những hành vi sai lệch tiêu cực, thể hiện thái độ lệch lạc, coi thường các giá trị truyền thống đạo lý, xem nhẹ các nguyên tắc, quy định của pháp luật hiện hành. Nó đã và đang là những vấn nạn gây nhức ' nhối, bức xúc trong dư luận xã hội, sự lo lắng trong các gia đình, nhà trường và là mối bận tâm của các cơ quan chức năng nhà nước.

Hậu quả tiêu cực mà tệ nạn xã hội có thể gây ra là rất khó lường. Một mặt, người dính líu vào các tệ nạn xã hội có thể tự hủy hoại sức khỏe, đánh mất danh dự, nhân cách

của chính mình; buông thả mình theo lối sống phóng túng, truy lạc và thực dụng. Mặt khác, khoảng cách giữa tệ nạn xã hội và hành vi phạm pháp, phạm tội chỉ gần nhau trong gang tấc. Để thoả mãn các nhu cầu ảo, bất chính, lợi ích phi pháp của bản thân, người ta có thể dính líu vào các hành vi phạm tội như trộm cắp, lừa đảo, cướp giật tài sản...

Giới trẻ nói chung và sinh viên nói riêng, thuộc lớp thanh niên có độ tuổi từ 18 đến 23 - 25, đang trong giai đoạn chuyển từ sự chín muồi về thể chất sang sự trưởng thành về phương diện tâm lý - xã hội. Đây là giai đoạn phát triển mạnh nhất về tình cảm, đạo đức và thẩm mỹ; hình thành, ổn định về tính cách và có vai trò “người lớn” thực sự (có các quyền công dân, chịu trách nhiệm về hành vi của mình, độc lập trong suy nghĩ, phán đoán...). Đây cũng là thời kỳ ở mỗi sinh viên có nhiều biến động mạnh mẽ về thái độ, động cơ và thang giá trị xã hội, xác định con đường sống và lập nghiệp trong tương lai.

Tuy nhiên, thời kỳ sinh viên còn được gọi là “*thời kỳ bão táp và căng thẳng*”. Trí thức tích lũy chưa đầy đủ, tự ý thức còn thấp, thiếu kinh nghiệm đối nhân xử thế, dễ “nổi khùng” khi bị phê bình, ham muốn khám phá những điều “mới lạ” một cách thái quá cùng với cuộc sống xa gia đình, thiếu sự quản lý của cha mẹ... thường là nguyên nhân khiến sinh viên dễ dính líu vào các thói hư, tật xấu, tham gia vào các loại tệ nạn xã hội, thậm chí là phạm tội.

Chính vì vậy, giáo dục, định hướng để sinh viên nhận thức đầy đủ về thực trạng, nguyên nhân và những tác hại của tệ nạn xã hội trong sinh viên, xây dựng các giải pháp có tính khả thi và hiệu quả nhằm phòng chống tệ nạn xã hội trong sinh viên là vấn đề có ý nghĩa thực tiễn rất quan trọng và mang tính cấp thiết. Đó cũng là lý do tôi chọn vấn đề “các giải pháp giảm thiểu tệ nạn xã hội trong sinh viên” để đến với hội thảo khoa học lần này.

Mục đích của bài viết là nghiên cứu lý luận và thực tiễn nhằm làm sáng tỏ thực trạng, các nguyên nhân làm phát sinh cũng như những hậu quả tiêu cực mà các loại hình tệ nạn xã hội có thể gây ra cho sinh viên hiện nay; trên cơ sở đó, bài viết đề xuất và luận giải một số giải pháp khả thi nhằm ngăn chặn, phòng chống các tệ nạn xã hội trong sinh viên hiện nay.

Để đạt được mục đích nghiên cứu đặt ra trên đây, đề tài tập trung giải quyết các nhiệm vụ sau:

- Nghiên cứu lý luận một số vấn đề đề chung về tệ nạn xã hội cũng như tình hình tệ nạn xã hội trong sinh viên ở nước ta hiện nay
- Thu thập thông tin phục vụ việc đánh giá thực trạng các loại tệ nạn xã hội xảy ra trong sinh viên, ý thức phòng chống tệ nạn xã hội trong sinh viên
- Đề xuất và luận chứng tính khả thi của một số giải pháp nhằm phòng chống, giảm thiểu có hiệu quả các loại tệ nạn xã hội và nâng cao ý thức phòng chống tệ nạn xã hội của sinh viên trong giai đoạn hiện nay.

Đây là một vấn đề vừa mang tính lý luận, vừa mang tính thực tiễn; vì vậy, phương pháp nghiên cứu của bài viết là sử dụng các phương pháp phân tích và tổng hợp, khái quát hóa, trừu tượng hóa và thu thập các dữ liệu... để nghiên cứu các vấn đề lý luận.

II. MỘT SỐ VẤN ĐỀ CHUNG VỀ TỆ NẠN XÃ HỘI

1. Khái niệm

Xét theo nghĩa gốc của thuật ngữ, thuật ngữ “tệ nạn” được cấu tạo bởi hai từ: “tệ” và “nạn”; trong đó, “tệ” có nghĩa là sai trái, xấu xa, trái với luân thường đạo lý, truyền thống của cộng đồng, đáng bị coi thường, cần phải bị lên án; “nạn” có nghĩa là những lẽ tạt, thói quen có tác động xấu, ảnh hưởng tiêu cực tới lối sống lành mạnh, tiến bộ trong các cộng đồng người, trong xã hội nói chung. Tính từ “xã hội” đứng sau thuật ngữ “tệ nạn” nói lên rằng, những thói hư, tật xấu, hành vi tiêu cực... thường phổ biến, lan truyền trong các cá nhân, các nhóm xã hội nhất định, trở thành những vấn đề xã hội nghiêm trọng: hủy hoại phẩm chất, nhân cách, sức khỏe cá nhân; gây tổn thất về kinh tế, tiền bạc của các gia đình, nhà nước và xã hội; gây hoang mang, lo lắng và bức xúc trong dư luận xã hội; ảnh hưởng tiêu cực tới trật tự, kỷ cương, an toàn xã hội. Như vậy, *Tệ nạn xã hội là hiện tượng xã hội có tính tiêu cực, biểu hiện thông qua các loại hành vi sai lệch chuẩn mực xã hội, vi phạm đạo đức, pháp luật hiện hành, phá vỡ thuần phong mỹ tục, lối sống lành mạnh, tiến bộ trong xã hội, gây ra hoặc có thể gây những tác hại, hậu quả nghiêm trọng cho các cá nhân, gia đình và xã hội.*

2. Các loại tệ nạn xã hội

Hiện nay trong xã hội đã có những tệ nạn xã hội nguy hiểm và đang xuất hiện thêm không ít những biến thể của tệ nạn cũ khiến cho những người không vững vàng dễ dàng sa bẫy.

2.1 Tệ nạn ma túy

Ma túy là một chất gây nghiện cực mạnh đối với con người, khi sử dụng người đó sẽ mất đi thần trí, mất ý thức và bị chất gây nghiện làm cho ảo giác. Người nghiện ma túy sẽ bị chúng điều khiển hành vi, ảnh hưởng đến sức khỏe, và tinh thần của bản thân cũng như người thân. Bởi khi đã nghiện thì phải sử dụng chất đó thường xuyên nếu không cơ thể sẽ tạo nên một cảm giác khó chịu, khiến kẻ nghiện đó vật vờ.

Mà để mua được chất đó cần số tiền cũng khá cao, trong khi người nghiện mất đi khả năng làm việc, cơ thể mệt mỏi nên thường nảy ra ý định xấu xa như trộm cắp, cướp giật để có tiền mua chúng. Có thể thấy tệ nạn ma túy nguy hiểm đến xã hội nhường nào, khi một người nghiện thì những người xung quanh sẽ có nguy cơ bị xâm phạm, trộm cắp.

Người nghiện/lệ thuộc vào ma túy còn bị ma túy gây tác hại lâu dài cho con cái, nòi giống; các chất ma túy ảnh hưởng đến hệ thống hoocmon sinh sản, làm giảm khả

năng sinh hoạt tình dục, ảnh hưởng đến quá trình phân bào hình thành các giao tử, tạo cơ hội cho các gen độc có điều kiện hoạt hoá, dẫn tới suy yếu giống nòi³⁴.

Ngoài ra ma túy chính là nguồn lây nhiễm nhân cho đại dịch HIV, căn bệnh thế kỷ khiến người nhiễm chết dần, chết mòn mà y học chưa có thuốc đặc trị.

2.2 Tệ nạn mại dâm

Mại dâm là một tệ nạn trái ngược với thuần phong mỹ tục của con người Việt. Mại dâm là hoạt động cung cấp dịch vụ tình dục ngoài hôn nhân. Những mua dâm và bán dâm thực hiện hành vi trao đổi vật chất để thỏa mãn nhu cầu. . Nói đến “mại dâm” là người ta thường nghĩ đến người phụ nữ, nhưng trên thực tế có cả nam giới hành nghề này. Con số trên thực tế cho thấy, có 95% người làm nghề mại dâm là phụ nữ và 5% người làm nghề này là nam giới. Điều đó cho thấy, phụ nữ chiếm phần lớn hơn trong nghề này (bán dâm)³⁵.

Tệ nạn này chính là nguồn cơn mất đi hạnh phúc gia đình, cùng với đó là con đường lây truyền HIV nhanh chóng. Do những người bán dâm và mua dâm thực hiện quan hệ với nhiều người chưa an toàn khiến cho dễ lây lan nhanh. Những người có gia đình còn có nguy cơ lây lan cho vợ và con mình trong cuộc sống hằng ngày.

2.3 Tệ nạn cờ bạc

Cờ bạc là cũng là một hoạt động khiến người chơi nghiện chúng, khi chơi cờ bạc có tính chất đồ đen thì người chơi sẽ có một khoản tiền lớn nếu thắng mà không phải làm gì. Điều này đã đánh vào tâm lý ham chơi lười làm của nhiều người. Khi đã đổ tiền vào cờ bạc, nếu bị thua sẽ có xu hướng mong muốn gỡ lại nhưng không biết rằng sẽ càng lún sâu hơn vào vũng bùn ấy. Từ đó thì sẽ bán hết tài sản, vay mượn để chơi.

Tệ nạn cờ bạc hiện nay được biến thể với nhiều hình thức nhất như bài bạc, đá gà, xóc đĩa, tài xỉu, đặt cược bóng, cá cược,...

2.4 Tệ nạn mê tín dị đoan

Mê tín dị đoan là tệ nạn xuất hiện trong chính văn hóa tâm tinh của con người, tin tưởng vào những điều mơ hồ, siêu nhiên không có thực khiến cho những người tin vào điều đó dễ bị lừa gạt mất tiền bạc, sức khỏe sa sút.

Bởi nhiều người không tin vào khoa học chữa trị mà chỉ tin và chữa bệnh bởi thầy bà, cùng với đó là hoạt động xem bói đoán tương lai. Lợi dụng tâm lý đó thì những kẻ hành nghề sai trái đã lợi dụng lòng tin để chiếm đoạt tài sản nhanh chóng.

2.5 Tệ nạn rượu bia

³⁴ <http://www.lamdong.gov.vn/vi-VN/a/phongchongmatuy/tachai/Pages/Tac-hai-ma-tuy.aspx>, truy cập ngày 13/09/2023

³⁵ <http://www.ict-dongthap.gov.vn/Detail.aspx?Channel=11&RecID=683>, , truy cập ngày 13/09/2023

Rượu bia là chất gây hại cơ thể con người với vô vàn căn bệnh như ung thư gan, xơ gan, viêm gan, máu loãng, thận yếu,...

Nếu các tác động ức chế của rượu cứ lặp đi lặp lại nhiều lần (uống liên tục, thường xuyên), sẽ có sự thay đổi về chuyển hóa cơ bản (basal metabolism) của các tế bào não. Các tế bào não sau đó sẽ lệ thuộc vào rượu, nó chỉ hoạt động khi có rượu thấm vào não và hoạt động bất thường theo tác dụng của rượu. Đó chính là cơ chế của chứng nghiện rượu³⁶. Rượu bia có thể khiến người sử dụng chúng bị mất đi khả năng kiểm soát và tỉnh táo để lái xe nên thường gây ra những vụ tai nạn giao thông nghiêm trọng, gia đình bị bạo hành bởi người uống rượu bia, hoặc các vụ hiếp dâm diễn ra do không kiểm soát sự thú tính của bản thân.

3. Tác hại của tệ nạn xã hội

Tệ nạn xã hội có tác hại vô cùng lớn đến các nhóm chủ thể trong xã hội như:

3.1 Tác hại đối với chính bản thân người tham gia các tệ nạn xã hội

Các tệ nạn xã hội có thể gây những tổn thương nghiêm trọng đối với sức khỏe của chính bản thân người tham gia (gây các bệnh về hệ hô hấp, hệ tim mạch, hệ thần kinh đối với người nghiện ma túy...); làm tha hóa về nhân cách, rối loạn về hành vi, rơi vào lối sống buông thả, dễ vi phạm pháp luật và phạm tội.

3.2 Tác hại đối với gia đình

Đối với các gia đình có người thân tham gia các tệ nạn xã hội sẽ có thể bị khủng hoảng về mặt tài chính cũng như tinh thần. Ví dụ như: tệ nạn về ma túy, cờ bạc khiến cho các gia đình bị mâu thuẫn dẫn đến đổ vỡ nhất là những cặp vợ chồng trẻ hay là bạo lực gia đình do áp lực kinh tế vì nợ nần cờ bạc hoặc vì không có tiền sử dụng ma túy.

3.3 Tác hại đối với xã hội

- Có tính lây lan nhanh trong xã hội: tệ nạn xã hội là những hiện tượng có tính chất cộng đồng nên thường dễ nhanh chóng lan tỏa trong một khoảng thời gian ngắn.

- Tồn tại và phát triển dưới nhiều hình thức như mại dâm, ma túy, cờ bạc... Đối tượng tham gia rất đa dạng và phức tạp về thành phần.

- Các đối tượng hoạt động có nhiều phương thức, thủ đoạn tinh vi để đối phó với lực lượng chức năng và che mắt quần chúng nhân dân thường cấu kết với nhau thành đường dây, ổ nhóm.

- Tệ nạn xã hội thường có quan hệ chặt chẽ với tội phạm hình sự như các tội phạm xâm phạm tính mạng, sức khỏe, nhân phẩm, danh dự của con người, các tội phạm về ma túy, các tội xâm phạm an toàn công cộng, trật tự công cộng. Đó là biểu hiện của các hiện tượng tiêu cực xã hội và có sự chuyển hóa lẫn nhau.

³⁶ TS. DS. Nguyễn Hữu Đức (Trường Đại học Y-Dược Thành phố Hồ Chí Minh), Tệ nạn nghiện rượu: vấn đề y học và xã hội, Bài viết đăng tại: http://www.ykhoanet.com/xahoi/ytecongcong/30_133.htm.

- Địa bàn tập trung hoạt động thường là những nơi tập trung đông người, các khu công nghiệp, du lịch, nơi người dân có trình độ dân trí thấp, có xu hướng tập trung thành băng đảng, ổ nhóm.

III. TÌNH HÌNH TỆ NẠN XÃ HỘI TRONG SINH VIÊN Ở NƯỚC TA HIỆN NAY

Cùng với tình hình tệ nạn xã hội nói chung, tình hình tệ nạn xã hội trong đối tượng học sinh, sinh viên ở nước ta hiện nay cũng đang diễn biến theo chiều hướng hết sức phức tạp. Các nghiên cứu, thống kê cho thấy, trong sinh viên có sự xuất hiện và tồn tại hầu như đủ các loại tệ nạn xã hội, từ ma túy, mại dâm, cờ bạc cho tới say rượu, nghiện chơi game online, bạo lực học đường... Tệ nạn xã hội ở một bộ phận sinh viên được ví như “luồng gió đen” đang len lỏi khắp các trường đại học. Đó cũng là nguyên nhân dẫn sinh viên tới các hành vi phạm tội. Theo thống kê của cơ quan công an, mỗi năm ở các trường đại học ít nhất có hàng chục vụ sinh viên phạm pháp hình sự.

Trước hết, phải kể tới tình trạng phạm tội buôn bán ma túy và nghiện ma túy trong sinh viên. Những năm trước đây, đối tượng buôn bán ma túy thường mua chuộc, dụ dỗ những người nông dân ít hiểu biết pháp luật để vận chuyển ma túy thuê cho chúng, song gần đây, mục tiêu này đã chuyển sang giới sinh viên, nhất là số sinh viên ở các tỉnh được đánh giá là trọng điểm về ma túy. Chỉ vì thiếu hiểu biết pháp luật, thiếu kỹ năng sống, không tu dưỡng bản thân và bị cuốn theo lối sống xa hoa nơi đô thị, nhiều học sinh, sinh viên đã, đang bị các đối tượng buôn “cái chết trắng” làm mờ mắt, lôi kéo vào con đường phạm tội.

Theo số liệu thống kê từ Cục phòng, chống tệ nạn xã hội của Bộ Lao động - Thương binh và xã hội, tính đến tháng 12/2020 nước ta có 235.000 người nghiện ma túy có hồ sơ quản lý của cả nước, trong đó dưới 16 tuổi chiếm 0,1%, từ 16-30 tuổi chiếm 48%, nếu tính đến độ tuổi 35 thì tỷ lệ này lên tới 76%. Đáng báo động, có khoảng 60% người sử dụng ma túy lần đầu tiên có độ tuổi từ 15 – 25 tuổi³⁷. Trước thực tế có nhiều chủng loại ma túy giá thành rẻ, dễ sử dụng, nhiều trẻ em từ 13 – 14 tuổi đã sử dụng ma túy. Thậm chí, có nhiều trường hợp chỉ 13 – 14 tuổi đã thường xuyên rối loạn tâm thần, hoang tưởng, rối loạn nhịp tim... như người nghiện ma túy lâu năm. Đau lòng hơn, có những sinh viên vì tiêm chích ma túy đã bị nhiễm HIV/AIDS hoặc chết vì sốc thuốc.

Cờ bạc (lô, đề, cá độ bóng đá...) không phải là hiện tượng mới lạ gì trong giới sinh viên. Có những sinh viên chơi lô, đề hết cả tiền triệu, cả xe máy, máy tính xách tay đắt tiền; thậm chí lấy cả sổ đỏ ngôi nhà gia đình đang sinh sống đem đi “cắm” để thỏa mãn “con khát đồ đen”. Vào mùa bóng đá, dưới cái vỏ bọc “cổ động viên nhiệt tình”,

³⁷<https://tienphong.vn/thuc-trang-bao-dong-ve-nhan-thuc-cua-hoc-sinh-sinh-vien-ve-ma-tuy-post1342648.tpo>, truy cập ngày 14/09/2023.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

nhiều sinh viên sẵn sàng “độc túi” để tham gia các trò cá độ bóng đá. Đến các điểm chơi bi a, bi lắc có thể dễ dàng bắt gặp các nhóm sinh viên các trường đại học đang “say mê” với cuộc chơi vì mỗi ván chơi ít nhất cũng phải có 50.000 đồng.

Không đam mê cờ bạc, nhưng một số sinh viên các trường đại học lại mê mẩn, sống với thế giới ảo nhiều hơn với thế giới thật. Vì đam mê game online, có những sinh viên đã bỏ ra tiền thật để mua lấy những “vũ khí” ảo nhằm trang bị cho nhân vật của mình thật tinh nhuệ. Số tiền chi ra từ vài trăm nghìn đồng rồi lên đến vài triệu, thậm chí lên tới hàng chục triệu lúc nào cũng chẳng biết. Hậu quả là, kết quả học hành sút kém; nợ nần bắt đầu chồng chất, những sinh viên này bị các chủ nợ săn lùng, bị báo lên Ban giám hiệu nhà trường. Vấn đề xem xét các hình thức kỷ luật, thậm chí là bị lưu ban, đuổi học được đặt ra.

Hiện tượng sinh viên uống rượu và say rượu đã trở thành chuyện thường ngày đối với nhiều người. Bất cứ một dịp nào, từ sinh nhật, ngày lễ tết, ngày cuối tuần, thậm chí là không cần “nhân dịp”, các nam sinh viên cũng tụ tập uống rượu. Ai cũng biết uống rượu nhiều sẽ rất có hại cho lục phủ, ngũ tạng, nhưng tất cả đều phớt lờ và cho rằng “vui là chính, sức khỏe là thứ yếu”. Thậm chí, những khi “cạn tiền”, nhiều sinh viên còn đi mua những loại rượu rẻ tiền chỉ vài nghìn/lít, nghĩa là “rượu thì ít, còn thì nhiều”. Uống những loại này, đầu đau như búa bổ, mắt nở hoa cà hoa cải vô cùng hại người. Biết thế, nhưng tất cả đều bỏ qua, chỉ cần lúc “trăm phần trăm” thấy vui là được.

Theo báo cáo chưa đầy đủ của các địa phương trên cả nước số người mại dâm có hồ sơ quản lý là 14.802 đối tượng trong tổng số ước tính trên 35.000 người bán dâm. Người tham gia mại dâm ngày càng trẻ hóa: 16 - 18 tuổi chiếm 16,3%, từ 18- 25 tuổi: 45%, từ 25- 35 tuổi: 32%... [Cục Phòng chống tệ nạn xã hội, Bộ Lao động Thương binh Xã hội, 2015]

Không hẳn là mại dâm, song tình trạng “yêu liều” cũng đang là một vấn đề đáng báo động trong sinh viên hiện nay. Yêu liều ở đây là yêu nhiều, yêu vô tội vạ, bạ đâu yêu đấy. Nếu chỉ là tình yêu trong sáng, thì yêu nhiều cũng không gây hậu quả gì nghiêm trọng. Nhưng một bộ phận sinh viên hiện nay đang đánh đồng tình yêu với tình dục. Hậu quả là tình trạng mang thai ngoài ý muốn và nạo phá thai là giải pháp bắt buộc đối với họ. Không ít “nam thanh nữ tú” sinh viên đã phải lén lút đến những phòng khám hoa liễu để chữa trị căn bệnh “khó nói”. Khám chữa bệnh không đến nơi đến chốn đã khiến một số sinh viên phải trả giá quá đắt cho những phút giây lầm lỡ khi không còn khả năng sinh con.

Nguy hiểm nhất đối với các nam sinh viên là tình trạng “tình cho không biếu không”. Đó là tình trạng những cô gái có “lý lịch tình dục” không rõ ràng tự nguyện đến sống chung với các nam sinh viên ở nhà trọ. Họ chỉ cần có một chỗ ăn, ở không mất tiền, ngoài ra không có yêu cầu gì khác; đổi lại, các nam sinh viên “muốn gì cũng được”.

Đây thực chất là những cô gái bán dâm đã hết thời, nay tìm cách mời chài, chèo kéo những nam sinh viên vốn tò mò, thích của lạ. Những đối tượng này có nguy cơ bị nhiễm HIV và các bệnh truyền nhiễm khác là rất cao.

IV. CÁC GIẢI PHÁP GIẢM THIỂU TỆ NẠN XÃ HỘI TRONG SINH VIÊN

1. Tạo môi trường văn hóa - xã hội lành mạnh phục vụ các hoạt động học tập, rèn luyện, vui chơi, giải trí cho sinh viên

Trên cơ sở nhận thức sâu sắc vai trò của văn hóa, trong Chiến lược phát triển kinh tế xã hội 2001 - 2010, Đảng ta đã nhấn mạnh: “*Nâng cao tính văn hóa trong mọi hoạt động kinh tế, chính trị, xã hội và sinh hoạt của nhân dân*”³⁸. Văn hóa là nền tảng tinh thần của xã hội. Xây dựng và phát triển nền văn hóa tiên tiến, đậm đà bản sắc dân tộc vừa là mục tiêu, vừa động lực thúc đẩy sự phát triển kinh tế - xã hội. Đối với các thế hệ sinh viên vai trò này lại càng có giá trị to lớn hơn nữa vậy nên việc tạo môi trường văn hóa - xã hội lành mạnh phục vụ các hoạt động học tập, rèn luyện, vui chơi, giải trí cho sinh viên là vô cùng cần thiết.

1.1 Tăng cường công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên

Thứ nhất, nâng cao nhận thức của đội ngũ cán bộ, giảng viên, sinh viên trong trường về vai trò, tầm quan trọng của công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên. Trước hết, cần tăng cường sự lãnh đạo, chỉ đạo của Đảng ủy, Ban Giám hiệu nhà trường đối với công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên. Tiếp theo, vấn đề không kém phần quan trọng là sự chỉ đạo nghiêm túc, kịp thời công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên từ phía Ban Giám hiệu nhà trường. Chi bộ, Ban lãnh đạo các phòng chức năng, khoa chuyên môn, trung tâm trong trường phải coi công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên là nhiệm vụ chính trị thường xuyên, có sự chỉ đạo nghiêm túc, đôn đốc kịp thời nhằm thực hiện có hiệu quả công tác này.

Về phía đội ngũ cán bộ, giảng viên, đảng viên, khi tham gia vào công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên phải coi đây như là một nhiệm vụ chính trị của họ. Công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên phải gắn với hoạt động giáo dục, đào tạo pháp luật; giáo dục, đào tạo pháp luật hỗ trợ cho công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống vì giữa chúng luôn có mối liên hệ mật thiết với nhau. Các nhà giáo cần phải đổi mới giáo dục chính trị, tư tưởng, đạo đức, tránh giảng chính trị, đạo đức suông; chính trị, đạo đức, lối sống phải

³⁸ Đảng Cộng sản Việt Nam, Văn kiện Đại hội đại biểu toàn quốc lần thứ IX, Nxb. Chính trị Quốc gia, Hà Nội, 2001, tr. 208.

gắn với pháp luật, phải gắn với định hướng nghề nghiệp mà sinh viên sẽ lựa chọn sau khi tốt nghiệp ra trường.

Về phía sinh viên, cần nhìn nhận nghiêm túc về vai trò, tầm quan trọng của giáo dục chính trị, tư tưởng, đạo đức, lối sống đối với chính mình, tránh tình trạng học qua loa, đại khái cho xong. Chừng nào việc học tập chính trị, tư tưởng, đạo đức, lối sống trở thành nhu cầu tự thân, là yếu tố thường trực trong ý thức của mỗi sinh viên luật thì công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho họ mới thực sự đi vào chiều sâu và đạt hiệu quả như mong muốn.

Thứ hai, *cần xác định rõ những nội dung giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên, tránh tình trạng giáo dục chung chung, không có trọng tâm, trọng điểm và hiệu quả. Nội dung giáo dục chính trị, tư tưởng, đạo đức, lối sống đòi hỏi phải quán triệt cho sinh viên luật các chủ trương, đường lối của Đảng, chính sách pháp luật của Nhà nước, tiếp tục học tập tấm gương đạo đức Hồ Chí Minh, giới thiệu các phẩm chất đạo đức nghề luật...*

Thứ ba, *khi đã xác định rõ nội dung giáo dục chính trị, tư tưởng, đạo đức, lối sống, cần đổi mới phương pháp, hình thức giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên luật. Phương pháp giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên phải thực sự sinh động, hấp dẫn, cuốn hút sinh viên, hướng tới rèn luyện cho họ kỹ năng sống, giao tiếp, thực hành, áp dụng những hiểu biết về chính trị, tư tưởng, đạo đức, lối sống trong đời sống thường nhật.*

Thứ tư, *tiến hành sơ kết, tổng kết, đánh giá, rút kinh nghiệm về công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên nhằm thường xuyên nâng cao chất lượng, hiệu quả của công tác này. Qua sơ kết, tổng kết, chúng ta sẽ biết được những thành công, kết quả đã đạt được cũng như những hạn chế, bất cập còn tồn tại trong công tác giáo dục chính trị, tư tưởng, đạo đức, lối sống cho sinh viên; những thuận lợi và khó khăn khi triển khai công tác này; chỉ ra nguyên nhân của những thành công và hạn chế; rút ra được những bài học kinh nghiệm cần thiết...*

1.2 Chú trọng xây dựng các thiết chế văn hóa phục vụ các hoạt động rèn luyện, vui chơi, giải trí ngoài giờ học cho sinh viên

Xây dựng các thiết chế văn hóa phục vụ các hoạt động rèn luyện, vui chơi, giải trí ngoài giờ học cho sinh viên có nghĩa là tạo ra, trang bị những phương tiện vật chất phục vụ cho các hoạt động, sinh hoạt văn hóa, văn nghệ, vui chơi, giải trí của sinh viên. Đó có thể là sân vận động (mini), nhà thi đấu thể thao sinh viên, rạp chiếu phim, nhà văn hóa sinh viên... Cùng với các phương tiện vật chất đó còn cần phải có người đứng ra tổ chức các hoạt động văn hóa, thể thao thiết thực, có ý nghĩa nhằm lôi cuốn, thu hút sinh viên tham gia (tổ chức các giải thể thao, liên hoan văn nghệ, các loại hình câu lạc

bộ sinh viên). Những hoạt động văn hóa lành mạnh, thiết thực và bổ ích đồng thời giúp sinh viên tránh xa được cám dỗ của các loại tệ nạn xã hội.

Trong thời buổi “tắc đất tắc vàng” như hiện nay, tình trạng chung của nhiều trường là cơ sở vật chất, ký túc xá, nhà văn hóa, sân chơi... cho sinh viên còn thiếu trầm trọng. Nhu cầu hoạt động tập thể, giao lưu của sinh viên là rất lớn và cần thiết, nhưng các cách thức tổ chức sinh hoạt văn hóa lại ít được quan tâm. Từ việc thiếu chỗ cho sinh viên vui chơi, giải trí, tham gia sinh hoạt văn hóa lành mạnh, sinh viên sẽ tìm đến những điểm chơi game online, bia, đánh bài...

Ở nhiều đơn vị trường đại học, do nhiều nguyên nhân, vấn đề xây dựng các thiết chế văn hóa phục vụ các hoạt động rèn luyện, vui chơi, giải trí ngoài giờ học cho sinh viên cũng chưa thực sự được quan tâm và đang trong tình trạng thiếu trầm trọng. Số chỗ ở trong ký túc xá vốn đã rất ít so với nhu cầu nội trú của sinh viên thì nay đã bị trưng dụng phân nửa làm văn phòng cho các khoa, phòng, trung tâm hay khuôn viên trường lại bị trưng dụng làm chỗ để xe. Những thiết chế văn hóa như rạp chiếu phim, sân vận động mini, nhà văn hóa sinh viên... đều là những thứ xa lạ, “trong mơ cũng không dám nghĩ đến” đối với sinh viên. Tuy nhiên, chúng ta không quên rằng, hoạt động ngoài giờ học của đại bộ phận sinh viên đều nằm ngoài tầm nhìn và sự kiểm soát của nhà trường. Lấy gì đảm bảo rằng, sinh viên những người đang học tập, tiếp thu kiến thức và hiểu biết pháp luật không sa đà vào các loại tệ nạn xã hội ở mức độ khác nhau?

Từ thực trạng trên đây, chúng ta thấy rằng ngay từ bây giờ, lãnh đạo các nhà trường khi xây dựng các công trình trong khuôn viên trường đã phải tính tới vấn đề củng cố, xây dựng các thiết chế văn hóa phục vụ các hoạt động rèn luyện, vui chơi, giải trí ngoài giờ học cho sinh viên. Đồng thời cũng cần đầu tư xây dựng hoặc nâng cấp một tòa nhà có sẵn thành Nhà văn hóa sinh viên của mỗi trường đại học. Nhu cầu về Nhà văn hóa sinh viên hiện nay là hết sức cấp thiết; bởi lẽ, sinh viên luật cần có một nơi cố định để duy trì sự tồn tại và hoạt động của các loại hình câu lạc bộ sinh viên, như câu lạc bộ luật gia trẻ, câu lạc bộ thơ ca, câu lạc bộ nữ công gia chánh... Nhà văn hóa sinh viên cũng là nơi sinh viên tổ chức các hoạt động giao lưu, gặp gỡ; nói chuyện thời sự, sinh hoạt khoa học theo chủ đề; tổ chức các cuộc thi tài năng trong sinh... Giảng đường đại học luật cần cho hoạt động học tập, lĩnh hội tri thức pháp lý của sinh viên luật bao nhiêu thì Nhà văn hóa sinh viên cần thiết cho hoạt động rèn luyện, vui chơi, giải trí của sinh viên luật bấy nhiêu.

1.3. Nâng cao chất lượng, hiệu quả các hoạt động văn hóa - văn nghệ, thể dục thể thao, các cuộc vận động và các hoạt động xã hội khác trong sinh viên

Để nâng cao chất lượng, hiệu quả các hoạt động văn hóa văn nghệ, thể dục thể thao, các cuộc vận động và các hoạt động xã hội khác trong sinh viên, chúng ta cần tập trung làm tốt một số nội dung sau:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Các hoạt động phong trào văn hóa - văn nghệ, thể dục, thể thao cần đi vào chiều sâu, thực chất và hiệu quả hơn bằng nhiều phương thức đa dạng, phong phú, sinh động, tránh phô trương, hình thức rườm rà. Ngoài các dịp liên hoan văn nghệ, thi đấu thể thao nhân các ngày lễ, kỷ niệm quan trọng, cần thường xuyên triển khai các hoạt động văn hóa, văn nghệ, thể dục, thể thao, sinh hoạt khoa học, hái hoa dân chủ, nói chuyện thời sự theo chủ đề... ở quy mô nhỏ, nhẹ nhàng, do Ban chủ nhiệm các loại hình câu lạc bộ sinh viên hoặc các hạt nhân nòng cốt đứng ra tổ chức. Các câu lạc bộ luật gia trẻ, câu lạc bộ thơ có thể tổ chức sinh hoạt định kỳ hàng tháng. Các câu lạc bộ thể thao, tùy theo từng môn như cờ vua, cờ tướng, bóng bàn, cầu lông..., có thể tổ chức luyện tập hàng ngày, hàng tuần; định kỳ hàng quý tổ chức thi đấu giao hữu. Tạo được các diễn đàn, sân chơi thu hút sinh viên tham gia cũng có nghĩa là chúng ta tạo môi trường văn hóa lành mạnh phục vụ các hoạt động rèn luyện, vui chơi, giải trí cho sinh viên, giúp họ tránh xa các tệ nạn xã hội.

- Các phong trào, các cuộc vận động được phát động trong sinh viên cũng cần đi vào thực chất bằng những hình thức thiết thực và cần có các cơ chế để đánh giá tính hiệu quả của chúng. Đã đến lúc chúng ta phải ngồi lại, tiến hành các khảo sát thực tế làm cơ sở để sơ kết, tổng kết các cuộc vận động, rút ra các bài học kinh nghiệm để triển khai các phong trào, các cuộc vận động trong sinh viên được thiết thực và hiệu quả hơn.

- Riêng đối với công tác phòng, chống tệ nạn xã hội trong sinh viên, cần có hoạt động ký cam kết phòng chống ma túy và các tệ nạn xã hội được thực hiện trên hội trường hàng năm, ngoài ra cần thành lập Câu lạc bộ phòng, chống tệ nạn xã hội trong sinh viên.

2. Tăng cường vai trò, trách nhiệm của gia đình và các cơ quan chức năng bên ngoài nhà trường trong việc giáo dục, quản lý sinh viên

2.1. Tăng cường vai trò, trách nhiệm của các gia đình trong việc chăm sóc, giáo dục và quản lý con em

2.1.1 Chuẩn bị tốt hành trang kiến thức tâm lý, hiểu biết xã hội, kinh nghiệm giao tiếp cho con cái trước khi nhập trường, chính thức trở thành sinh viên

- Cha mẹ, người thân cần dành nhiều thời gian để trò chuyện, giáo dục con về truyền thống của gia đình, dòng họ nhằm khơi gợi niềm tự hào và quyết tâm phấn đấu của thế hệ sau; dạy cho con những bài học về luân thường, đạo lý, cách đối nhân, xử thế trong cuộc sống tập thể xa nhà; nhắc nhở con về tác hại, hậu quả của các loại tệ nạn xã hội để con tuyệt đối tránh xa, biết cách chọn bạn tốt để kết giao và tránh xa các đối tượng xấu.

- Thu xếp để các em được gặp gỡ, trò chuyện với những sinh viên là người cùng làng, cùng xã để các em chủ động nắm bắt những thông tin cần thiết về cuộc sống, sinh hoạt ở thành phố, đặc biệt là ở các khu nhà trọ sinh viên.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Cha mẹ cần thống nhất và đề ra cho con một số quy định về chế độ sinh hoạt, giờ giấc học tập, nghỉ ngơi...; về mức chu cấp kinh phí phục vụ ăn uống, sinh hoạt tùy thuộc vào điều kiện, khả năng kinh tế của gia đình. Dù kinh tế gia đình có ở mức giàu có thì vẫn phải đề ra cho con một hạn mức vừa phải phù hợp tương đối với mặt bằng chung trong xã hội, tạo cho con thái độ biết trân trọng đồng tiền và thói quen tiết kiệm trong chi tiêu.

- Đối với những sinh viên có hoàn cảnh gia đình éo le, cha mẹ ly thân, ly hôn... thì chính các bậc làm cha, làm mẹ và người thân càng phải quan tâm đặc biệt hơn tới các em. Đối với số sinh viên này, sự chăm sóc, động viên, giáo dục, định hướng cho các em biết cách vượt qua hoàn cảnh, tránh xa tệ nạn xã hội càng phải được tăng cường nhiều hơn.

2.1.2 Thiết lập các cơ chế đáng tin cậy nhằm kiểm tra, giám sát, quản lý quá trình học tập, rèn luyện của con cái trong những năm học đại học

Thứ nhất, nhờ bạn bè, người thân ở các thành phố nơi con đang học đại học thường xuyên quan tâm, động viên, nhắc nhở việc ăn ở, học hành của con cái. Đây là cơ chế “kiểm tra mềm” nhưng sẽ phát huy hiệu quả cao nếu biết vận dụng một cách linh hoạt.

Thứ hai, thiết lập và giữ mối liên hệ thường xuyên với chủ nhà trọ, cảnh sát khu vực hoặc những người hàng xóm xung quanh nơi con cái đang thuê trọ nhằm nắm bắt kịp thời tình hình sinh hoạt của con cái. Bất cứ phụ huynh sinh viên nào có con cái ở nhà trọ cũng có thể sử dụng cơ chế này nếu thực sự quan tâm đến con cái.

Thứ ba, phụ huynh sinh viên cần giữ vững mối liên hệ với các đơn vị chức năng của trường, nhất là Phòng Công tác sinh viên để nắm bắt tình hình học tập của con cái. Phụ huynh sinh viên cũng có thể xin số điện thoại và giữ mối liên hệ với cô vấn học tập để nắm bắt tình hình học tập của con.

Thứ tư, định kỳ hoặc đột xuất (tốt nhất là đột xuất), các bậc phụ huynh cần phải thu xếp thời gian đến nơi con mình đang sinh sống và học tập để thăm, trực tiếp kiểm tra việc ăn ở, học hành của con.

2.2. Tăng cường vai trò, trách nhiệm của các cơ quan chức năng bên ngoài nhà trường, chủ nhà trọ trong việc giáo dục và quản lý sinh viên ngoại trú

2.2.1 Tăng cường vai trò, trách nhiệm của Chính quyền địa phương, Công an phường sở tại, đặc biệt là cảnh sát khu vực, trong việc giáo dục, quản lý sinh viên luật ngoại trú

Về phía Công an phường sở tại, cần làm tốt các công việc quản lý sau đây đối với số sinh viên ngoại trú trên địa bàn mình phụ trách:

- Trên cơ sở giấy chứng nhận của nhà trường cho phép sinh viên ở ngoại trú, Công an phường tạo những điều kiện tốt nhất để giải quyết thủ tục đăng ký tạm trú cho

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

sinh viên ngoại trú theo đúng Nghị định số 51/CP của Chính phủ về việc đăng ký và quản lý hộ khẩu, Thông tư hướng dẫn của Bộ Nội vụ (nay là Bộ Công an) và các quy định của Quy chế này.

- Lãnh đạo Công an phường sở tại cần giao trách nhiệm cho cảnh sát khu vực trách nhiệm định kỳ tổ chức họp với toàn thể sinh viên ngoại trú trên địa bàn mình phụ trách nhằm quán triệt sinh viên thực hiện nghiêm chỉnh pháp luật của Nhà nước, các quy định của địa phương về giữ gìn, bảo vệ trật tự, kỷ cương, an toàn xã hội trên địa.

- Công an phường sở tại, trên cơ sở nắm bắt, quản lý sinh viên ngoại trú trên địa bàn, có trách nhiệm cấp cho sinh viên giấy nhận xét về việc chấp hành luật pháp của Nhà nước, quy định của chính quyền địa phương, những thành tích đóng góp cho địa phương, hoặc những khuyết điểm vi phạm của sinh viên.

2.2.2 Các cơ quan chức năng cần tăng cường hơn nữa công tác quản lý các tụ điểm vui chơi, giải trí, hiệu cầm đồ, dịch vụ Internet... xung quanh trường đại học, ký túc xá, các khu nhà trọ sinh viên

- Tăng cường các hoạt động tuần tra, kiểm soát tại các khu vực xung quanh các trường đại học, khu ký túc xá, khu nhà trọ sinh viên.

- Tăng cường công tác kiểm tra hành chính đối với các bàn bán vé xổ số, các quán nước xung quanh trường đại học, ký túc xá, khu nhà trọ sinh viên, nhất là vào “giờ cao điểm” từ 16h đến 17h hàng ngày. Đây là khoảng thời gian mà sinh viên các trường đại học ghé vào chơi lô, đề.

- Đối với các quán game, dịch vụ Internet... xung quanh các trường đại học, ký túc xá, các khu nhà trọ sinh viên, các cơ quan chức năng cần yêu cầu các chủ quán ký cam kết thực hiện nghiêm túc các quy định của pháp luật liên quan đến hoạt động kinh doanh loại dịch vụ này, như không kinh doanh, sử dụng các trò chơi có nội dung độc hại, thực hiện đúng quy định về giờ đóng cửa quán.

- Đối với các hiệu cầm đồ xung quanh các ký túc xá, khu nhà trọ, vì lợi nhuận và cạnh tranh với các hiệu cầm đồ khác trong việc thu hút khách hàng là sinh viên nên các chủ hiệu cầm đồ thường nhận cầm đồ bất cứ món hàng nào mà không cần tìm hiểu nguồn gốc, xuất xứ, giấy tờ liên quan đến các món đồ đó.

2.2.3 Nâng cao ý thức trách nhiệm của các chủ nhà trọ trong việc giáo dục, quản lý sinh viên ngoại trú

Cơ chế thực hiện biện pháp này chỉ có thể là sự phối kết hợp chặt chẽ, gắn kết giữa gia đình, người thân của sinh viên và chủ nhà trọ.

Một là, tùy theo số lượng nhà trọ có thể cho thuê, sau khi đã ổn định số lượng sinh viên thuê trọ, các chủ nhà trọ cần tổ chức họp sinh viên để thống nhất và quán triệt việc thực hiện nội quy nhà trọ hoặc cùng sinh viên xây dựng nội quy nhà trọ.

Hai là, theo điều kiện tối đa có thể, các chủ nhà trọ cần duy trì trật tự và bảo đảm an ninh cho khu nhà trọ sinh viên một cách ổn định, lâu dài. Khu nhà trọ cần được thiết kế “kín cổng, cao tường”, có đầy đủ “cửa đóng, then cài” để sinh viên “đi đóng, về mở”.

Ba là, các chủ nhà trọ cần thường xuyên giáo dục, đôn đốc, nhắc nhở sinh viên thuê trọ chấp hành nghiêm chỉnh pháp luật của Nhà nước, các quy định của chính quyền địa phương; thực hiện tốt các quy định về khai báo tạm trú, tạm vắng; vận động sinh viên thuê trọ tích cực tham gia các phong trào văn hóa, văn nghệ, thể dục thể thao, từ thiện, tình nguyện... do địa phương tổ chức.

Bốn là, các chủ nhà trọ cần có sự phối hợp, hợp tác chặt chẽ với chính quyền, công an địa phương trong việc thực hiện các quy định pháp luật liên quan đến hoạt động kinh doanh nhà trọ.

Năm là, các chủ nhà trọ cần giữ mối liên hệ chặt chẽ, thường xuyên với gia đình (cha mẹ, người thân) của những sinh viên thuê trọ tại khu vực nhà mình trên cơ sở thỏa thuận giữa hai bên.

3. Phát huy vai trò, trách nhiệm của các đơn vị, hội và đoàn thể trong trường đối với việc quản lý, giáo dục, định hướng sinh viên phòng, chống và giảm thiểu tệ nạn xã hội

3.1 Tăng cường hơn nữa vai trò, trách nhiệm và sự phối hợp giữa các khoa chuyên môn, phòng chức năng trong việc quản lý, giáo dục và định hướng sinh viên luật phòng chống tệ nạn xã hội

3.1.1 Vai trò, trách nhiệm của các khoa chuyên môn trong việc quản lý, giáo dục và định hướng sinh viên phòng chống tệ nạn xã hội

Một là, tùy theo lĩnh vực chuyên môn của từng khoa, có thể tổ chức biên soạn các tài liệu chuyên sâu về pháp luật phòng chống tệ nạn xã hội để phổ biến, tuyên truyền trong sinh viên luật thông qua các hình thức như nói chuyện chuyên đề, phát tài liệu miễn phí cho sinh viên... **Hai là**, phối hợp với các Phòng Đào tạo, Phòng Công tác sinh viên, Hội Sinh viên, Đoàn Thanh niên tổ chức và chủ trì các cuộc hội thảo theo các chủ đề về phòng chống tệ nạn xã hội trong sinh viên, như tổ chức cho sinh viên đăng ký bài viết, phân công giáo viên hướng dẫn sinh viên viết bài, thẩm định nội dung, chủ trì hội thảo. Đây là một loại diễn đàn rất quan trọng và cần thiết nơi sinh viên có thể bày tỏ tiếng nói, quan điểm của họ về tệ nạn xã hội; thu hút các sinh viên khác tham dự hội thảo. **Ba là**, mỗi khoa, dựa vào đội ngũ cán bộ, giảng viên của mình, có thể đảm nhiệm vai trò, trách nhiệm khác nhau trong giáo dục, định hướng sinh viên phòng chống tệ nạn xã hội. **Bốn là**, các khoa chuyên môn cần tích cực phối hợp với các đơn vị chức năng, hội, đoàn thể trong trường tổ chức các cuộc thi tìm hiểu pháp luật về phòng chống tệ nạn xã hội cho sinh viên toàn trường.

3.1.2 Vai trò, trách nhiệm của Phòng Đào tạo, Phòng Công tác sinh viên trong việc quản lý, giáo dục và định hướng sinh viên phòng chống tệ nạn xã hội

Trong quá trình thực hiện các chức năng, nhiệm vụ của mình, lãnh đạo, nhân viên Phòng Đào tạo có thể phát huy vai trò giáo dục, định hướng sinh viên phòng chống tệ nạn xã hội thông qua những hình thức khác nhau, như thường xuyên nhắc nhở sinh viên tuân thủ các nội quy, quy chế học tập, rèn luyện, tránh xa tệ nạn xã hội; lồng ghép nội dung giáo dục phòng chống tệ nạn xã hội trong các dịp gặp gỡ, tiếp xúc, giao lưu, tư vấn học tập cho sinh viên. Bộ phận xây dựng kế hoạch giảng dạy, thời khóa biểu có thể nhanh chóng, kịp thời cung cấp thời khóa biểu cá nhân từng học kỳ của sinh viên cho gia đình, người thân của họ khi có yêu cầu.

Phòng Công tác sinh viên có vai trò, trách nhiệm to lớn trong quản lý sinh viên, định hướng họ tự phòng chống và tham gia phòng chống tệ nạn xã hội.

Thứ nhất, trong quá trình thực hiện các chức năng, nhiệm vụ của mình, Phòng Công tác sinh viên cần lồng ghép các nội dung về phòng chống tệ nạn xã hội để tuyên truyền, phổ biến trong sinh viên. **Thứ hai**, Phòng Công tác sinh viên cần quan tâm và chú trọng đầu tư, định hướng để việc tổ chức các phong trào, hoạt động cho sinh viên đi vào thực chất, có chiều sâu và phát huy được hiệu quả trong sự phối kết hợp chặt chẽ giữa Phòng Công tác sinh viên với Đoàn Thanh niên, Hội Sinh viên... **Thứ ba**, Phòng Công tác sinh viên nên đề xuất với lãnh đạo Nhà trường và chủ trì xây dựng Bản quy định về vai trò, trách nhiệm của sinh viên luật trong việc tự phòng chống và tham gia phòng chống tệ nạn xã hội. **Thứ tư**, Phòng Công tác sinh viên cần tích cực động viên, khuyến khích sinh viên nhiệt tình tham gia các cuộc hội thảo khoa học trong sinh viên về phòng chống tệ nạn xã hội, các cuộc thi tìm hiểu pháp luật về phòng chống tệ nạn xã hội khi chúng được tổ chức. **Thứ năm**, đối với số sinh viên nội trú, Phòng Công tác sinh viên tăng cường phối hợp chặt chẽ hơn nữa với Phòng Quản trị, Đoàn thanh niên, Hội sinh viên, Trạm y tế, theo dõi, kiểm tra việc thực hiện nội quy ký túc xá sinh viên; có biện pháp xử lý kịp thời đối với những sinh viên có hành vi sai lệch, có biểu hiện tham gia vào các loại tệ nạn xã hội. **Thứ sáu**, Phòng Công tác sinh viên phối hợp với các cơ quan hữu quan để quản lý số sinh viên ngoại trú, thực hiện tốt Quy chế công tác học sinh, sinh viên ngoại trú trong các trường đại học, cao đẳng, trung học chuyên nghiệp. **Thứ bảy**, Phòng Công tác sinh viên cần phải chú trọng việc thiết lập và củng cố mối quan hệ giữa Nhà trường với gia đình sinh viên nhằm phối hợp giải quyết những vấn đề có liên quan đến sinh viên.

3.1.3 Phòng bảo vệ phối hợp chặt chẽ với Phòng quản trị (bộ phận quản lý ký túc xá) trong việc quản lý và định hướng số sinh viên nội trú phòng chống tệ nạn xã hội

Phòng bảo vệ quản lý chặt chẽ giờ giấc ra vào ký túc xá của sinh viên nội trú, xử lý nghiêm các trường hợp sinh viên vi phạm nội quy, tăng cường công tác tuần tra, kiểm

soát các khu vực trong trường; thường xuyên nhắc nhở sinh viên giữ gìn vệ sinh môi trường, chấp hành nội quy, quy chế, không tham gia vào các loại tệ nạn xã hội

Để góp phần nâng cao ý thức phòng chống tệ nạn xã hội cho sinh viên nội trú, bộ phận quản lý ký túc xá cần thường xuyên duy trì chế độ trực ban, làm tốt công tác khai báo tạm trú, tạm vắng, nhắc nhở sinh viên chấp hành nội quy ký túc xá, xử lý nghiêm các trường hợp vi phạm để răn đe, giáo dục các sinh viên khác; giữ mối liên hệ với gia đình, người thân của những sinh viên nội trú; tuyên truyền phổ biến pháp luật về phòng chống tệ nạn xã hội trong sinh viên...

3.2 Phát huy mạnh mẽ vai trò, trách nhiệm của Đoàn Thanh niên, Hội sinh viên trong việc giáo dục, định hướng sinh viên phòng chống tệ nạn xã hội

Thứ nhất, Đoàn Thanh niên, Hội sinh viên phối hợp với các Khoa chuyên môn, đội ngũ giảng viên nhà trường tổ chức biên soạn bộ tài liệu chuẩn phục vụ công tác tuyên truyền phòng chống tệ nạn xã hội trong sinh viên.

Thứ hai, ngoài việc tổ chức cho sinh viên luật ký cam kết phòng chống ma túy và các loại tệ nạn xã hội, Đoàn Thanh niên và Hội sinh viên còn cần phối hợp với nhau để thường xuyên duy trì các hoạt động tuyên truyền phòng chống tệ nạn xã hội nhằm củng cố ý thức phòng chống tệ nạn xã hội trong sinh viên luật bằng nhiều hình thức đa dạng.

Thứ ba, cùng với việc đi sâu, đi sát, nắm bắt tình hình ăn ở, học tập, sinh hoạt của đoàn viên, hội viên, động viên họ cố gắng vượt khó, vươn lên trong học tập, rèn luyện; Đoàn Thanh niên và Hội Sinh viên cần lựa chọn các sinh viên ưu tú, nhiệt tình làm hạt nhân nòng cốt để thành lập Đội sinh viên tuyên truyền phòng chống tệ nạn xã hội.

Thứ tư, trong thời gian tới, Đoàn Thanh niên và Hội sinh viên nên phối hợp với các đơn vị chức năng trong trường triển khai cuộc vận động như “*Sinh viên luật gương mẫu, đi đầu thực hiện trong phòng chống tệ nạn xã hội*”. Việc đầu tiên nên làm là tổ chức cuộc thi tìm hiểu pháp luật về phòng chống tệ nạn xã hội trong toàn thể sinh viên.

4. Nâng cao ý thức đấu tranh tự phê bình và phê bình của sinh viên trong phòng, chống các tệ nạn xã hội

4.1 Nâng cao ý thức đấu tranh tự phê bình của sinh viên trong phòng chống tệ nạn xã hội

Để nâng cao ý thức đấu tranh tự phê bình trong phòng chống tệ nạn xã hội, bản thân mỗi sinh viên cần làm tốt các nội dung, yêu cầu sau:

Thứ nhất, mỗi sinh viên tự nâng cao nhận thức, hiểu biết về bản chất của các loại tệ nạn xã hội. Về bản chất, tệ nạn xã hội là hiện tượng xã hội có tính tiêu cực, biểu hiện thông qua các loại hành vi sai lệch chuẩn mực xã hội, vi phạm đạo đức, pháp luật hiện hành, phá vỡ thuần phong mỹ tục, lối sống lành mạnh, tiến bộ trong xã hội, có thể gây

những hậu quả nghiêm trọng cho các cá nhân, gia đình và xã hội. Với quan niệm về bản chất của tệ nạn xã hội nêu trên, cần hiểu rằng, tệ nạn xã hội không chỉ bao gồm ma túy, mại dâm, mà còn bao gồm những hành vi sai lệch khác (thường xảy ra trong sinh viên), như chơi lô, đề, đánh bài ăn tiền, cá độ bóng đá, say rượu, nghiện game online...

Thứ hai, mỗi sinh viên cần tiếp tục tự nâng cao nhận thức, hiểu biết về những tác hại, hậu quả mà các loại tệ nạn xã hội có thể gây ra cho sinh viên. Căn cứ để một loại hành vi bị coi là tệ nạn xã hội chủ yếu là do những tác hại, hậu quả mà hành vi đó có thể gây ra cho cá nhân người tham gia, thực hiện hành vi đó. Tệ nạn xã hội trong sinh viên luôn có những tác động, ảnh hưởng nghiêm trọng đối với hoạt động học tập, rèn luyện của bản thân mỗi sinh viên.

Thứ ba, nâng cao nhận thức, hiểu biết về những nguyên nhân dẫn sinh viên đến chỗ mắc phải các loại tệ nạn xã hội. Có rất nhiều nguyên nhân khiến sinh viên sa ngã, mắc phải các loại tệ nạn xã hội, như: sống xa nhà, không có sự quản lý của cha mẹ, người thân; thiếu nghị lực rèn luyện, phấn đấu; bị các đối tượng xấu rủ rê, lôi kéo, ép buộc; đua đòi theo bạn bè... Sự nhận thức đầy đủ, đúng đắn về các nguyên nhân này cũng là một cách để mỗi sinh viên đấu tranh tự phê bình, tự mình tránh xa những cám dỗ, cạm bẫy của các loại tệ nạn xã hội.

Thứ tư, nâng cao nhận thức, hiểu biết về biện pháp phòng chống tệ nạn xã hội trong sinh viên. Nếu như nguyên nhân phát sinh tệ nạn xã hội trong sinh viên được nhìn nhận từ bốn phía: phía môi trường xã hội (tác động tiêu cực), phía hoạt động các cơ quan nhà nước (buông lỏng quản lý), phía gia đình và nhà trường (buông lỏng giáo dục, quản lý) và phía bản thân mỗi sinh viên; thì nguyên nhân từ phía bản thân mỗi sinh viên có tính chất quyết định. Vì vậy, biện pháp khắc phục các nguyên nhân từ phía bản thân mỗi sinh viên là quan trọng nhất trong đấu tranh tự phê bình của mỗi sinh viên.

4.2 Nâng cao ý thức đấu tranh phê bình của sinh viên trong phòng chống tệ nạn xã hội

Một là, mỗi sinh viên luật hãy chủ động, tích cực tham gia tuyên truyền cho các sinh viên khác về bản chất, tác hại, hậu quả, nguyên nhân dẫn đến tệ nạn xã hội trong sinh viên; giúp nhau nâng cao ý thức phòng chống tệ nạn xã hội.

Hai là, tích cực tham gia tuyên truyền pháp luật về phòng chống tệ nạn xã hội trong sinh viên, trong cộng đồng. Một số người vẫn chủ quan khi cho rằng, đã là sinh viên luật thì đương nhiên họ phải có kiến thức, hiểu biết pháp luật về phòng chống tệ nạn xã hội.

Ba là, sinh viên luật cùng nhau tự giác thực hiện tốt các biện pháp phòng chống tệ nạn xã hội trong sinh viên do các đơn vị chức năng, các hội, đoàn thể trong trường, các cơ quan nhà nước và chính quyền địa phương đưa ra.

Bốn là, nếu biết trong lớp, trong phòng ở, khu vực nhà trọ có sinh viên tham gia vào một loại tệ nạn xã hội nào đó thì hãy tìm cách động viên, thuyết phục họ từ bỏ tệ nạn xã hội.

V. KẾT LUẬN

Phòng chống và giảm thiểu tệ nạn xã hội là một bộ phận quan trọng trong sự nghiệp cách mạng của nhân dân ta. Đây là một trong những điều kiện cơ bản để ổn định và lành mạnh hóa xã hội, góp phần đẩy mạnh quá trình phát triển và tiến bộ xã hội góp phần làm cho sự nghiệp đổi mới đạt những kết quả vững chắc. Vấn đề này lại các đặc biệt quan trọng với các lứa học sinh, sinh viên là thế hệ trẻ tương lai của đất nước. Để phòng chống và giảm thiểu được tệ nạn xã hội trong sinh viên là một vấn đề phức tạp và khó khăn; phải sử dụng đồng bộ các biện pháp hành chính, giáo dục, pháp luật,... Đồng thời cũng cần có sự phối kết hợp giữa các cơ quan, đơn vị, từ cả phía gia đình sinh viên và từ cả xã hội để góp phần bảo đảm cho công tác phòng chống cũng như giảm thiểu tệ nạn xã hội trong sinh viên được phát huy hiệu quả một cách tốt nhất.

TÀI LIỆU THAM KHẢO

Phòng chống tác hại của ma túy, Cổng thông tin điện tử Chính phủ, <http://www.lamdong.gov.vn/vi-VN/a/phongchongmatuy/tachai/Pages/Tac-hai-ma-tuy.aspx>, số báo đăng ngày 10/07/2020.

Thương Huyền (2021), Cổng thông tin điện tử Chính phủ, *Ma túy thế hệ mới - Mối hiểm họa học đường*, số báo đăng ngày 08/11/2021 [ttp://www.ict-dongthap.gov.vn/Detail.aspx?Channel=11&RecID=683](http://www.ict-dongthap.gov.vn/Detail.aspx?Channel=11&RecID=683)

TS. DS. Nguyễn Hữu Đức (Trường Đại học Y-Dược Thành phố Hồ Chí Minh), *Tệ nạn nghiện rượu: vấn đề y học và xã hội*, Bài viết đăng tại: http://www.ykhoanet.com/xahoi/ytecongcong/30_133.htm.

Thực trạng báo động về nhận thức của học sinh, sinh viên về ma túy, Báo Tiền phong, số báo đăng ngày 03/06/2021, <https://tienphong.vn/thuc-trang-bao-dong-ve-nhan-thuc-cua-hoc-sinh-sinh-vien-ve-ma-tuy-post1342648.tpo>

Đảng Cộng sản Việt Nam, Văn kiện Đại hội đại biểu toàn quốc lần thứ IX, Nxb. Chính trị Quốc gia, Hà Nội, 2001, tr. 208.

CÔNG TÁC BẢO VỆ AN NINH TƯ TƯỞNG SINH VIÊN TRÊN KHÔNG GIAN MẠNG THỜI KỲ CHUYỂN ĐỔI SỐ TẠI TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN

Trung tá, TS. Nguyễn Trần Tuấn

Trường Đại học An ninh nhân dân

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> an ninh tư tưởng; chuyển đổi số; không gian mạng; sinh viên.	Các thế lực thù địch đang tích cực sử dụng không gian mạng vào các hoạt động tuyên truyền phá hoại tư tưởng sinh viên với nhiều hình thức, thủ đoạn tinh vi, nguy hiểm. Bài viết làm rõ cách thức, phương pháp Trường Đại học ANND tổ chức bảo vệ an ninh tư tưởng sinh viên trên không gian mạng thời kỳ chuyển đổi số

Với đặc điểm nổi trội là tốc độ kết nối nhanh, phạm vi chia sẻ rộng, hiệu quả tác động lớn không gian mạng đang trở thành môi trường cung cấp, chia sẻ, trao đổi, khai thác sử dụng thông tin, đem lại những lợi ích to lớn, từng bước khẳng định vai trò thiết yếu trong đời sống xã hội. Tuy nhiên, bên cạnh những mặt tích cực, không gian mạng cũng trở thành công cụ mà các thế lực thù địch, phản động tận dụng tối đa để nguy tạo và lan truyền những quan điểm sai trái, thù địch với trọng tâm là hòng xóa bỏ nền tảng tư tưởng của Đảng Cộng sản Việt Nam.

Thực hiện âm mưu này, chúng đã xây dựng hàng loạt tin, bài, hình ảnh, bịa đặt, cắt ghép, thậm chí là xây dựng cả phim, phóng sự để xuyên tạc bản chất khoa học, cách mạng nền tảng tư tưởng của Đảng, phủ nhận vai trò và thành tựu lãnh đạo của Đảng, lấy sự sụp đổ của Liên Xô để quy kết sai lầm của “chủ nghĩa Mác - Lênin” cũng là sai lầm của Đảng Cộng sản Việt Nam. Tập trung hướng lái, định hướng dư luận “một Đảng Cộng sản cầm quyền thì chỉ dẫn đến độc tài, độc trị, không có dân chủ” nếu có thì là “giả tạo” trái với nguyên tắc nhà nước pháp quyền của dân, do dân, vì dân, bầu cử trong Đảng đều là “màn kịch dân chủ”, do Đảng Cộng sản tự làm, tự diễn không đại diện cho nhân dân nhằm vận động quần chúng đòi thực hiện “đa nguyên chính trị”, “đa đảng đối lập”... Cùng với đó, các thế lực thù địch sử dụng các vụ, việc hiện tượng đã, đang diễn ra ở một số lĩnh vực, một số cơ quan ban, ngành để quy kết cho bản chất của Đảng, Nhà nước nhằm lôi kéo người dân đồng lòng phản ứng, ủng hộ quan điểm sai trái, gây chia rẽ, kích động thù hận, làm mất uy tín Đảng, Nhà nước với quần chúng Nhân dân.

Trong khi đó, hiện nay cùng với sự đầu tư phát triển khoa học công nghệ, thực hiện nhiều chính sách, chiến lược chuyển đổi số quốc gia đáp ứng yêu cầu thời kỳ công

nghiệp hóa, hiện đại hóa đất nước theo sát sự phát triển của thế giới môi trường quốc tế, không gian mạng đang và ngày càng trở nên phổ biến trong xã hội nước ta. Nhiều sinh viên sử dụng điện thoại thông minh smartphone, máy vi tính để tham gia mạng xã hội như Facebook, Zalo, Twitter, Wechat... Tuy nhiên, thực tiễn cũng cho thấy vẫn còn tồn tại một bộ phận quần chúng có nhận thức mơ hồ, dao động về tư tưởng, mất phương hướng chính trị, thậm chí còn tiếp tay, giúp sức cho những việc làm sai trái, tạo sự nhiễu loạn thông tin trên môi trường không gian mạng; thường xuyên chia sẻ, thích (like) những bài, báo, trang mạng, bài viết, blog, video của những phần tử chống đối, phản động, chia sẻ thông tin kích động biểu tình hay hình ảnh, video, clip về cảnh tụ tập đông người, biểu tình, gây rối, ủng hộ lời xúi giục của kẻ xấu, có những hành động vi phạm pháp luật, gây mất an ninh trật tự...

Nhận thức đúng vai trò, vị trí và tác động của không gian mạng đến đời sống xã hội nói chung và sinh viên nói riêng đồng thời thực hiện Quyết định số 311/QĐ-TTg, ngày 05/3/2022 về “Chương trình giáo dục lý tưởng cách mạng, đạo đức, lối sống, văn hóa cho thanh niên, thiếu niên trên không gian mạng giai đoạn 2022 – 2030” trong đó xác định “cần chủ động nắm bắt “mặt trận” tư tưởng và định hướng dư luận xã hội càng sớm càng tốt; phải xác định hoạt động thông tin, tuyên truyền và định hướng dư luận xã hội trên không gian mạng là nhiệm vụ trọng tâm, cần được ưu tiên trong công tác tư tưởng của Đảng”. Trường Đại học An ninh nhân dân (ANND) đã có nhiều hoạt động, chương trình, kế hoạch thiết thực nhằm nâng cao nhận thức, bảo vệ an ninh tư tưởng sinh viên đồng thời phát huy vai trò sinh viên trong bảo vệ nền tảng tư tưởng của đảng trên không gian mạng thời kỳ chuyển đổi số. Mục tiêu của chương trình hướng tới củng cố, nâng cao năng lực nhận diện, sức đề kháng của sinh viên góp phần chủ động phòng ngừa, phát hiện và tham gia tích cực vào phản bác quan điểm sai trái, thù địch trên không gian mạng đồng thời tích cực tham gia bảo vệ nền tảng tư tưởng của Đảng thời kỳ chuyển đổi số. Giáo dục sinh viên ý thức đấu tranh phản bác luận điệu xuyên tạc, sai trái, thù địch trên không gian mạng, kết hợp “xây” và “chống”, trong đó xây dựng lập trường, bản lĩnh chính trị, kỹ năng xử lý, ứng xử trên không gian mạng cho sinh viên đóng vai trò quan trọng hàng đầu. “Xây” đi đôi với “chống” là một trong những nguyên tắc căn bản để giáo dục, rèn luyện tư tưởng chính trị, đạo đức, lối sống, văn hóa, hướng tới phát triển nhân cách toàn diện cho sinh viên trong các trường đại học hiện nay. “Xây” là nhiệm vụ cơ bản, lâu dài, xuyên suốt, “chống” những biểu hiện lệch lạc trong ứng xử trên không gian mạng trước những thông tin xấu, độc, là nhiệm vụ quan trọng, cấp bách trong công tác giáo dục sinh viên trong các trường đại học,... từ đó góp phần ngăn chặn, đẩy lùi những biểu hiện chưa phù hợp, chưa đúng đắn, thậm chí “tự diễn biến” về tư tưởng chính trị, đạo đức, lối sống trong thanh niên, sinh viên, trước tác động của những thông tin xuyên tạc, sai trái, chống phá của các thế lực phản động, thù địch trên không

gian mạng. Cùng với việc xây dựng, bồi dưỡng những phẩm chất chính trị, đạo đức cách mạng tốt đẹp, phải đồng thời phát hiện sớm, định hướng, hướng dẫn sinh viên phòng, tránh, đấu tranh chống những cái xấu, cái sai.

Với những định hướng trên, qua công tác giáo dục, đào tạo trường Đại học ANND đã không chỉ góp phần bảo vệ tư tưởng sinh viên mà còn hướng sinh viên tích cực tham gia đấu tranh, phản bác thông tin, quan điểm sai trái, thù địch trên không gian mạng. Đã tích cực tham gia chia sẻ, lan tỏa sâu rộng những thông tin tích cực, góp phần nâng cao tinh thần cảnh giác, nhận thức của sinh viên trong việc chấp hành pháp luật, đấu tranh với luận điệu xuyên tạc, thông tin sai sự thật của các phần tử cơ hội chính trị, phản động; tích cực tham gia đấu tranh phản bác các quan điểm sai trái, thù địch; quán triệt và thực hiện có hiệu quả các chỉ thị, nghị quyết của Đảng, Nhà nước về bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch... Sinh viên ANND đã phát hiện và ngăn chặn nhiều tin giả và các tài khoản Facebook đăng tải thông tin sai sự thật. Mỗi sinh viên ANND đều phấn đấu rèn luyện là một “chiến binh” “sắc về thông tin, vững về kiến thức” để tham gia phản bác lại các quan điểm, luận điệu xuyên tạc của các thế lực thù địch trên không gian mạng.

Nhằm xây dựng đội ngũ sinh viên có đủ năng lực, trình độ tham gia bảo vệ nền tảng tư tưởng của đảng trên không gian mạng thời kỳ chuyển đổi số, công tác giáo dục chính trị, tư tưởng cho sinh viên Đại học ANND luôn nhận được sự quan tâm của Đảng Ủy, Ban Giám hiệu, nhất là trong quá trình quán triệt và thực hiện Nghị quyết số 35-NQ/TW, ngày 22/10/2018 của Bộ Chính trị khóa XII “Về tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác quan điểm sai trái, thù địch trong tình hình mới” và những vấn đề liên quan đến công tác giáo dục tư tưởng chính trị theo tinh thần Nghị quyết của Đại hội XIII của Đảng. Việc tổ chức học tập, phổ biến các nghị quyết của Trung ương, Bộ Công an liên quan tới công tác tư tưởng đến sinh viên luôn được các Khoa, Phòng, Trung tâm của trường tiến hành với tinh thần đổi mới, kịp thời, hiệu quả, với những nội dung được lựa chọn thiết thực, bám sát tình hình thực tiễn; trong đó chú trọng đến chiều sâu của công tác giáo dục nhằm nâng nhận thức, ý thức đấu tranh phản bác các luận điệu xuyên tạc, sai trái, thù địch trên không gian mạng.

Nhà trường đã tổ chức nhiều buổi nói chuyện chuyên đề về các lĩnh vực chính trị, thời sự và kỹ năng nhận diện, phản bác các quan điểm sai trái thù địch, bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng cho sinh viên toàn trường. Trường cũng thường xuyên mời các chuyên gia đến từ Hội đồng lý luận Trung ương, lãnh đạo Bộ Công an, cán bộ thực tiễn chia sẻ các vấn đề có tính thời sự, nhận diện được những thủ đoạn, phương thức chống phá của các thế lực thù địch, nhất là những thủ đoạn nhằm vào giới trẻ, từ đó có ý thức nâng cao cảnh giác, ứng xử phù hợp với những thông tin xấu, độc trên không gian mạng. Trường cũng hỗ trợ cho Đoàn Thanh niên, các trung đội

học viên nguồn kinh phí để xây dựng các kho tư liệu sinh hoạt, phòng truyền thống; các hoạt động ngoại khóa lồng ghép việc giáo dục ý thức đấu tranh phản bác những luận điệu xuyên tạc, sai trái, thù địch trên không gian mạng... Đội ngũ giáo viên nhà trường cũng tổ chức, hướng dẫn sinh viên xây dựng những trang thông tin điện tử, trang mạng xã hội, hướng dẫn sinh viên viết bài, đăng, chia sẻ thông tin phục vụ công tác tuyên truyền, định hướng tư tưởng, giáo dục ý thức chính trị, tư tưởng cho sinh viên nói riêng và quần chúng nói chung.

Việc giáo dục ý thức đấu tranh phản bác các luận điệu xuyên tạc, sai trái, thù địch trên không gian mạng cũng được đội ngũ giáo viên trường quan tâm đưa vào nội dung biên soạn tài liệu và truyền tải thường xuyên, liên tục đến sinh viên thông qua các bài giảng trên lớp. Phương thức, nội dung, phương tiện giáo dục được đổi mới, nhằm tăng tính hấp dẫn và hiệu quả giáo dục đối với sinh viên, như giáo dục bằng truyền thông đa phương tiện, công nghệ thông tin, xây dựng các diễn đàn, hội nhóm theo sở thích, giáo dục truyền thống về nguồn... đổi mới phương pháp giảng dạy để sinh động hơn các nội dung chính trị, lấy người học làm trung tâm. Chú trọng khai thác, sử dụng không gian mạng để phổ biến những thông tin lý luận chính trị thông qua trang thông tin điện tử của trường. Quan tâm trang bị những kiến thức chính trị - pháp luật, bồi đắp nhận thức chính trị, đạo đức cách mạng một cách tự nhiên, tự nguyện, xây dựng cơ sở khoa học cho nhận thức và niềm tin vào nền tảng tư tưởng của Đảng, con đường đi lên chủ nghĩa xã hội ở nước ta... Việc giáo dục chủ nghĩa Mác - Lê-nin, tư tưởng Hồ Chí Minh cho sinh viên không dừng lại ở những nhận thức cảm tính mà hướng tới chuyển hoá thành tình cảm, ý chí, niềm tin chính trị, động cơ và hành động cách mạng đối với mỗi sinh viên, giúp sinh viên có đủ kiến thức, tri thức chính trị để nhận biết và xử lý, ứng xử đúng, linh hoạt trước những thông tin, vấn đề chính trị phức tạp trên môi trường không gian mạng.

Phòng công tác chính trị, Quản lý học viên, Ban thanh niên trường thường xuyên tìm hiểu, theo dõi, nắm bắt và kịp thời định hướng tư tưởng sinh viên qua việc cùng tham dự các hoạt động sinh hoạt tại cơ sở, qua các diễn đàn và không gian mạng, nhất là mạng xã hội, bảo đảm sinh viên không bình luận tiêu cực, phát tán thông tin xấu, độc, không bị kích động, lôi kéo bởi các phần tử phản động để tham gia các hoạt động tụ tập đông người khi diễn ra các vấn đề nóng của xã hội... Chủ động xây dựng, duy trì hoạt động các trang thông tin điện tử, trang mạng xã hội phù hợp với sở thích, tâm sinh lý lứa tuổi để sinh viên trao đổi, chia sẻ thông tin, kỹ năng nhận biết, ứng xử và phản bác lại những thông tin xấu, độc, góp phần giúp sinh viên nâng cao nhận thức, tăng khả năng “tự đề kháng” trên môi trường mạng. Mỗi sinh viên an ninh là một chiến sĩ trên mặt trận tư tưởng, “xung kích” sử dụng mạng xã hội với tinh thần “lấy cái đẹp, dẹp cái xấu”.

Các hoạt động giáo dục ý thức chính trị trên mạng xã hội cho sinh viên cũng được thực hiện thông qua các cuộc thi viết, thi sân khấu hóa, thi báo cáo viên giỏi, thi đội

tuyên truyền ca khúc cách mạng. Coi trọng tổ chức hoạt động biểu dương, tôn vinh các tấm gương sinh viên tiêu biểu trong học tập và tham gia các phong trào chính trị - xã hội của nhà trường. Nhiều hoạt động mang tính định hướng văn hóa sử dụng mạng xã hội cho sinh viên đã được tổ chức sôi nổi như: Chuỗi chương trình tuyên truyền Luật An ninh mạng, Luật An toàn thông tin, Bộ Quy tắc ứng xử trên không gian mạng; Hướng dẫn kỹ năng sử dụng Internet an toàn; phổ biến quy định bảo vệ thông tin cá nhân trên không gian mạng; Phát động phong trào “Người đoàn viên công an tiêu biểu, tích cực trên không gian mạng”;... đã góp phần nâng cao “sức đề kháng” cho sinh viên, tạo nên lớp “vaccine” phòng ngừa âm mưu, hoạt động của các thế lực thù địch trên không gian mạng. Từ các sân chơi trên, ý thức chính trị cũng như ý thức đấu tranh phản bác các luận điệu xuyên tạc, thù địch trên không gian mạng của sinh viên trong toàn trường cũng được nâng lên.

Tuy nhiên, bên cạnh những thành tựu đạt được, công tác giáo dục chính trị, tưởng cho sinh viên trên không gian mạng thời kỳ chuyển đổi số tại Trường Đại học ANND vẫn còn tồn tại một số hạn chế, như: Do ảnh hưởng của công việc học tập, việc xây dựng, chọn lọc thông tin phản bác quan điểm sai trái, thù địch trên không gian mạng vẫn chưa được tiến hành thường xuyên; các trang thông tin mới chỉ có sự tham gia của sinh viên an ninh chưa có sự tương tác nhiều với sinh viên của các trường khác; một số sinh viên còn hạn chế về kỹ năng sử dụng internet, mạng xã hội, trách nhiệm chưa cao trong việc chia sẻ thông tin tốt, câu chuyện đẹp, còn thờ ơ với việc chia sẻ thông tin tốt nhưng lại thích những tin tức “giật gân”, câu like...

Được đào tạo chính quy, tinh nhuệ, hiện đại, nắm bắt tốt về công nghệ thông tin trong chuyển đổi số quốc gia, sinh viên Đại học ANND được xác định là một trong những đầu mối quan trọng, lực lượng nòng cốt, tiên phong trong tham gia nhiệm vụ bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác quan điểm sai trái, thù địch trong thời kỳ chuyển đổi số. Để nâng cao hơn nữa nhận thức, trách nhiệm, phát huy vai trò xung kích, sáng tạo của sinh viên ANND trong bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác quan điểm sai trái, thù địch trên không gian mạng, thời gian tới, sinh viên cần tập trung thực hiện tốt các vấn đề sau:

Một là, căn cứ vào những yêu cầu thực tiễn, Đảng ủy, Ban giám hiệu trường Đại học ANND cần tiếp tục xây dựng, ban hành các nghị quyết, chương trình hành động, đề ra các chủ trương, biện pháp thực hiện nhiệm vụ bảo vệ an ninh tư tưởng sinh viên. Quán triệt, tuyên truyền, phổ biến nhiệm vụ bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch đến toàn thể giáo viên, sinh viên. Chỉ đạo tổ chức việc thực hiện nhiệm vụ bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch, đề ra cách thức tổ chức phù hợp để phát huy vai trò của sinh viên; huy động cơ sở vật chất và các điều kiện bảo đảm triển khai nhiệm vụ

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

bảo vệ nền tảng tư tưởng của Đảng có hiệu quả. Kiểm tra, giám sát việc thực hiện nhiệm vụ, kịp thời phát hiện những cách làm hay, những mô hình tiêu biểu, những điển hình để tuyên dương, nhân rộng, cũng như điều chỉnh, uốn nắn những cá nhân, tổ chức, đoàn thể chưa thực hiện tốt nhiệm vụ; kịp thời giúp đỡ các sinh viên có những dấu hiệu bàng quan chính trị, phai nhạt lý tưởng, hay bị các thế lực phản động lôi kéo đi ngược lại quan điểm của Đảng, chính sách, pháp luật của Nhà nước.

Hai là, nâng cao trách nhiệm, vai trò nêu gương của đội ngũ sinh viên An ninh trong thực hiện nhiệm vụ bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng trong thời kỳ chuyển đổi số. Mỗi sinh viên phải nhận thức đúng về vai trò, vị trí quan trọng của chuyển đổi số quốc gia trong tình hình hiện nay. Từ đó tích cực học tập nâng cao trình độ, năng lực khai thác, sử dụng công nghệ thông tin, xác định đúng nhiệm vụ, vai trò của mình trong thực hiện nhiệm vụ bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng; tích cực cập nhật những kỹ năng nhận diện và đấu tranh chống lại âm mưu, thủ đoạn của các thế lực thù địch trên mạng xã hội và các kênh truyền thông khác; tỉnh táo, bản lĩnh trước các thông tin xấu độc, trước những thủ đoạn lôi kéo, mua chuộc của các thế lực thù địch; có hiểu biết và trách nhiệm khi tương tác trên mạng xã hội; chủ động chia sẻ tin tốt, tin hay với phương châm “lấy cái đẹp dẹp cái xấu”. Tuyệt đối thực hiện nghiêm quy định của pháp luật, của ngành, của đơn vị khi tham gia mạng xã hội.

Hai là, nhà trường cần tăng cường hơn nữa công tác nắm tình hình trên không gian mạng, phát hiện các trang thông tin, bài có nội dung xấu, độc, thù địch để kịp thời tham mưu Ban Giám hiệu chỉ đạo các Khoa, Phòng, Trung tâm có giải pháp ngăn chặn, xử lý; mở rộng và nâng cao hơn nữa hiệu quả hoạt động các trang thông tin trong đấu tranh phản bác quan điểm sai trái, thù địch; hướng dẫn sinh viên sử dụng tài khoản mạng xã hội cá nhân như một kênh tuyên truyền nhằm nâng cao cảnh giác cho người thân, bạn bè, người thân, không để họ vi phạm pháp luật trên không gian mạng, không nghe theo lời xúi giục, luận điệu xuyên tạc của các thế lực thù địch đồng thời huy động người thân cùng tham gia công tác đấu tranh phản bác thông tin xấu, độc. Phát huy tối đa hiệu quả, mặt tích cực của không gian mạng phục vụ công tác tuyên truyền, định hướng, kịp thời cung cấp thông tin chính thống đến quần chúng nhân dân. Huy động 100% lực lượng sinh viên tham gia viết bài, bình luận phản bác các thông tin xấu độc; chia sẻ, lan tỏa, phủ xanh thông tin tích cực đến cộng đồng mạng cũng như người thân, bạn bè, quần chúng nhân dân nơi đoàn viên cư trú.

Bốn là, kịp thời nắm bắt diễn biến tư tưởng sinh viên cả trong môi trường thực và trên không gian mạng từ đó có những điều chỉnh, định hướng nhận thức, tuyên truyền cho sinh viên phù hợp thực tiễn. Công tác tuyên truyền cần mang tính định hướng, “lấy cái đẹp, dẹp cái xấu” trong lực lượng sinh viên, phát huy vai trò xung kích, tiên phong của sinh viên ANND tham gia thực hiện các nhiệm vụ chính trị bảo vệ nền tảng tư tưởng

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

của Đảng trong thời kỳ chuyển đổi số quốc gia. Đối với đội ngũ giáo viên, cần tiếp tục nâng cao năng lực, trình độ chuyên môn, nắm vững chủ trương, chính sách của Đảng, Nhà nước phát huy tinh thần tích cực, sáng tạo trong hướng dẫn, tập hợp sinh viên để có những cách làm hay, sáng tạo bám sát thực tiễn để nâng cao hơn nữa hiệu quả đấu tranh phản bác quan điểm sai trái thù địch bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng. phát huy vai trò gương mẫu của các chủ thể giáo dục và vai trò của giảng viên giảng dạy lý luận chính trị trong công tác bảo vệ nền tảng tư tưởng của Đảng. Các giáo viên tiếp tục nêu gương trong việc sử dụng không gian mạng để đấu tranh phản bác các quan điểm sai trái, thù địch. Nêu gương gắn với các hoạt động chính trị của đội ngũ nhà giáo đem lại tác động to lớn đến sinh viên, thúc đẩy quá trình học tập, rèn luyện và ý thức tự giác trong nhận diện, đấu tranh với các biểu hiện, lời nói, hành vi, thông tin xấu, độc. Kiên quyết phòng, chống sự suy thoái về tư tưởng chính trị, đạo đức, lối sống, “tự diễn biến”, “tự chuyển hóa” trong nội bộ.

Năm là, Trường Đại học ANND tiếp tục kiến nghị Bộ Công an để đầu tư, tăng cường củng cố cơ sở vật chất, các phương tiện, trang thiết bị phục vụ công tác phản bác quan điểm sai trái thù địch bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng. Phối hợp với các trường, cơ sở đào tạo trên địa bàn để huy động nguồn lực xã hội tham gia vào bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng cho sinh viên An ninh nói riêng và quần chúng trên không gian mạng nói chung.

Trung tá, TS. Nguyễn Trần Tuấn

Tài liệu tham khảo:

Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII, Nxb Chính trị quốc gia Sự thật, Hà Nội, 2021.

Nghị quyết số 35-NQ/TW ngày 22/10/2018 của Bộ Chính trị khóa XII.

Quyết định số 311/QĐ-TTg ngày 05/3/2022 của Thủ tướng chính phủ.

GIẢI PHÁP AN NINH MẠNG VÀ BẢO MẬT THÔNG TIN TẠI TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN TRONG THỜI KỲ CHUYỂN ĐỔI SỐ

CYBER SECURITY AND INFORMATION SECURITY SOLUTIONS AT PEOPLE'S SECURITY UNIVERSITY IN THE PERIOD OF DIGITAL TRANSFORMATION

Lê Cao Hoàng Thiên*, Nguyễn Phạm Minh Hiếu, Bùi Quốc Huy, Đặng Bá Hưng
Trường Đại học An ninh nhân dân

*Email: lecaohoangthien17@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa: an ninh mạng, bảo mật thông tin, chuyển đổi số</i>	Với sự phát triển của công nghệ thông tin trong các trường đại học tại Việt Nam hiện nay, mạng lưới thông tin tại khuôn viên trường ngày càng có vai trò quan trọng hơn, và dần trở thành cơ sở hạ tầng quan trọng cho việc giảng dạy, nghiên cứu khoa học, quản lý nhân sự, tài chính và hợp tác quốc tế tại các trường Đại học. Tuy nhiên, còn tiềm ẩn những nguy cơ rủi ro bị tấn công không gian mạng. Vì vậy việc đảm bảo an ninh mạng và bảo mật thông tin cơ sở dữ liệu đã trở thành vấn đề quan trọng nhất trong việc xây dựng và phát triển đại học. Đặc biệt là các trường Công an, Quân đội vấn đề bảo mật là hết sức quan trọng trong an ninh chính trị nội bộ và bảo vệ bí mật nhà nước. Trong bài viết này, tác giả trình bày các vấn đề tồn tại trong vấn đề an ninh và bảo mật thông tin tại trường Đại học An ninh nhân dân và đề xuất các biện pháp cho vấn đề an ninh mạng và thông tin trong thời kỳ chuyển đổi số hiện nay.
<i>Keywords: cybersecurity, information security, digital transformation</i>	ABSTRACT With the development of information technology in universities in Vietnam today, information network at the campus are more and more important, and gradually become an essential infrastructure for teaching, scientific research, personnel management, finance and international cooperation at the University. However, using the network on campus still has potential risks of cyber attacks. Therefore, ensuring network security and database

information security has become the most important issue in the construction and development of the university. Especially in Police and Military schools, security is extremely important in internal political security and protecting state secrets. In this article, the author presents existing problems in information security and confidentiality at People’s Security University and propose measures for cybersecurity and information in the current Digital age.

1. Giới thiệu:

Trong thời đại thông tin hiện nay, Internet thâm nhập vào mọi mặt của đời sống và sản xuất của con người. Với sự phát triển không ngừng của Internet, các loại tội phạm sử dụng công nghệ cao nảy sinh, tồn tại và phát triển nhanh chóng, đe dọa nghiêm trọng đến an toàn thông tin mạng. Hiện nay, các trường đại học ở Việt Nam đã ứng dụng công nghệ thông tin thường xuyên hơn và đóng vai trò quan trọng trong việc tăng cường công tác quản lý giảng dạy, nghiên cứu khoa học, quản lý nhân sự, tài chính và hợp tác quốc tế. Tuy nhiên, các trường đại học cũng phải đối mặt với những rủi ro lớn về bảo mật như rò rỉ dữ liệu, tấn công của hacker và các vấn đề khác, ảnh hưởng tiêu cực đến hoạt động giảng dạy và sự phát triển của nhà trường. Trước những vấn đề này, Bộ Giáo dục và Đào tạo đã ban hành Quyết định số 5809/QĐ-BGDĐT về việc “Ban hành Quy định bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các đơn vị thuộc Bộ Giáo dục và Đào tạo”. Qua đó, các cơ sở giáo dục đại học cần nắm bắt một cách toàn diện tình hình an ninh mạng lưới các thành viên hiện tại, xây dựng đội ngũ chuyên gia về thông tin, bảo mật, riêng tư, tạo lập hệ thống bảo mật hợp lý, bí mật, cải tiến các ứng dụng trên môi trường mạng, tăng cường giáo dục, nhận thức về bảo mật cơ sở dữ liệu trực tuyến, đảm bảo an ninh mạng và thông tin trong đội ngũ cán bộ, giảng viên và sinh viên trong trường. Trong bài viết này, tác giả trình bày những vấn đề tồn tại về an ninh, an toàn thông tin tại Trường Đại học An ninh nhân dân và đề xuất các giải pháp giải quyết vấn đề an ninh mạng và thông tin trong thời kỳ chuyển đổi số.

2. Cơ sở lý thuyết:

2.1. Những khái niệm cơ bản

2.1.1. An ninh mạng

Theo khoản 1 Điều 2 Luật An ninh mạng 2018 định nghĩa an ninh mạng như sau: An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Theo Wikipedia

An ninh mạng (cybersecurity), an ninh máy tính (computer security), bảo mật công nghệ thông tin (IT security) là việc bảo vệ hệ thống mạng máy tính khỏi các hành vi trộm cắp hoặc làm tổn hại đến phần cứng, phần mềm và các dữ liệu, cũng như các nguyên nhân dẫn đến sự gián đoạn, chuyển lệch hướng của các dịch vụ hiện đang được được cung cấp.

An ninh mạng là thực tiễn của việc bảo vệ các hệ thống điện tử, mạng lưới, máy tính, thiết bị di động, chương trình và dữ liệu khỏi những cuộc tấn công kỹ thuật số độc hại có chủ đích. Tội phạm mạng có thể triển khai một loạt các cuộc tấn công chống lại các nạn nhân hoặc doanh nghiệp đơn lẻ; có thể kể đến như truy cập, làm thay đổi hoặc xóa bỏ dữ liệu nhạy cảm; tống tiền; can thiệp vào các quy trình kinh doanh.

An ninh mạng máy tính bao gồm việc kiểm soát truy cập vật lý đến phần cứng, cũng như bảo vệ chống lại tác hại có thể xảy ra qua truy cập mạng máy tính, cơ sở dữ liệu (SQL injection) và việc lợi dụng lỗ hổng phần mềm (code injection). Do sai lầm của những người điều hành, dù cố ý hoặc do bất cẩn, an ninh công nghệ thông tin có thể bị lừa đảo phi kỹ thuật để vượt qua các thủ tục an toàn thông qua các phương pháp khác nhau.

An ninh mạng hoạt động thông qua một cơ sở hạ tầng chặt chẽ, được chia thành ba phần chính: bảo mật công nghệ thông tin, an ninh mạng và an ninh máy tính.

Bảo mật công nghệ thông tin (với cách gọi khác là bảo mật thông tin điện tử): Bảo vệ dữ liệu ở nơi chúng được lưu trữ và cả khi các dữ liệu này di chuyển trên các mạng lưới thông tin. Trong khi an ninh mạng chỉ bảo vệ dữ liệu số, bảo mật công nghệ thông tin nắm trong tay trọng trách bảo vệ cả dữ liệu kỹ thuật số lẫn dữ liệu vật lý khỏi những kẻ xâm nhập trái phép.

An ninh mạng: Là một tập hợp con của bảo mật công nghệ thông tin. An ninh mạng thực hiện nhiệm vụ đảm bảo dữ liệu kỹ thuật số trên các mạng lưới, máy tính và thiết bị cá nhân nằm ngoài sự truy cập, tấn công và phá hủy bất hợp pháp.

An ninh máy tính: Là một tập hợp con của an ninh mạng. Loại bảo mật này sử dụng phần cứng và phần mềm để bảo vệ bất kỳ dữ liệu nào được gửi từ máy tính cá nhân hoặc các thiết bị khác đến hệ thống mạng lưới thông tin. An ninh máy tính thực hiện chức năng bảo vệ cơ sở hạ tầng công nghệ thông tin và chống lại các dữ liệu bị chặn, bị thay đổi hoặc đánh cắp bởi tội phạm mạng.

Lĩnh vực này dần trở nên quan trọng do sự phụ thuộc ngày càng nhiều vào các hệ thống máy tính và Internet tại các quốc gia, cũng như sự phụ thuộc vào hệ thống mạng không dây như Bluetooth, Wi-Fi, cùng với sự phát triển của các thiết bị "thông minh", bao gồm điện thoại thông minh, TV và các thiết bị khác kết nối vào hệ thống Internet of Things.

2.1.2. Bảo mật thông tin

Chắc hẳn, khái niệm bảo mật hệ thống thông tin không còn là khái niệm xa lạ gì với mỗi chúng ta. Bảo mật thông tin hay còn gọi là Information Security không đơn thuần là bảo vệ thông tin của cá nhân người dùng mà đây còn là những chiến lược nhằm ngăn chặn những hành vi trái phép liên quan tới tài sản, dữ liệu, thông tin riêng của cá nhân hay tổ chức nào đó.

2.1.3. Chuyển đổi số

Để có thể định nghĩa một cách ngắn gọn và dễ hiểu thì chuyển đổi số (Digital Transformation trong tiếng Anh) là sự tích hợp các công nghệ kỹ thuật số vào tất cả các lĩnh vực của một doanh nghiệp, tận dụng các công nghệ để thay đổi căn bản cách thức vận hành, mô hình kinh doanh và cung cấp các giá trị mới cho khách hàng của doanh nghiệp đó cũng như tăng tốc các hoạt động kinh doanh. Chuyển đổi số cũng là một sự thay đổi về văn hóa của các doanh nghiệp, đòi hỏi các doanh nghiệp phải liên tục thay đổi, thử nghiệm cái mới và thoải mái chấp nhận các thất bại.

Tại Việt Nam, khái niệm “Chuyển đổi số” thường được hiểu theo nghĩa là quá trình thay đổi từ mô hình doanh nghiệp truyền thống sang doanh nghiệp số bằng cách áp dụng công nghệ mới như dữ liệu lớn (Big Data), Internet cho vạn vật (IoT), điện toán đám mây (Cloud)... nhằm thay đổi phương thức điều hành, lãnh đạo, quy trình làm việc, văn hóa công ty.

Không chỉ có vai trò quan trọng tại các doanh nghiệp mà chuyển đổi số còn đóng vai trò quan trọng trong các lĩnh vực khác của xã hội như chính phủ, truyền thông đại chúng, y học, khoa học, giáo dục...

“Chuyển đổi số” (Digital Transformation) có thể dễ bị nhầm lẫn với khái niệm “Số hóa” (Digitizing). Để phân biệt hai khái niệm này, có thể hiểu rằng “Số hóa” là quá trình hiện đại hóa, chuyển đổi các hệ thống thường sang hệ thống kỹ thuật số (chẳng hạn như chuyển từ tài liệu dạng giấy sang các file mềm trên máy tính, số hóa truyền hình chuyển từ phát sóng analog sang phát sóng kỹ thuật số...); trong khi đó, “Chuyển đổi số” là khai thác các dữ liệu có được từ quá trình số hóa, rồi áp dụng các công nghệ để phân tích, biến đổi các dữ liệu đó và tạo ra các giá trị mới hơn. Có thể xem “Số hóa” như một phần của quá trình “Chuyển đổi số”

2.2. Chính sách của nhà nước về an ninh mạng

Ưu tiên bảo vệ an ninh mạng trong quốc phòng, an ninh, phát triển kinh tế - xã hội, khoa học, công nghệ và đối ngoại.

Xây dựng không gian mạng lành mạnh, không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Ưu tiên nguồn lực xây dựng lực lượng chuyên trách bảo vệ an ninh mạng; nâng cao năng lực cho lực lượng bảo vệ an ninh mạng và tổ chức, cá nhân tham gia bảo vệ an ninh mạng; ưu tiên đầu tư cho nghiên cứu, phát triển khoa học, công nghệ để bảo vệ an ninh mạng.

Khuyến khích, tạo điều kiện để tổ chức, cá nhân tham gia bảo vệ an ninh mạng, xử lý các nguy cơ đe dọa an ninh mạng; nghiên cứu, phát triển công nghệ, sản phẩm, dịch vụ, ứng dụng nhằm bảo vệ an ninh mạng; phối hợp với cơ quan chức năng trong bảo vệ an ninh mạng.

Tăng cường hợp tác quốc tế về an ninh mạng. (Điều 3 Luật an ninh mạng)

2.3. Nguyên tắc bảo vệ an ninh mạng

Tuân thủ Hiến pháp và pháp luật; bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; phát huy vai trò nòng cốt của lực lượng chuyên trách bảo vệ an ninh mạng.

Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh mạng, bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia với nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quyền con người, quyền công dân, tạo điều kiện cho cơ quan, tổ chức, cá nhân hoạt động trên không gian mạng.

Chủ động phòng ngừa, phát hiện, ngăn chặn, đấu tranh, làm thất bại mọi hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; sẵn sàng ngăn chặn các nguy cơ đe dọa an ninh mạng.

Triển khai hoạt động bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; áp dụng các biện pháp bảo vệ hệ thống thông tin quan trọng về an ninh quốc gia.

Hệ thống thông tin quan trọng về an ninh quốc gia được thẩm định, chứng nhận đủ điều kiện về an ninh mạng trước khi đưa vào vận hành, sử dụng; thường xuyên kiểm tra, giám sát về an ninh mạng trong quá trình sử dụng và kịp thời ứng phó, khắc phục sự cố an ninh mạng.

Mọi hành vi vi phạm pháp luật về an ninh mạng phải được xử lý kịp thời, nghiêm minh. (Điều 4 Luật an ninh mạng)

2.4. Các mối đe dọa đối với an ninh mạng và an ninh thông tin trong trường học

Vấn đề an toàn và an ninh trở thành mối quan tâm chính của trường đại học hiện nay. Sự gia tăng nhanh chóng của việc triển khai công nghệ khiến bảo mật an ninh mạng đã trở nên cần thiết trong nỗ lực điều chỉnh các biện pháp bảo vệ, dù trực tiếp hay gián tiếp, nhằm ngăn chặn hệ thống khỏi các cuộc tấn công vào môi trường mạng. Tuy nhiên, ngay cả khi hệ thống mạng có cài đặt phần mềm chống virus và tường lửa cũng khó ngăn chặn hacker đánh cắp, giả mạo, phá hoại và các hình thức tấn công khác vào dữ

liệu, thông tin của máy chủ. Ngoài ra, nhân viên, giảng viên và học viên có thể vô tình truy cập các trang web không an toàn, vô tình tải xuống các tài liệu không thể xác định được nguồn gốc. Các trang web và tài liệu đó không thể xác định được tin tặc đã có tải virus lên hay chưa, khiến toàn bộ mạng của trường gặp rủi ro.

Có 2 lý do chính khiến hacker thích tấn công mạng trường học:

Thứ nhất, nguồn thông tin, dữ liệu trong trường rất lớn và có giá trị tương đối cao. Vì lý do này, một số tin tặc lợi dụng sơ hở trong mạng trường để đánh cắp thông tin, dữ liệu bất hợp pháp và phá hoại chúng.

Thứ hai, các biện pháp bảo vệ của các trường đại học tương đối chậm và chưa phát triển đồng bộ. Kiến trúc mạng và chế độ người dùng về cơ bản được áp dụng giống nhau, điều này làm cho tội phạm mạng có thể xâm nhập vào những người dùng khác nhau của mạng trường theo cách tương tự.

Ngoài ra còn có rất nhiều phần mềm hỗ trợ hacker Internet như công cụ truy cập từ xa, công cụ tấn công trang web, công cụ quét cổng, công cụ tràn, công cụ rình mò mạng và công cụ chuyển hướng cổng. Một số công cụ này rất dễ sử dụng và có tính hủy diệt cao. Chỉ cần những người có một chút kiến thức về Internet cơ bản là có thể sử dụng được chúng. Điều này cũng khiến một số học sinh vì tò mò nên đã sử dụng các phần mềm hacker này để tấn công vào hệ thống mạng và ứng dụng của trường. Trên thực tế, vào năm 2021, vụ việc hacker bán 300.000 thông tin cá nhân của sinh viên đại học ở Việt Nam đã được ghi nhận. Ngoài các thông tin về học sinh như tuổi, tên, địa chỉ, số điện thoại, file dữ liệu còn chứa nhiều thông tin khác nhau như tài khoản ngân hàng, CMND phụ huynh, địa chỉ liên kết bị mất... Vì vậy, có thể thấy mạng lưới của trường học có nguy cơ bị hacker tấn công bất cứ lúc nào.

3. Phương pháp nghiên cứu:

Về lý thuyết: Nghiên cứu những đặc điểm của cổng/trang thông tin điện tử của trường, các lỗ hổng và các hình thức tấn công nhằm vào cổng/trang thông tin điện tử đó. Sau đó tìm hiểu, nghiên cứu và áp dụng các giải pháp để phòng chống tấn công các lỗ hổng, cũng như ngăn chặn các hình thức tấn công trên cổng/trang thông tin điện tử trường. Các giải pháp được nghiên cứu, tổng hợp từ nhiều nguồn khác nhau tùy vào mỗi loại lỗ hổng và mỗi hình thức tấn công mà có những giải pháp riêng. Từ đó, tổng hợp đưa ra những giải pháp tổng thể giúp đảm bảo an ninh an toàn cho hệ thống cổng/trang thông tin điện tử của trường.

Về mặt thực nghiệm: Từ những giải pháp đã nghiên cứu, chúng tôi lựa chọn mô hình và triển khai thử nghiệm một số biện pháp cơ bản, quan trọng nhằm đánh giá một cách khách quan các giải pháp. Sử dụng phương pháp điều tra xã hội học, thông qua bảng hỏi Google Form cho đối tượng là học viên hệ đào tạo chính quy hai trung đội Khóa D31. Sau khi có kết quả điều tra xã hội học, tác giả tiến hành sử dụng phương

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

pháp phân tích, tổng hợp để từ các số liệu thu thập của học viên hai trung đội sau đó tiến hành phân tích, tổng hợp thành các quan điểm, đưa ra nhận xét, đánh giá về vấn đề nhận thức về an toàn thông tin và giải pháp về bảo vệ an toàn thông tin. Cùng với đó, thực hiện phương pháp thống kê, so sánh sau đó dựa trên cơ sở số liệu đã thu thập tiến hành hành phân loại, phân tích số liệu, tổng hợp, vẽ sơ đồ, đồ thị nhằm so sánh, đối chiếu thống kê số liệu về thực trạng nhận thức, thái độ và trách nhiệm về tình hình an ninh trên không gian mạng, cũng như các giải pháp cho vấn đề đó của học viên trường Đại học An ninh nhân dân. Qua đó, phản ánh bức tranh tổng thể về kết quả đạt được, hạn chế, khó khăn trong công tác này. Đồng thời, đưa ra các khuyến nghị giúp đảm bảo an ninh an toàn cho các công/trang thông tin điện tử.

4. Kết quả nghiên cứu và thảo luận:

4.1. Kết quả nghiên cứu:

4.1.1. Bảng

Số học viên được chọn tham gia khảo sát như sau: Chọn 2 lớp khóa D31 trường Đại học An ninh nhân dân.

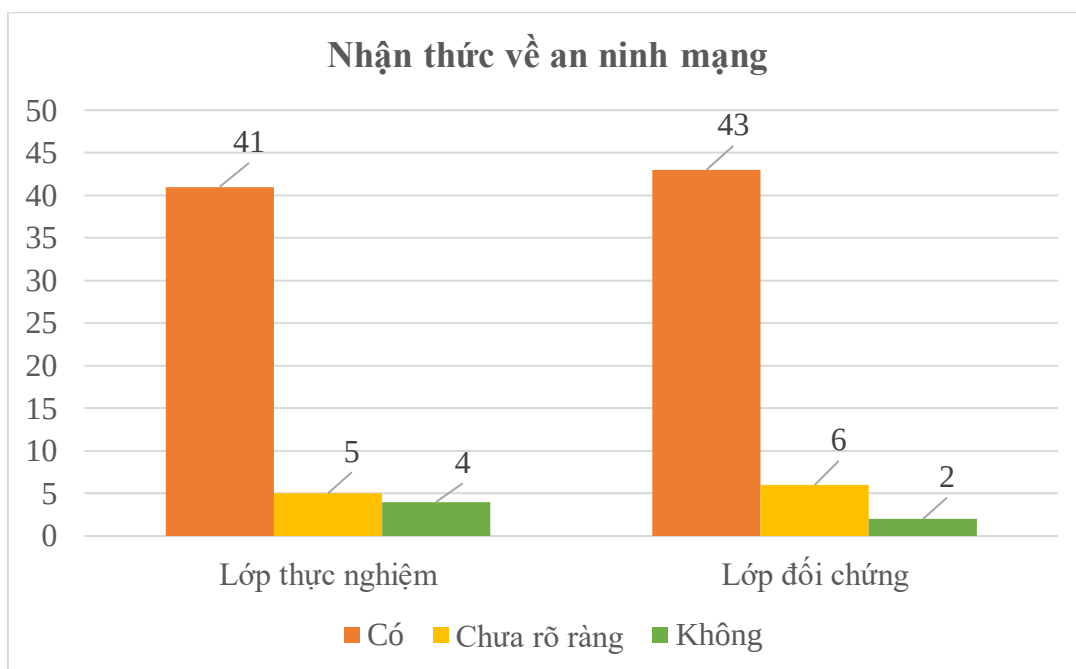
Bảng 1

Số liệu học viên tham gia khảo sát

STT	Nội dung khảo sát	Số học viên lớp thực nghiệm	Số học viên lớp đối chiếu
1	Nhận thức về an ninh mạng	50	51
2	Nhận thức về sự nguy hiểm của an ninh mạng	50	51
3	Nhận thức được những quy định trong Luật An ninh mạng 2018	50	51
4	Kỹ năng xử lý khi bị tin tặc tấn công	50	51
5	Thái độ, trách nhiệm của học viên trường Đại học An ninh nhân dân về vấn đề đảm bảo bí mật thông tin trên không gian mạng	50	51

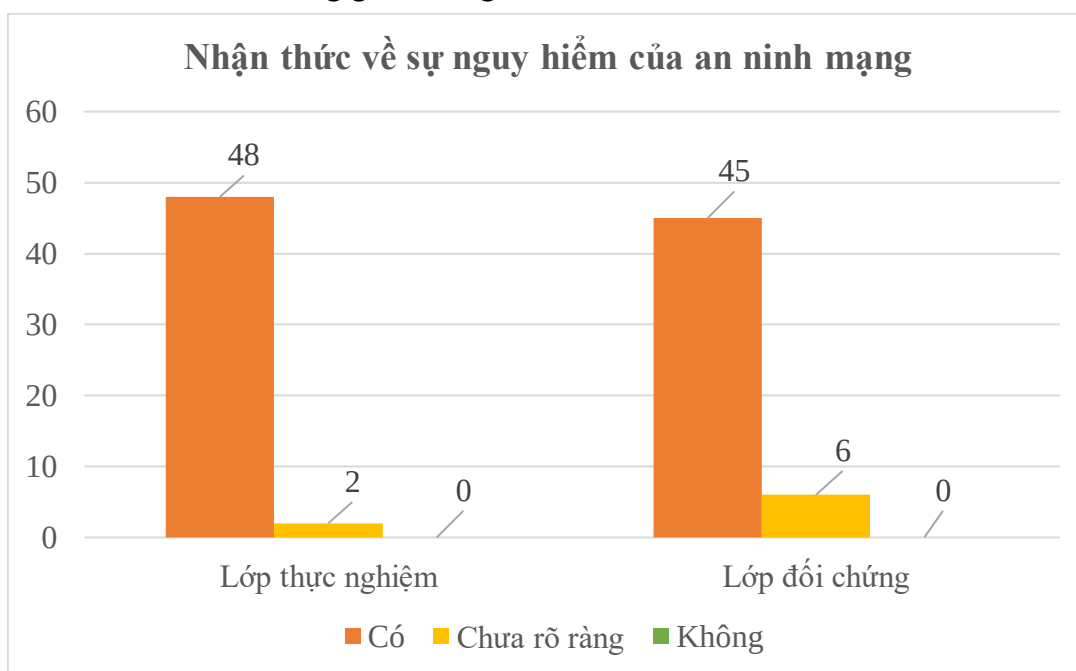
4.1.2. Hình

Qua đồ thị biểu diễn nhận thức về an ninh mạng, ta thấy sự chênh lệch giữa lớp đối chứng và lớp thực nghiệm là không đáng kể. Số học viên có trình độ nhận thức về an ninh mạng, an toàn thông tin là khá cao, đáp ứng nhu cầu thực tiễn của ngành. Tuy nhiên vẫn còn một số ít bộ phận học viên chưa có nhận thức đúng về an ninh mạng.



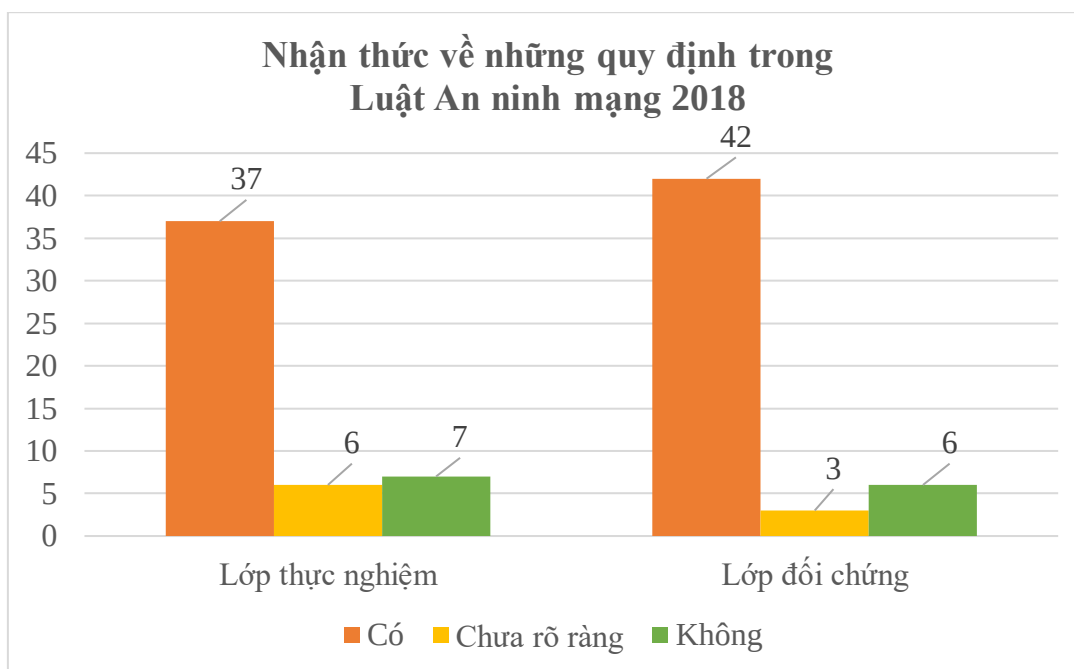
Hình 1: Khảo sát nhận thức về an ninh mạng

Qua đồ thị biểu diễn nhận thức về sự nguy hiểm của an ninh mạng, ta thấy trình độ nhận thức của hai lớp không khác biệt quá lớn. Vì đã được trang bị kiến thức thực tiễn về ngành nên đa số các học viên đều có nhận thức đúng đắn về sự nguy hiểm khi mất an toàn an ninh trên không gian mạng.



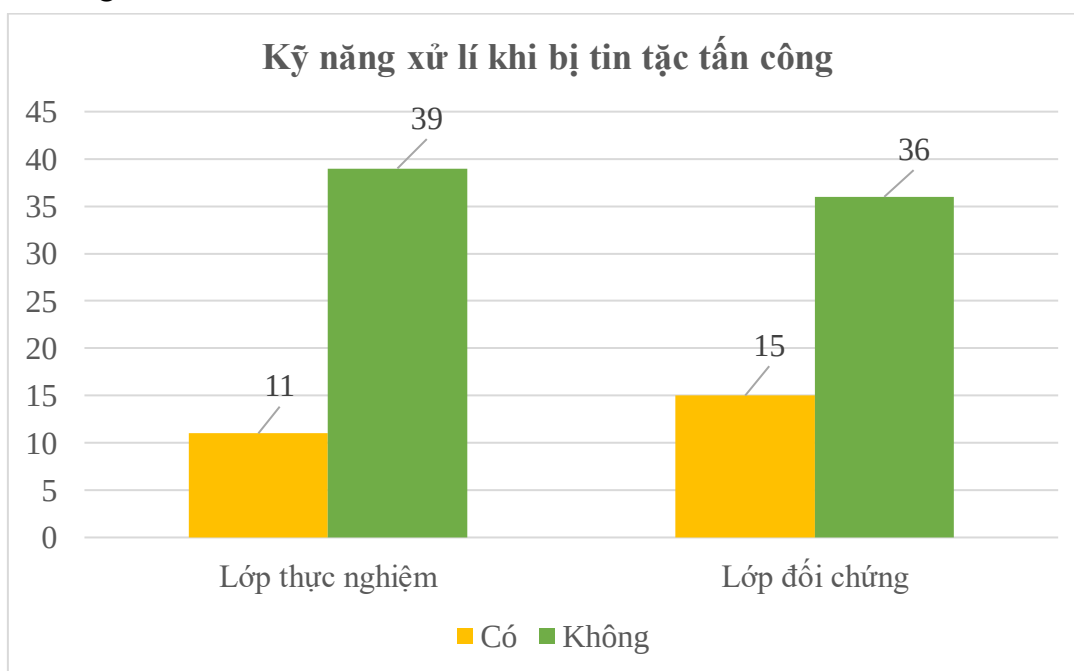
Hình 2: Khảo sát nhận thức về sự nguy hiểm của an ninh mạng

Nhận xét về nhận thức của học viên đối với những quy định trong Luật An ninh mạng 2018 đối với học viên hai lớp đối chứng và thực nghiệm ta thấy trình độ của hai lớp không có sự chênh lệch quá lớn. Tuy nhiên ta nhận thấy vẫn còn một vài học viên vẫn chưa nắm vững về các quy định có trong điều Luật do chưa thật sự nghiêm túc.



Hình 3: Khảo sát nhận thức về những quy định trong Luật An ninh mạng 2018

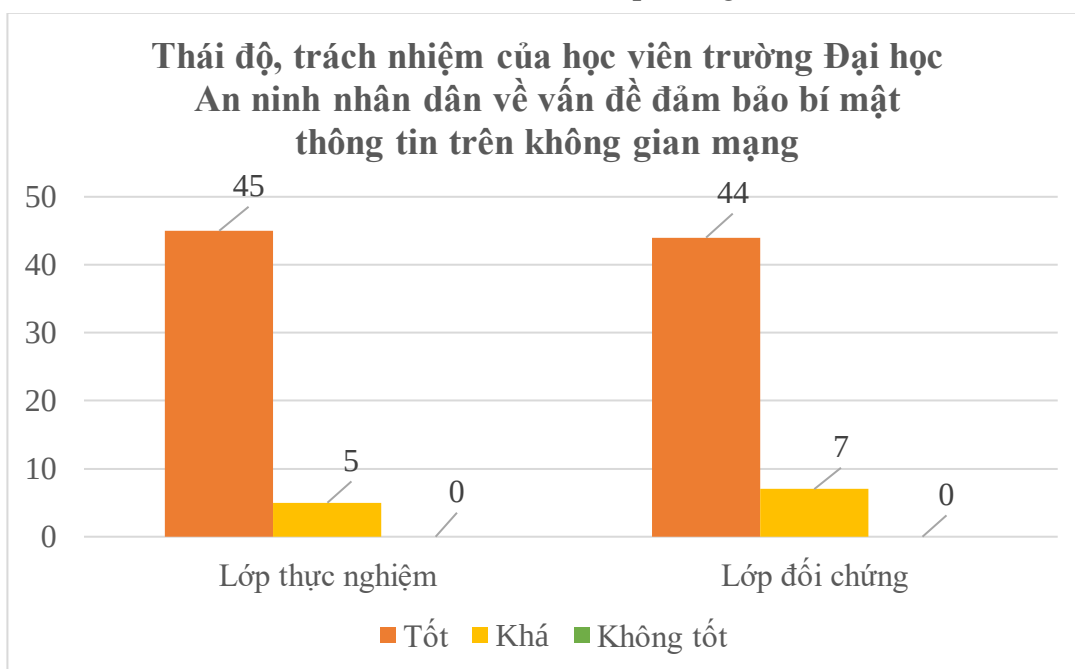
Đa số học viên hai lớp đối chứng và thực nghiệm chưa được trang bị kiến thức và kỹ năng xử lý thông tin khi bị tin tặc tấn công. Qua số liệu ta thấy, có từ 70% - 80% học viên không thể tự bảo vệ được thông tin cá nhân. Đây là một con số đáng ngại và đáng báo động.



Hình 4: Khảo sát kỹ năng xử lý khi bị tin tặc tấn công

Đồ thị biểu diễn thái độ, trách nhiệm của học viên trường Đại học An ninh nhân dân về vấn đề đảm bảo bí mật thông tin trên không gian mạng ở hai lớp đối chứng và thực nghiệm cho thấy chênh lệch không nhiều lắm. Tỷ lệ học viên đạt nhận thức ở mức tốt chiếm khá cao, bình quân chiếm tỷ lệ 90% ở lớp thực nghiệm. Các học viên đều tự nhận thức được năng lực, thái độ, trách nhiệm của bản thân đối với bảo mật thông tin

trên không gian mạng. Số còn lại đạt mức khá và không tốt cần phải nhận thức lại thái độ, trách nhiệm của mình tránh để bị tin tặc đánh cắp thông tin, dữ liệu.



Hình 5: Khảo sát thái độ, trách nhiệm của học viên trường Đại học An ninh nhân dân về vấn đề đảm bảo bí mật thông tin trên không gian mạng

4.2. Thảo luận:

Qua các phương pháp khảo sát, ta thấy rằng hầu hết học viên trường Đại học An ninh nhân dân được trang bị khá đầy đủ kiến thức về an toàn thông tin, an ninh mạng. Học viên của trường có sự nhạy bén về vấn đề mất an toàn mạng, an toàn thông tin trên không gian mạng. Và vì thế có sự quan tâm, phòng ngừa trước mọi nguy cơ, mọi khả năng mà tin tặc có thể tấn công gây mất an toàn, an ninh mạng, đặc biệt là nguy cơ để lộ bí mật của ngành, bí mật của Nhà nước.

Thực tiễn khảo sát cho chúng ta thấy được một thực trạng đáng lo ngại, nếu như bị tin tặc tấn công thì đa số các học viên dù hiểu được sự nguy hiểm của việc mất, lộ thông tin nhưng họ lại rất thiếu kỹ năng trong việc xử lý và phòng chống các loại tội phạm đó và đặc biệt vẫn còn một số ít học viên chưa có nhận thức tốt về an toàn thông tin và an ninh trên không gian mạng. Đó là lí do vì sao nhóm tác giả đề xuất tăng cường phổ cập kiến thức về an toàn thông tin và an ninh trên không gian mạng cho tất cả các lớp học, mở các buổi tuyên truyền và các buổi sinh hoạt về vấn đề an ninh trên không gian mạng.

So với các đề tài trước đây, tác giả thấy đề tài của mình vẫn còn mới và non trẻ nhưng vẫn tạo được sự khác biệt, toàn diện, và có những điểm bám sát vào tình hình thực tế của học viên tại trường Đại học An ninh nhân dân.

5. Kết luận và gợi ý:

5.1. Kết luận:

Trong thời đại thông tin, an ninh mạng và an toàn thông tin An ninh mạng đã và đang đi vào mọi ngóc ngách của đời sống xã hội và dần trở thành một phần quan trọng của mỗi tổ chức, cá nhân. Trong quá trình quản lý mạng trong khuôn viên trường, cần phải xây dựng một hệ thống an toàn và an ninh mạng ổn định trong khuôn viên trường. Cần tiến hành giám sát, phân tích theo thời gian thực các hoạt động mạng trên môi trường mạng, phát hiện kịp thời các hoạt động mạng bất thường, đồng thời liên tục cập nhật, phát triển các giải pháp an ninh mạng mới về chiến lược, công nghệ quản lý và từng bước hoàn thiện hệ thống an ninh mạng của trường học.

Xây dựng kế hoạch quy hoạch và nâng cao trình độ kỹ thuật của đội ngũ quản lý mạng, nâng cao nhận thức về bảo mật của người dùng mạng trong các trường đại học, đồng thời ngăn chặn và giảm thiểu tối đa mọi hành vi truy cập, vận hành và sử dụng bất hợp pháp thông qua các phương tiện kỹ thuật và phương pháp quản lý mạng, giảm thiểu tối đa sự mất an toàn ở mức tối thiểu giúp xây dựng và phát triển thông tin công nghệ ở các trường Đại học An ninh nhân dân.

5.2. Gợi ý

Để đảm bảo an ninh mạng và an ninh thông tin tại trường Đại học An ninh nhân dân, tác giả đề xuất một số biện pháp như sau:

5.2.1. Xây dựng chính sách bảo mật thông tin toàn diện

Nhiều trường đại học tin rằng việc đảm bảo an ninh thông tin thuộc về đội ngũ kỹ thuật nhà trường. Trên thực tế, đây phải là sự kết hợp giữa đội ngũ kỹ thuật và nhà trường. Nhà trường cần xây dựng kế hoạch và giải pháp an ninh hệ thống mạng để ứng phó khi xảy ra sự cố khẩn cấp. Khi có phương án xảy ra sự cố khẩn cấp với hệ thống mạng, nhà trường sẽ chủ động ngăn chặn, giảm thiểu thiệt hại cho hệ thống của mình. Một giải pháp an ninh mạng toàn diện, phù hợp với từng loại hình tổ chức là sự lựa chọn tối ưu vừa tiết kiệm chi phí vận hành vừa đảm bảo an ninh tối đa.

5.2.2. Nâng cao trình độ kỹ thuật về an toàn, bảo mật mạng của đội ngũ kỹ thuật viên

Với việc nâng cấp các vấn đề an ninh mạng, khó tránh khỏi sự tồn tại của các lỗ hổng bảo mật. Công nghệ quản lý mạng nhìn chung còn thấp, hacker có thể xâm nhập và tấn công mạng trường khá dễ dàng.

Cùng với việc tăng cường, nâng cấp mạng và an toàn thông tin trong trường, cần nâng cao trình độ kỹ thuật của kỹ thuật viên trong trường thông qua trao đổi kỹ thuật giữa trường và các cơ quan, tổ chức, an ninh chuyên về hệ thống an ninh mạng và công nghệ cao.

5.2.3. Nâng cao nhận thức về an toàn thông tin cho cán bộ, giảng viên và học viên trong nhà trường

Việc triển khai các phương tiện kỹ thuật và xây dựng hệ thống tiêu chuẩn là biện pháp cơ bản nhất để đảm bảo an toàn thông tin nội bộ của trường. Làm thế nào để triển khai các hệ thống an ninh hiệu quả trong hệ thống an ninh và liên tục nâng cao nhận thức về an toàn mạng cho tất cả cán bộ, giảng viên và học viên là điều quan trọng. Vì vậy, tầm quan trọng của quản lý mạng lưới trường là quản lý con người.

Mặt khác, nhân viên kỹ thuật mạng cần nâng cao nhận thức về bảo mật trên ứng dụng của người dùng mạng trong khuôn viên trường. Đặc biệt, chúng ta cần hình thành thói quen sử dụng mạng xã hội thông minh và nâng cao nhận thức về an ninh mạng như thay đổi mật khẩu thường xuyên, đặt mật khẩu không quá đơn giản (như 123456, 123456@oke,...), không truy cập các trang web độc hại, trang web không an toàn, không tùy ý tải xuống và cài đặt phần mềm không xác định, không tiết lộ thông tin riêng tư cá nhân, ... Ngoài ra, cần nhắc nhở mọi người bảo vệ dữ liệu và thông tin quan trọng trong máy tính hoặc thiết bị điện tử cá nhân thật tốt, nếu không, một khi gặp phải tình trạng tấn công từ tin tặc thì dữ liệu trong thiết bị sẽ đánh cắp và dẫn đến hậu quả không thể tưởng tượng được.

5.2.4. Xây dựng các giải pháp tăng cường an ninh mạng và an ninh thông tin cơ sở dữ liệu

Qua phần giới thiệu trước, tác giả nhận thấy cần xây dựng các biện pháp an ninh mạng và an toàn thông tin để tăng cường an ninh mạng và an toàn thông tin cơ sở dữ liệu trong trường. Tuy nhiên, việc phát triển các biện pháp phòng ngừa cần kết hợp với các công nghệ an ninh mạng hiện nay. Hiện nay, công nghệ an ninh mạng nói chung chủ yếu bao gồm công nghệ số hóa hạ tầng mạng, công nghệ kiểm soát truy cập, công nghệ phát hiện xâm nhập, công nghệ trí tuệ nhân tạo, công nghệ tường lửa.

Công nghệ số hóa hạ tầng mạng: Hạ tầng công nghệ số hóa là mô phỏng hạ tầng mạng vật lý hoàn chỉnh dựa trên phần mềm. Cơ sở hạ tầng mạng số hóa cung cấp các tính năng và đảm bảo giống như mạng vật lý. Chúng cung cấp các lợi ích hoạt động và độc lập với phần cứng của số hóa - phân bổ tài nguyên nhanh, triển khai liên tục, bảo trì tự động và hỗ trợ cho cả ứng dụng hiện có và ứng dụng mới. Công nghệ số hóa giới thiệu các thiết bị, cơ sở hạ tầng mạng và logic dịch vụ cơ sở hạ tầng mạng - cổng, bộ chuyển mạch, bộ định tuyến, tường lửa, bộ cân bằng tải, VPN và nhiều thứ khác để kết nối các khối hoạt động. Các ứng dụng chạy trên cơ sở hạ tầng mạng số hóa cũng tương tự như chạy trên cơ sở hạ tầng mạng vật lý. Người dùng có thể tạo cơ sở hạ tầng mạng có khả năng mở rộng cao, mang lại mức độ hoạt động hiệu quả hơn, linh hoạt hơn, phân bổ tài nguyên nhanh hơn, xử lý sự cố và nhân bản, quá trình giám sát, QoS (Quality of Service) và bảo mật, tất cả đều được hỗ trợ bởi phần mềm số hóa cơ sở hạ tầng mạng.

Công nghệ kiểm soát truy cập: Mục đích chính của công nghệ kiểm soát truy cập là ngăn chặn truy cập trái phép vào bất kỳ tài nguyên nào và đảm bảo rằng việc vận hành

và sử dụng hệ thống máy tính bên ngoài nằm trong phạm vi pháp lý. Công nghệ kiểm soát truy cập thông qua cơ chế ủy quyền mạng, thông qua các ủy quyền khác nhau cho những người dùng mạng khác nhau trong khuôn viên trường, để hạn chế hoặc cấm người dùng trái phép truy cập.

Công nghệ phát hiện xâm nhập: Công nghệ phát hiện xâm nhập phân tích các hành động, nhật ký bảo mật, kiểm tra dữ liệu hoặc thông tin khác có sẵn trên mạng để cố gắng hiểu ý định và mục đích xâm nhập của tin tặc. Công nghệ phát hiện xâm nhập là một loại công nghệ được thiết kế và cấu hình để đảm bảo an ninh cho máy tính hệ thống, có thể phát hiện và báo cáo kịp thời các hiện tượng trái phép hoặc bất thường trong hệ thống. Nó là một công nghệ được sử dụng để phát hiện các hành vi vi phạm chính sách bảo mật trong mạng máy tính. Thông qua công nghệ này, nó có thể phát hiện ra ý định tấn công của kẻ tấn công và phương thức tấn công kịp thời cũng như các biện pháp tương ứng để ngăn chặn các dấu hiệu của một chương trình độc hại. Mặc dù nó không phải là toàn năng và không thể xác định được tất cả các mối đe dọa nhưng nó là một công cụ thiết yếu giúp giảm lượng thời gian mà các chuyên gia công nghệ thông tin cần để điều tra các cảnh báo.

Công nghệ tường lửa: Tường lửa là một loại biện pháp kỹ thuật nhằm bảo vệ an ninh mạng máy tính. Nó có thể được sử dụng như một rào cản giữa mạng nội bộ của trường và an ninh mạng bên ngoài, để ngăn chặn sự xâm nhập của thế giới bên ngoài. Nó có thể quản lý quyền truy cập của người dùng vào mạng trong khuôn viên trường. Mặt khác, nó có thể quét các gói dữ liệu đi vào mạng trong khuôn viên trường nên có thể ngăn chặn một cách hiệu quả cuộc tấn công và sự xâm nhập của vi rút.

LỜI CẢM ƠN

Trong quá trình thực hiện nghiên cứu, tác giả đã gặp không ít khó khăn và thách thức. Nhưng nhờ có sự giúp đỡ và hướng dẫn tận tình của cố vấn, tác giả đã có thể định hướng và hoàn thành đúng hạn bài tham luận này. Trước hết, tác giả xin gửi lời cảm ơn chân thành và sâu sắc đến cố vấn của mình, người đã luôn dành thời gian và tâm huyết để hỗ trợ tác giả trong suốt quá trình nghiên cứu.

Ngoài ra, tác giả cũng muốn gửi lời cảm ơn đến các đồng chí trong tiểu đội, những người đã giúp đỡ và hỗ trợ tác giả trong quá trình tìm kiếm nguồn tài liệu, số liệu cần thiết để hoàn thành tốt bài nghiên cứu này. Sự đóng góp của các đồng chí không chỉ giúp cho tác giả hoàn thành tốt nghiên cứu mà còn giúp cho tác giả trang bị được thêm nhiều kiến thức và kỹ năng quý báu.

Tuy nhiên, nhận thức của tác giả về chủ đề nghiên cứu vẫn còn hạn chế và nghiên cứu cũng có thể chưa hoàn toàn đầy đủ và chính xác. Tác giả nhận thức được điều đó và mong muốn nhận được sự đóng góp, góp ý tận tình đến từ quý thầy cô có kinh nghiệm trong lĩnh vực này, để tác giả có thể rút kinh nghiệm và cải tiến công trình của mình.

Với tinh thần cầu tiến, mong muốn tiến bộ, tác giả tin rằng những đóng góp và góp ý của quý thầy cô sẽ giúp cho tác giả trang bị thêm nhiều kiến thức và kỹ năng quý báu, cũng như hoàn thiện và nâng cao chất lượng bài nghiên cứu của mình.

Một lần nữa, tác giả xin chân thành cảm ơn tất cả những người đã giúp đỡ và hỗ trợ tác giả trong quá trình hoàn thành bài nghiên cứu.

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. Luật an ninh mạng số 24/2018/QH14 ngày 12/06/2018 của Quốc hội nước CHXHCN Việt Nam.
2. Bộ công an (2011), An toàn thông tin và công tác phòng chống tội phạm sử dụng công nghệ cao, Nhà xuất bản Công an nhân dân, Hà Nội. Tr. 258-266, 286-716.
3. Nguyễn Ngọc Cường (2012), Tin học ứng dụng trong điều tra tội phạm, Nhà xuất bản Công an nhân dân, Hà Nội. Tr.181-186, 302-315.
4. Chính Phủ (2013), Nghị định 72/2013/NĐ-CP của chính phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng, Hà Nội.
5. Bộ Thông tin và Truyền thông (2011), hướng dẫn đảm bảo an toàn thông tin cho các cổng/trang thôn tin điện tử, Hà Nội.
6. Chính Phủ (2007), Nghị định 64/2007/NĐ-CP của Chính phủ về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, Hà Nội.

Tiếng Anh

1. “Definition of computer security”. Encyclopedia. Ziff Davis, PCMag.
2. Rouse, Margaret. “Social engineering definition”. TechTarget.
3. "Reliance spells end of road for ICT amateurs", The Australian.
4. Narayana, I.N.C.S., Gopinath, G., Mogan, K.P.C. et al. (2014), "A multilevel thrust filtration defending mechanism against DDoS attacks in cloud computing environment", *International Journal of Grid and Utility Computing*, Vol. 5, No. 4, pp.236-248.
5. Naser, S., Kamil, S. and Thomas, N. (2015), "A case study in inspecting the cost of security in cloud computing", *Electronic Notes in Theoretical Computer Science*, Vol. 318, No. 11, pp. 179-196.
6. Stuttard D, PintoM (2012), *The web application hacker's handbook*, 2nd Ed, ISBN-13: 978-1118026472, ISBN-10: 1118026470.
7. Thomson, G. (2012), "BYOD: Enabling the chaos", *Network Security*, 2012(2), pp.5-8, DOI:10.1016/S1353-4858(12)70013-2.
8. Vance, A., Siponen, M., & Pahlila, S. (2012), "Motivating IS security compliance: Insights from habit and protection motivation theory", *Information & Management*, 49(3-4), 190-198, DOI:10.1016/j.im.2012.04.002.

9. William Stalling, Lawrie Brown (2012), Computer Security Principles and Practice Second Edition, University of New South Wales, Australian Defence Force Academy.
10. Gasser, Morrie (1988). Building a Secure Computer System (PDF). Van Nostrand Reinhold. tr. 3. ISBN 0-442-23022-2.

**GIẢI PHÁP GÓP PHẦN BẢO ĐẢM AN NINH CON NGƯỜI
TRƯỚC VẤN ĐỀ LỘ LỘT DỮ LIỆU CÁ NHÂN
TRONG THỜI KÌ CHUYỂN ĐỔI SỐ
SOLUTIONS CONTRIBUTING TO ENSURE HUMAN
SECURITY BEFORE THE PROBLEM OF PERSONAL DATA
EXPOSURE DURING THE PERIOD OF
DIGITAL TRANSFORMATION**

Nguyễn Nhựt Phi*, Nguyễn Hoàng Trí, Nguyễn Thanh Tuấn

Trường Đại học An ninh nhân dân

*Tác giả liên hệ: [nguyennhutphi512002@gmail.com]

THÔNG TIN	TÓM TẮT
Từ khóa: an ninh con người, bảo đảm, dữ liệu cá nhân, lộ lọt, chuyển đổi số	Bài viết góp phần làm rõ những tác động, ảnh hưởng của vấn đề lộ lọt dữ liệu cá nhân trong thời kỳ chuyển đổi số đến an ninh con người; công tác ngăn ngừa lộ lọt dữ liệu cá nhân bảo đảm an ninh con người; dự báo và đề xuất giải pháp góp phần bảo đảm an ninh con người trước vấn đề lộ lọt dữ liệu cá nhân trong thời kỳ chuyển đổi số thông qua phương pháp nghiên cứu tài liệu, phương pháp phân tích, tổng hợp, phương pháp dự báo khoa học.
Keywords: human security, assurance, period on human security; prevention of personal data personal data, intrusion, digital transformation	ABSTRACT The article contributes to clarifying the impact of personal data disclosure during the digital transformation human security, assurance, period on human security; prevention of personal data personal data, intrusion, digital transformation leakage to ensure human security; Forecast and propose solutions that contribute to ensuring human security against the problem of personal data leakage in the digital transformation period through research, analysis, synthesis and forecasting methods.

Trong thế giới ngày nay, cuộc sống con người bị đe dọa bởi nhiều yếu tố, như: Chiến tranh, dịch bệnh, thiên tai, nạn đói, biến đổi khí hậu,... Do vậy, an ninh con người luôn là vấn đề quan tâm hàng đầu của các quốc gia trên thế giới, trong đó có Việt Nam. Theo “Báo cáo phát triển con người” năm 1994 của Liên hợp quốc, an ninh con người được đánh giá qua hai tiêu chí: Một là, an toàn không bị đe dọa bởi đói nghèo, bệnh tật, sự áp bức. Hai là, được bảo vệ khi gặp những rủi ro bất thường trong cuộc sống. Hai tiêu chí trên được cụ thể hóa ở bảy lĩnh vực: An ninh kinh tế là việc bảo đảm về việc

làm và thu nhập cơ bản; an ninh lương thực là việc bảo đảm được nhu cầu tối thiểu về lương thực, thực phẩm; an ninh sức khỏe là việc bảo đảm ở mức tối thiểu về phòng - chống dịch bệnh và chăm sóc y tế; an ninh môi trường là việc được bảo vệ trước thiên tai, tai họa do con người gây ra và sự ô nhiễm môi trường sống; an ninh cá nhân là việc được bảo vệ trước những hành vi tội phạm, bạo lực hoặc lạm dụng thể chất do bất kể chủ thể nào gây ra; an ninh cộng đồng là việc được duy trì các mối quan hệ và giá trị truyền thống của cộng đồng; an ninh chính trị là việc tôn trọng các quyền con người cơ bản, nhất là các quyền dân sự, chính trị [1].

Ở Việt Nam, vấn đề an ninh con người và bảo đảm an ninh con người luôn được Đảng, Nhà nước quan tâm, thể hiện trong các văn bản của Đảng. Đặc biệt trong Văn kiện Đại hội Đại biểu toàn quốc lần thứ XIII của Đảng đã đặt nhân tố con người, an ninh con người làm trung tâm của mọi hoạt động, bảo vệ an ninh con người vừa là mục tiêu phấn đấu, vừa là động lực bảo đảm cho sự ổn định chính trị xã hội và xây dựng, phát triển đất nước trường tồn, thịnh vượng, “Chú trọng an ninh, an toàn là một trong những yếu tố hàng đầu trong cuộc sống của người dân” [2]; “Thực hiện tốt chính sách xã hội, bảo đảm an ninh xã hội, an ninh con người, tạo chuyển biến mạnh mẽ trong quản lý phát triển xã hội, thực hiện tiến bộ, công bằng xã hội, nâng cao chất lượng cuộc sống và chỉ số hạnh phúc của con người Việt Nam” [2].

Trên thế giới, chuyển đổi số bắt đầu được nhắc đến nhiều vào khoảng năm 2015, phổ biến từ năm 2017. Ở Việt Nam, chuyển đổi số bắt đầu được đề cập nhiều vào khoảng năm 2018. Chuyển đổi số là quá trình thay đổi tổng thể và toàn diện của cá nhân, tổ chức về cách sống, cách làm việc và phương thức sản xuất dựa trên các công nghệ số. Trong thời đại chuyển đổi số hiện nay, dữ liệu cá nhân trên không gian mạng trở thành một kho lưu trữ khổng lồ mà nếu các cá nhân, tổ chức không có biện pháp bảo vệ tương xứng, đúng cách thì sẽ tạo điều kiện thuận lợi để tội phạm lợi dụng thực hiện các hành vi vi phạm pháp luật, tác động tiêu cực đến an ninh con người.

Theo khoản 1 Điều 2 Nghị định 13/2023/NĐ-CP ngày 17/4/2023 quy định về bảo vệ dữ liệu cá nhân thì dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. Cụ thể:

Dữ liệu cá nhân cơ bản bao gồm: Họ, chữ đệm và tên khai sinh, tên gọi khác (nếu có); ngày, tháng, năm sinh; ngày, tháng, năm chết hoặc mất tích; giới tính; nơi sinh, nơi đăng ký khai sinh, nơi thường trú, nơi tạm trú, nơi ở hiện tại, quê quán, địa chỉ liên hệ; quốc tịch. Hình ảnh của cá nhân; số điện thoại, số chứng minh nhân dân, số định danh cá nhân, số hộ chiếu, số giấy phép lái xe, số biển số xe, số mã số thuế cá nhân, số bảo hiểm xã hội, số thẻ bảo hiểm y tế. Tình trạng hôn nhân; thông tin về mối quan hệ gia

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

đình (cha mẹ, con cái); thông tin về tài khoản số của cá nhân; dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng... (Xem hình 1).

Dữ liệu cá nhân nhạy cảm là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân. Bao gồm quan điểm chính trị, quan điểm tôn giáo; tình trạng sức khỏe và đời tư được ghi trong hồ sơ bệnh án, không bao gồm thông tin về nhóm máu. Thông tin liên quan đến nguồn gốc chủng tộc, nguồn gốc dân tộc; thông tin về đặc điểm di truyền được thừa hưởng hoặc có được của cá nhân; thông tin về thuộc tính vật lý, đặc điểm sinh học riêng của cá nhân; thông tin về đời sống tình dục, xu hướng tình dục của cá nhân... Dữ liệu về tội phạm; thông tin khách hàng của tổ chức tín dụng, chi nhánh ngân hàng nước ngoài... (Xem hình 1).



Hình 1. Dữ liệu cá nhân

Hiến pháp năm 2013 đã khẳng định quyền riêng tư của cá nhân là bất khả xâm phạm, đồng thời phát triển mở rộng phạm vi quyền riêng tư không chỉ là quyền bất khả xâm phạm về thân thể, nhà ở, thư tín mà còn bao gồm quyền bảo vệ bí mật cá nhân, trong đó có thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình (Điều 21). Mặc dù, hệ thống pháp luật Việt Nam hiện hành chưa sử dụng cụm từ “dữ liệu cá nhân”, chưa có nhiều định nghĩa về “dữ liệu cá nhân” cũng như bảo vệ dữ liệu cá nhân, tuy nhiên với các quy định về quyền bí mật đời sống riêng tư, bí mật cá nhân cùng các quy định liên quan tới “thông tin cá nhân”, “thông tin riêng”, “thông tin số”; “thông tin cá nhân trên môi trường mạng”; “thông tin bí mật đời tư”... trong các văn bản hiện hành, Nghị định được xây dựng tiếp cận theo hướng “dữ liệu cá nhân” và “bảo vệ dữ liệu cá nhân” là vấn đề có liên quan tới quyền riêng tư, được pháp luật bảo vệ, phù hợp với tinh thần của Hiến pháp. Công dân Việt Nam có quyền bất khả xâm phạm, quyền giữ bí mật về dữ liệu cá nhân. Dữ liệu cá nhân được pháp luật Việt Nam bảo vệ, các hành vi xâm phạm dữ liệu cá nhân được xử lý nghiêm minh theo quy định pháp luật.

Những biến động trong an ninh quốc tế hiện nay đang ngày càng làm rõ ràng hơn phạm trù an ninh con người; các yếu tố thay đổi có ảnh hưởng sâu sắc và tác động đến an ninh con người. Theo đó, kỹ thuật số được xếp như một trong những vấn đề được quan tâm nhất mà hệ quả chính của nó là quá trình chuyển đổi số. Chuyển đổi số không chỉ mang lại cơ hội mà còn đặt ra những thách thức cho sự phát triển an ninh con người tại Việt Nam. Theo thống kê của Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) - Bộ Công an, Việt Nam hiện là quốc gia có tốc độ phát triển và ứng dụng Internet cao nhất thế giới. Số lượng người sử dụng Internet của Việt Nam đã đạt hơn 77,93 triệu người, tương đương với khoảng 79% dân số. Qua theo dõi, dữ liệu cá nhân của hơn 2/3 dân số nước ta đang được lưu trữ, đăng tải, chia sẻ và thu thập trên không gian mạng với nhiều hình thức và mức độ chi tiết khác nhau. Ở thời điểm hiện tại, tình trạng lộ lọt thông tin người dùng ở Việt Nam đang rất đáng báo động. Hoạt động mua bán dữ liệu cá nhân hiện đang diễn ra phổ biến, công khai, với các dữ liệu thô và dữ liệu cá nhân đã qua xử lý, nhiều hành vi chưa được xử lý vì thiếu quy định của pháp luật. Các doanh nghiệp, công ty kinh doanh dịch vụ có thu thập dữ liệu cá nhân của khách hàng, cho phép các đối tác thứ ba tiếp cận thông tin dữ liệu cá nhân nhưng không có yêu cầu, quy định chặt chẽ, để đối tác thứ ba chuyển giao, buôn bán cho các đối tác khác. Các doanh nghiệp chủ động thu thập thông tin cá nhân của khách hàng, hình thành kho dữ liệu cá nhân, phân tích, xử lý các loại dữ liệu đó để tiến hành kinh doanh, buôn bán. Trên các nền tảng mạng xã hội, cá nhân người dùng vô tình để lộ lọt thông tin vẫn còn phổ biến gây tác hại khôn lường đe dọa đến an ninh con người, như truy cập những clip ngắn, bài viết, link chứa mã độc đăng trên TikTok, Youtube, Instagram, Facebook, Google... Hoặc các đối tượng chủ động gọi điện, nhắn tin cho chủ tài khoản thông báo có khoản tiền, quà tặng, khuyến mại... chuyển vào tài khoản; hoặc sử dụng mạng xã hội, email, tin nhắn mạo danh ngân hàng điện tử thông báo tài khoản E-banking của chủ tài khoản bị xâm nhập trái phép và yêu cầu chủ tài khoản cung cấp thông tin đăng nhập, mã OTP. Bên cạnh đó, một số cá nhân thiếu thận trọng, chấp nhận đánh đổi việc cung cấp dữ liệu cá nhân để sử dụng các nền tảng dịch vụ như đã cung cấp số điện thoại, thậm chí địa chỉ nhà, số tài khoản cá nhân, thông tin căn cước công dân,... trên những trang web bán hàng online, các phần mềm chỉnh sửa, chuyển ảnh AI, các tựa game phổ biến,... thậm chí thông tin cá nhân có thể bị lộ lọt từ những ống kính camera đường phố.

Tại Việt Nam, tội phạm sử dụng công nghệ cao là loại tội phạm mới, đang có xu hướng phát triển, diễn biến hết sức phức tạp, đa dạng và khó lường, là mối đe dọa to lớn đối với sự ổn định, phát triển của các quốc gia và được xác định là một trong những nguy cơ, thách thức lớn nhất đối với an ninh con người. Thời gian qua, tình hình tội phạm công nghệ cao diễn ra trên phạm vi cả nước, với nhiều hình thức ngày càng tinh

vi hơn, số lượng vụ bị lừa đảo ngày càng tăng cao, gây hậu quả nghiêm trọng về tài sản và khiến người dân bức xúc, lo lắng. Tội phạm này sử dụng thông tin dữ liệu cá nhân đã được thu thập, xử lý để thực hiện các hành vi phạm tội, điển hình như: Giả danh cơ quan thực thi pháp luật để lừa đảo chiếm đoạt tài sản; truy cập trái phép vào những tài khoản số, chiếm quyền quản trị email tới các thông tin tài khoản ngân hàng; làm giả tín dụng, giả danh nhân viên ngân hàng, nhân viên nhà mạng, nhân viên điện lực và các loại hình khác để lừa đảo chiếm đoạt tài sản. Ngay cả những thông tin như tên của cá nhân, tên trường học, khu nội trú, các loại thẻ... cũng có thể trở thành thông tin hữu ích đối với tội phạm mạng khi người sử dụng đăng tải công khai trên mạng xã hội. Các tội phạm chiếm đoạt sử dụng nhằm mục đích không chế, thậm chí là tống tiền người dùng. Nguy hiểm hơn, những thông tin do chính chủ tự nguyện cung cấp có thể được sử dụng vào mục đích đe dọa tống tiền, bắt cóc hoặc lừa người sử dụng chuyển tiền vào tài khoản của tội phạm. Đáng lo ngại, thông tin cá nhân bị lộ lọt sẽ được các hacker sử dụng cho mục đích phạm tội, khi đã chiếm được những thông tin cá nhân như: chứng minh nhân dân, tài khoản ngân hàng,...các đối tượng dễ dàng chiếm đoạt tiền, mở các tài khoản ngân hàng, thẻ tín dụng để thực hiện hành vi của mình. Nhiều người sử dụng điện thoại thông minh có kết nối Internet nhận được tin nhắn quảng cáo mua bán bất động sản, mời sử dụng dịch vụ chăm sóc sắc đẹp miễn phí, thẩm mỹ viện, quảng cáo về khóa học tiếng Anh khi có con đang trong độ tuổi đi học,... mà họ không hề cung cấp số điện thoại hay thông tin cá nhân cho những người thực hiện cuộc gọi điện thoại đó. Nghiêm trọng hơn, ảnh thật của người dùng được đối tượng sử dụng hay còn gọi là bẫy lừa đảo cuộc gọi Deepfake, đó là việc dùng cuộc gọi video Deepfake để lừa đảo. Deepfake là công nghệ ứng dụng trí tuệ nhân tạo (AI) để tạo ra các đoạn video với hình ảnh khuôn mặt nhân vật giống hệt như hình ảnh người muốn giả mạo, từ đó đối tượng sẽ sử dụng những đoạn video này để đi lừa đảo bạn bè, người thân của người dùng đó, khiến nạn nhân khó mà biết được mình đã bị lừa.

Trên thực tế, nhiều người sử dụng các trang mạng của nước ta vẫn chưa ý thức được tính nghiêm trọng của vấn đề, thậm chí nhiều người khi biết thông tin của mình bị lộ, lọt thì họ cũng cho điều đó là bình thường, nên ít khi tiến hành khiếu nại, tố giác. Các đối tượng thực hiện hành vi xâm phạm đến an ninh con người thông qua dữ liệu cá nhân ngày càng đưa ra các phương thức, thủ đoạn tấn công, lừa đảo, chiếm đoạt tài sản ngày càng tinh vi, xảo quyệt theo xu hướng của công nghệ, đặc biệt là công nghệ trí tuệ nhân tạo (AI) ngày càng phát triển mạnh mẽ.

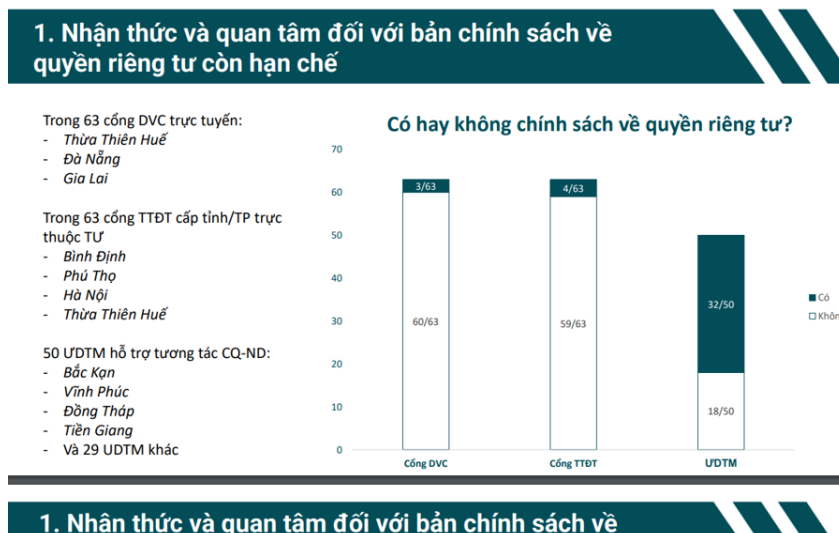
Nguyên nhân dẫn đến tình trạng lộ dữ liệu cá nhân gồm có những nội dung sau:

Một là, nhận thức về công tác bảo vệ dữ liệu cá nhân còn hạn chế

Nhận thức về bảo vệ thông tin cá nhân còn hạn chế, chưa phù hợp với tình hình thực tế, là nguyên nhân chính dẫn tới tình trạng lộ, lọt, chiếm đoạt thông tin cá nhân,

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

buôn bán dữ liệu cá nhân. Nhiều thông tin sinh trắc học, lý lịch cá nhân, mối quan hệ, tình trạng sức khỏe, tài chính được đăng tải công khai, trở thành nguồn dữ liệu để các phần mềm thu thập dữ liệu. Nhận thức của một số cán bộ, công chức, viên chức về cung cấp, quản lý hồ sơ cá nhân, dữ liệu cá nhân chưa đầy đủ, dẫn đến việc chỉ đạo, hướng dẫn, thực hiện nhiệm vụ lưu trữ ở một cơ quan, đơn vị chưa được quan tâm chú trọng đúng mức (Xem hình 2).



Hình 2. Nhận thức và quan tâm đối với chính sách quyền riêng tư

Hai là, quy định của pháp luật về bảo vệ thông tin cá nhân chưa hoàn thiện

Tuy đã được ghi nhận từ lâu, song những quy định pháp luật cụ thể về bảo vệ dữ liệu cá nhân được quy định rải rác trong các văn bản quy phạm pháp luật với mức độ khác nhau và chưa có quy định chi tiết, cụ thể và thiếu tính khả thi trên thực tế. Các văn bản pháp luật hiện hành hiện chưa đưa ra được một khái niệm thống nhất, đầy đủ dẫn đến khó hiểu và khó áp dụng pháp luật về bảo vệ dữ liệu cá nhân. Bên cạnh khái niệm dữ liệu cá nhân, thông tin cá nhân, một số văn bản quy phạm pháp luật còn sử dụng khái niệm thông tin riêng, thông tin bí mật đòi hỏi dẫn tới trùng lặp, khó áp dụng trong thực tiễn. Hệ thống pháp luật nước ta chưa có quy định xử lý việc tiết lộ thông tin cá nhân mà chưa có sự đồng ý của chủ thể, tạo nên lỗ hổng lớn trong thời đại sử dụng dữ liệu cá nhân như một nguyên liệu để phân tích phục vụ lợi ích kinh tế như hiện nay.

Hiện tại, mới chỉ có Luật An toàn thông tin mạng quy định về nguyên tắc bảo vệ thông tin cá nhân nhưng theo hướng cá nhân tự bảo vệ thông tin cá nhân của mình và tuân thủ quy định của pháp luật. Điều này đặt ra vấn đề cần bổ sung thêm các nguyên tắc khác để bảo vệ dữ liệu cá nhân.

Ba là, công tác bảo vệ dữ liệu cá nhân còn gặp nhiều khó khăn

Mặc dù có một số văn bản quy phạm pháp luật (Bộ luật hình sự, Bộ luật dân sự, Luật bảo vệ quyền lợi người tiêu dùng, Luật Công nghệ thông tin...) có đề cập tới khía cạnh bảo vệ dữ liệu cá nhân nhưng chưa đầy đủ và thiếu chế tài đủ mạnh để xử lý vi

phạm. Do đó, các cơ quan chức năng khó xác định và xử lý đúng tính chất, mức độ các hành vi vi phạm bảo vệ dữ liệu cá nhân theo quy định của pháp luật hiện hành.

Bốn là, công tác lưu trữ, bảo quản, xử lý dữ liệu cá nhân bộc lộ nhiều hạn chế trong thời đại học cách mạng khoa học công nghệ

Hiện nay, việc cập nhật, sử dụng dữ liệu cá nhân của các cơ quan, tổ chức nhà nước được thực hiện trên nhiều phương tiện lưu trữ khác nhau. Một số lưu trữ tại nước ngoài (Mỹ, Singapore). Do đó, chưa có quy định về lưu trữ, sử dụng dữ liệu cá nhân của các cơ quan, tổ chức được thuê lưu trữ; chưa có quy trình, trách nhiệm giám sát của các cơ quan chức năng.

Công tác thu thập, bổ sung dữ liệu cá nhân để bảo đảm tính chính xác chưa được quan tâm thực hiện thường xuyên; nguy cơ tài liệu lưu trữ bị hư hỏng, xuống cấp ngày càng cao; một số tài liệu không được bảo vệ, bảo quản, bị mối, mọt, côn trùng phá hoại, không có khả năng phục hồi; đối với dữ liệu điện tử không được cập nhật thường xuyên, chưa quan tâm sao lưu, bảo quản dữ liệu nên dữ liệu không sử dụng được khi cần khai thác.

Các dữ liệu cá nhân được mã hóa, lưu trữ vào cơ sở dữ liệu của các trang web thương mại điện tử nhưng hệ thống dữ liệu của doanh nghiệp không an toàn, bị tin tặc tấn công dẫn tới mất cơ sở dữ liệu.

Năm là, công tác tuyên truyền, phổ biến quy định của pháp luật về bảo vệ dữ liệu cá nhân chưa đáp ứng được yêu cầu, chưa theo kịp sự phát triển của khoa học công nghệ

Cơ quan, tổ chức nhà nước chưa chú trọng đến công tác tuyên truyền, phổ biến, nâng cao ý thức, trách nhiệm về công tác bảo vệ dữ liệu cá nhân. Người dùng chưa được tuyên truyền đúng mức nên phần lớn chưa ý thức được mức độ quan trọng của dữ liệu cá nhân, chưa có những biện pháp để tự bảo vệ thông tin cá nhân. Điều này xuất phát từ nguyên nhân chưa có cơ quan chuyên trách bảo vệ dữ liệu cá nhân, chưa có cơ quan chịu trách nhiệm về công tác tuyên truyền.

Sáu là, công tác đầu tư, kinh phí phục vụ bảo vệ dữ liệu cá nhân còn hạn chế. Công tác an ninh mạng đang thật sự cần thiết đối với nhiều cơ quan, tổ chức và doanh nghiệp, đặc biệt trong giai đoạn nước ta ngày càng hòa nhập sâu vào kinh tế thị trường và gia nhập WTO. Tuy nhiên, hoạt động triển khai thực tế không tương xứng với yêu cầu đặt ra, nhiều cơ quan, doanh nghiệp chưa thật sự coi trọng đến vấn đề này.

Bảy là, chưa khai thác, phát huy hết giá trị của dữ liệu cá nhân trong phát triển Chính phủ điện tử, hành chính công, phục vụ quản lý nhà nước, phát triển kinh tế xã hội

Việc lưu trữ dữ liệu cá nhân tại các cơ quan hành chính nhà nước được lưu trữ riêng biệt, chưa có tính đồng bộ, còn tình trạng tài liệu “bó gói”, “tích đống”, chưa phát huy được hết các giá trị của dữ liệu. Chưa phát huy hết nhu cầu về kết nối, chia sẻ, khai thác cơ sở dữ liệu dùng chung đang được lưu trữ tại các bộ, ngành, địa phương. Cơ quan

nhà nước chưa khai thác, xử lý, phân tích dữ liệu cá nhân tạo ra các dữ liệu tinh phục vụ cho phát triển kinh tế, xã hội.

Bên cạnh đó, theo khảo sát của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) 80% nguyên nhân lộ lọt dữ liệu cá nhân xuất phát từ sự bất cẩn của người dùng. Việc lộ, lọt dữ liệu cá nhân xuất phát chủ yếu từ nguồn thông tin của người dân cung cấp thông qua các hoạt động giao dịch mua bán trên mạng. Song ngay cả việc mua hàng trực tiếp tại những điểm bán hàng lớn, nguy cơ lộ thông tin cá nhân cũng vẫn xảy ra khi người dân tham gia các chương trình khuyến mãi hoặc làm thủ tục vay tiền trả góp để mua hàng,... người dân thường được yêu cầu cung cấp thêm số điện thoại, email,... hoặc người dân đôi khi lại sơ ý để công khai các thông tin cá nhân như số điện thoại trên mạng xã hội hoặc lựa chọn sử dụng dịch vụ của những bên trung gian kém uy tín, chính sách bảo mật thông tin không tốt mà người dùng không tìm hiểu kỹ hoặc không được bên thứ ba cung cấp một cách rõ ràng dẫn đến lộ, lọt thông tin người dùng.

Mặt khác, cũng có nhiều ứng dụng di động, trò chơi trực tuyến, ứng dụng hẹn hò,... yêu cầu các quyền truy cập dữ liệu (như danh sách bạn bè trên Facebook, hồ sơ cá nhân, danh bạ,...) dẫn đến người dùng vô tình chấp thuận cho các ứng dụng này khai thác thông tin cá nhân của mình. Việc cài đặt các ứng dụng, phần mềm không chính thống, chưa được kiểm duyệt hay trên những trang web không có uy tín là hình thức tự bán thông tin của mình, phổ biến nhất là việc xem phim trên những web lậu, không chính thống đã vô tình bị các đối tượng cài vào máy những con virus gián điệp mà người dùng không hề hay biết. Thẻ CCCD chứa nhiều dữ liệu cá nhân quan trọng, theo ghi nhận vẫn có rất nhiều trường hợp người dân “vô tư” chia sẻ ảnh chụp CCCD trên mạng xã hội, đây là việc làm tự mình “tặng” thông tin cá nhân cho đối tượng xấu nhằm mục đích trục lợi bất chính. Không chỉ do sự bất cẩn của người dùng, mà ngày nay có rất nhiều nguồn, thủ đoạn mà hacker có thể tấn công và khai thác vào các cơ sở dữ liệu do các đơn vị quản lý, nhất là những ngành yêu cầu người dân khi tham gia giao dịch phải cung cấp CMND/CCCD. Hiện nay, có rất nhiều doanh nghiệp, tổ chức lưu đầy đủ thông tin người dùng, không chỉ ngân hàng, ví điện tử, các dịch vụ tài chính, nhà mạng di động mà cả các ứng dụng gọi xe công nghệ... chưa có hệ thống bảo mật thông tin người dùng một cách tối ưu nhất mà vẫn còn nhiều lỗ hổng mà các hacker dễ dàng khai thác được, thậm chí, có thể do chính người bên trong các đơn vị quản lý cơ sở dữ liệu tuồn thông tin cá nhân ra bên ngoài. Trong đó cá biệt có những trường hợp doanh nghiệp, tổ chức chủ ý đưa thông tin khách hàng cho bên thứ hay rao bán thông tin khách hàng nhằm thu lợi bất chính, nhiều doanh nghiệp vẫn chưa xem trọng bảo quản thông tin người dùng, không thường xuyên nâng cấp hệ thống bảo mật, xuất hiện nhiều lỗ hổng nhưng sợ tốn kém dẫn đến thờ ơ trong việc bảo mật thông tin người dùng.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Vì vậy, để khắc phục vấn đề trên cũng như góp phần bảo đảm an ninh con người, cần nghiên cứu về giải pháp bảo đảm an ninh con người trước vấn đề lộ lọt dữ liệu cá nhân trong thời kỳ chuyển đổi số.

Trước tình hình đó, Bộ Công an đã phối hợp với các cơ quan, ban, ngành có liên quan triển khai nhiều giải pháp quản lý chặt chẽ thông tin trên không gian mạng, qua đó kiểm soát, hạn chế, ngăn chặn, gỡ bỏ kịp thời thông tin giả, xấu, độc hại, phản cảm. Bộ Công an đã chỉ đạo Công an các đơn vị, địa phương tăng cường công tác nắm tình hình, chủ động phát hiện những sơ hở thiếu sót trong công tác quản lý của các bộ, ngành, địa phương và hoạt động của các tập đoàn, công ty kinh doanh dịch vụ có thu thập dữ liệu cá nhân. Tuyên truyền, nâng cao nhận thức của một số cán bộ, công chức, viên chức về cung cấp, quản lý hồ sơ cá nhân, dữ liệu cá nhân và người dân, nhất là tâm lý sẵn sàng đánh đổi thông tin đời tư, thông tin cá nhân để lấy sự tiện ích về mặt công nghệ. Bên cạnh đó, Bộ Công an cũng chỉ rõ những âm mưu, phương thức, thủ đoạn hoạt động của tội phạm sử dụng công nghệ cao nhằm chiếm đoạt dữ liệu cá nhân; trang bị kiến thức cần thiết để mỗi người có thể tự bảo vệ thông tin cá nhân. Bộ Thông tin và Truyền thông đặt ra nhiệm vụ là tập trung bảo đảm an toàn thông tin cho người dân bằng các biện pháp: phát triển cổng khonggianmang.vn; đẩy mạnh sử dụng các app bảo vệ người dân; giám sát 24/7, phát hiện, cảnh báo, xử lý website lừa đảo, vi phạm pháp luật; hỗ trợ xử lý ngăn ngừa người dùng Internet Việt Nam truy cập vào các trang lừa đảo; kiểm tra việc tuân thủ các quy định về bảo vệ thông tin cá nhân đối với các nền tảng số. Tình trạng mua bán dữ liệu cá nhân đang diễn ra phổ biến, công khai, nhiều hành vi chưa được xử lý vì thiếu quy định của pháp luật. Lỗ hổng pháp lý là việc thiếu vắng cơ chế kiểm soát, bảo vệ dữ liệu cá nhân một cách toàn diện. Do đó, Bộ Công an đang nghiên cứu, dự kiến đến năm 2024 tham mưu Chính phủ trình Quốc hội Luật về bảo vệ dữ liệu cá nhân.

Thời gian tới, cùng với sự phát triển vượt bậc của khoa học - công nghệ, thủ đoạn của tội phạm sử dụng công nghệ cao ngày càng đa dạng và tinh vi hơn; thâm nhập vào đời sống dân sinh để lừa đảo dưới mọi hình thức - chiêu trò - mánh khóe trên tất cả bình diện, gây khó khăn cho lực lượng chức năng trong công tác đấu tranh, phòng ngừa. Cùng với đó, tình trạng lộ lọt dữ liệu cá nhân diễn biến rất phức tạp, theo chiều hướng gia tăng, gây ảnh hưởng không nhỏ đến an ninh con người. Do vậy, cần có những giải pháp khoa học, đồng bộ góp phần bảo đảm an ninh con người trước vấn đề lộ lọt dữ liệu cá nhân trong thời kỳ chuyển đổi số, cụ thể:



Một là, nâng cao nhận thức về an ninh con người trong tình hình mới. Về mặt nhận thức, tiếp tục xác định an ninh con người gắn với độc lập chủ quyền của quốc gia - dân tộc, của chế độ xã hội chủ nghĩa, an ninh quốc gia, trật tự an toàn xã hội; bảo vệ an ninh con người là bảo vệ an ninh quốc gia, coi an ninh con người là một bộ phận của an ninh quốc gia. Theo đó, cần cần tập trung khơi dậy mạnh mẽ tinh thần yêu nước, niềm tự hào, ý chí tự cường, lòng nhân ái, tinh thần đoàn kết, đồng thuận xã hội và khát vọng phát triển đất nước của toàn dân tộc. Xây dựng các cơ chế, chính sách phát huy tinh thần cống hiến vì đất nước của mọi người dân Việt Nam. Phát huy tối đa nhân tố con người, con người là trung tâm, chủ thể, là nguồn lực chủ yếu và mục tiêu của sự phát triển. Thực hiện tốt chính sách xã hội, bảo đảm an sinh và phúc lợi xã hội, tạo chuyển biến mạnh mẽ trong quản lý phát triển xã hội, thực hiện tiến bộ và công bằng xã hội; nâng cao chất lượng cuộc sống và hạnh phúc của Nhân dân cả nước.



Hình 3. Cách bảo vệ dữ liệu thông tin cá nhân

Hai là, tăng cường tuyên truyền, nâng cao nhận thức của người dân trong bảo vệ dữ liệu cá nhân góp phần đảm bảo an ninh con người trong thời kì chuyển đổi số. Do đó, công an các cấp, trong đó lực lượng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao làm nòng cốt chủ động tuyên truyền, phổ biến, giáo dục pháp luật cho nhân dân trong phòng ngừa, phát hiện tội phạm liên quan tới thông tin, dữ liệu cá nhân. Đồng thời, tăng cường cảnh báo về những rủi ro, nguy cơ và hệ lụy của việc tổ chức, người dân tham gia mua bán, giao dịch liên quan tới thông tin, dữ liệu cá nhân. Các vụ việc an ninh, trật tự liên quan tới thông tin, dữ liệu cá nhân cần được tổng kết, tuyên truyền rộng rãi trên báo chí để nhân dân cảnh giác, phòng ngừa.

Ba là, thường xuyên theo dõi, rà soát tình hình lộ lọt, mua bán dữ liệu thông tin cá nhân của cơ quan, tổ chức tại Việt Nam và cảnh báo, hỗ trợ xử lý kịp thời góp phần đảm bảo an ninh con người trong tình hình mới. Lực lượng An ninh kinh tế, Cảnh sát kinh tế, Cảnh sát hình sự, An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao tham mưu, hướng dẫn các bộ, ngành và địa phương quán triệt Nghị định 15/2020/NĐ-CP ngày 3/2/2020 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, tần số vô tuyến điện, công nghệ thông tin và giao dịch điện tử. Đồng thời phối hợp với các đơn vị chức năng của Bộ Công an, Bộ Ngoại giao, Bộ Tư pháp, Ngân hàng Nhà nước, Bộ Y tế, Bộ Tài chính, các doanh nghiệp về các biện pháp tăng cường quản lý nhà nước các hoạt động quản lý căn cước công dân,

hộ tịch, lý lịch tư pháp, hộ chiếu, ngân hàng, bảo hiểm y tế... Triển khai các biện pháp quản lý, kỹ thuật để bảo vệ thông tin cá nhân do mình thu thập, lưu trữ theo quy định về an toàn, an ninh mạng; thường xuyên giám sát, kiểm tra, đánh giá việc bảo vệ dữ liệu thông tin cá nhân của ngành, lĩnh vực, địa bàn thuộc phạm vi quản lý nhằm kịp thời ngăn chặn các hoạt động lợi dụng việc quản lý các thông tin, dữ liệu cá nhân của công dân để mua bán, trao đổi, sử dụng các thông tin, dữ liệu cá nhân trái pháp luật.

Bốn là, hoàn thiện khuôn khổ pháp lý và xây dựng các cơ chế quản lý toàn diện để bảo vệ dữ liệu cá nhân. Xác định các nội dung, nhiệm vụ cụ thể cần triển khai thực hiện theo quy định tại Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân; phân công trách nhiệm cho các cơ quan, đơn vị, địa phương để tổ chức triển khai thực hiện có hiệu quả trên địa bàn. Nâng cao nhận thức, trách nhiệm của các cấp, ngành, cán bộ và quần chúng Nhân dân trong việc triển khai thi hành Nghị định số 13/2023/NĐ-CP; bảo đảm sự phối hợp chặt chẽ giữa các cơ quan chức năng có liên quan, kịp thời hướng dẫn, giải quyết khó khăn, vướng mắc trong quá trình triển khai thực hiện. Để triển khai Nghị định hiệu quả, cần thực hiện tốt công tác tuyên truyền, công tác quản lý nhà nước về bảo vệ dữ liệu cá nhân; rà soát, đánh giá, phân loại dữ liệu cá nhân, xác định nội dung, biện pháp bảo vệ dữ liệu cá nhân và đẩy mạnh công tác điều tra, xử lý hành vi thu thập, chuyển giao, mua, bán trái phép dữ liệu cá nhân.

Tài liệu tham khảo:

Chương trình phát triển Liên hợp quốc (1994), *Báo cáo phát triển con người*, NewYork: Oxford University Press, 1994.

Đảng Cộng sản Việt Nam (2021), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII của Đảng*, Tập 1, Nxb Chính trị quốc gia Sự thật, Hà Nội (tr.156, tr.202) .

**HOÀN THIỆN PHÁP LUẬT VỀ BẢO VỆ THÔNG TIN
CÁ NHÂN CỦA SINH VIÊN TRONG CÁC CƠ SỞ GIÁO DỤC
TẠI VIỆT NAM HIỆN NAY**
**IMPROVING THE LEGAL SYSTEM ON PROTECTING
STUDENTS' PERSONAL INFORMATION IN VIETNAM
EDUCATIONAL INSTITUTIONS NOWADAYS**

Nguyễn Thái Bình, Đào Tấn Anh, Nguyễn Mai Thảo

Trường Đại học Luật TP. Hồ Chí Minh

Tác giả liên hệ: Tananhlaw@gmail.com

THÔNG TIN

TÓM TẮT

<i>Từ khóa:</i>	Thông tin cá nhân nói chung và thông tin cá nhân của sinh viên nói riêng được xác định chính là những thông tin nhằm định
<i>Thông tin cá nhân của sinh viên;</i>	danh một sinh viên (cá nhân) cụ thể. Thực tiễn hiện nay cho thấy rằng
<i>Pháp luật bảo vệ thông tin cá nhân; An ninh sinh viên.</i>	thông tin cá nhân của sinh viên bị rò rỉ, mua bán trái phép ngày càng diễn biến phức tạp kể cả về “chất” và “lượng”. Từ đó, nhóm tác giả tiến hành phân tích bài viết thành ba nội dung chính: (i) Khái quát chung về pháp luật bảo vệ thông tin cá nhân, trong nội dung này, nhóm tác giả đề cập đến khái niệm, quy định của pháp luật Việt Nam hiện hành về vấn đề trên; (ii) Thực trạng rủi ro đối với thông tin cá nhân của sinh viên trong các cơ sở giáo dục, trong nội dung này nhóm tác giả tiến hành khảo sát, đề cập đến một số vụ việc thực tế, đồng thời xác định được lý do xuất phát chủ yếu từ lợi ích kinh tế của hành vi xâm phạm thông tin cá nhân của sinh viên dẫn đến việc hiện nay số lượng chủ thể xâm phạm lớn, ngày càng tinh vi hơn; và (iii) Từ những phân tích trên, nhóm tác giả đưa ra một số kiến nghị hoàn thiện và phân thành hai nhóm chính, bao gồm hoàn thiện pháp luật và nâng cao hiệu quả bảo vệ thông tin cá nhân của sinh viên.
<i>Keywords:</i>	
Student's personal information; Law on Protection of personal information; Student security.	

ABSTRACT

Personal information in general and students' personal information in particular are defined as information that identifies a specific student (individual). Current practice shows that students' personal information being leaked and illegally traded is increasingly complicated, both in "quality" and "quantity". From there, the authors analyzed the article into three main contents: (i) General

overview of the law on personal information protection. In this content, the authors mentioned concepts and regulations of current Vietnamese law on the above issue; (ii) Current status of risks to students' personal information in educational institutions. In this content, the authors conducted a survey, mentioned a number of real cases, and identified the reason comes mainly from the economic benefits of infringing on students' personal information, leading to the current number of infringing subjects being large and becoming more and more sophisticated; and (iii) From the above analysis, the authors make a number of recommendations for improvement and divide them into two main groups, including completing the law and improving the effectiveness of protecting students' personal information.

1. Khái quát chung về pháp luật bảo vệ thông tin cá nhân của sinh viên

1.1. Định nghĩa về thông tin cá nhân và pháp luật bảo vệ thông tin cá nhân của sinh viên

Trước khi đưa ra được định nghĩa về thông tin cá nhân của sinh viên, nhóm tác giả đề cập đến một số thuật ngữ về thông tin cá nhân, dữ liệu cá nhân, từ đó đưa ra được định nghĩa về thông tin cá nhân của sinh viên, vì sinh viên thực chất là cá nhân và được phân biệt dựa trên căn cứ là cá nhân đang theo học tại các cơ sở giáo dục tại Việt Nam hiện nay.

Nghiên cứu dưới góc độ pháp lý, thông tin cá nhân hiện nay đã được pháp luật Việt Nam định nghĩa cụ thể tại một số văn bản quy phạm pháp luật. Theo khoản 15 Điều 3 Luật An toàn thông tin mạng năm 2015 sửa đổi, bổ sung năm 2018 (sau đây gọi là Luật An toàn thông tin mạng) đã quy định thông tin cá nhân là thông tin gắn với việc xác định danh tính của một người cụ thể. Tuy nhiên, cách định nghĩa này vẫn chưa thực sự rõ ràng và đầy đủ để có thể xác định cụ thể thông tin cá nhân bao gồm những thông tin nào. Tham khảo Nghị định số 64/2007/NĐ-CP của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước, tại khoản 5 Điều 3 Nghị định này đã quy định cụ thể hơn về những nguồn thông tin có thể được xác định là thông tin cá nhân theo hướng liệt kê, bao gồm: họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân, số hộ chiếu.

Bên cạnh thuật ngữ “thông tin cá nhân”, hiện nay pháp luật Việt Nam còn xuất hiện thuật ngữ “dữ liệu cá nhân” để quy định về vấn đề này. Tại khoản 1 Điều 2 Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân quy định dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng

tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể.

Theo một số quan điểm, khái niệm dữ liệu cá nhân trong pháp luật Việt Nam hiện nay vẫn chưa có sự thống nhất giữa các văn bản luật chuyên ngành hoặc giữa văn bản luật và văn bản dưới luật, chưa làm rõ các yếu tố cơ bản để xác định thông tin hay dữ liệu đó có phải là dữ liệu cá nhân, chưa thống nhất được thuật ngữ thông tin cá nhân hay dữ liệu cá nhân³⁹. Quan điểm này theo chiều hướng cần có sự thống nhất giữa hai thuật ngữ về thông tin cá nhân hay dữ liệu cá nhân. Tuy nhiên, theo quan điểm của các tác giả khi nghiên cứu định nghĩa của pháp luật về thông tin cá nhân và dữ liệu cá nhân tại Luật An toàn thông tin mạng năm 2015, Nghị định số 64/2007/NĐ-CP và Nghị định số 13/2023/NĐ-CP có thể thấy định nghĩa về dữ liệu cá nhân hàm chứa định nghĩa về thông tin cá nhân. Cụ thể, dữ liệu cá nhân theo Nghị định số 13/2023/NĐ-CP bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm, khi đối chiếu với định nghĩa về thông tin cá nhân tại Nghị định số 64/2007/NĐ-CP⁴⁰ có thể thấy các thông tin này thuộc vào nhóm dữ liệu cá nhân cơ bản theo quy định tại khoản 3 Điều 2 Nghị định số 13/2023/NĐ-CP.

Từ đó, thông tin cá nhân của sinh viên là những thông tin có thể xác định được một sinh viên cụ thể, và những thông tin đó có thể là họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân (căn cước công dân), số hộ chiếu. Đồng thời những thông tin cá nhân này của sinh viên được xác định là dữ liệu cá nhân cơ bản được bảo vệ theo Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân và các văn bản pháp luật khác có liên quan.

1.2. Nội dung pháp luật Việt Nam về bảo vệ thông tin cá nhân của sinh viên

Pháp luật Việt Nam hiện nay đã và đang dần hoàn thiện các quy định pháp luật có liên quan đến bảo vệ thông tin cá nhân nhất là trong xu hướng công nghiệp hóa, hiện đại hóa hiện nay. Trong phạm vi phần này, nhóm tác giả nêu sơ lược những quy định có liên quan đến các quy định về bảo vệ thông tin cá nhân của sinh viên thông qua nhóm quy định chung về bảo vệ thông tin cá nhân và nhóm quy định đặc thù về bảo vệ thông tin cá nhân của sinh viên.

Nhóm quy định chung về bảo vệ dữ liệu cá nhân:

(i) Hiến pháp năm 2013 được xem là luật “mẹ”, làm nền tảng và đặt ra những nguyên tắc trong quá trình xây dựng và thực thi pháp luật tại Việt Nam hiện nay. Tại Điều 21 quy định:

³⁹ Bạch Thị Nhã Nam (2022), *Hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân*, Tạp chí Nghiên cứu Lập pháp số 05 (453), tháng 03/2022, tr. 50 – 57.

⁴⁰ Xem khoản 5 Điều 3 Nghị định số 67/2007/NĐ-CP.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

“1. Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn.

2. Mọi người có quyền bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác.

3. Không ai được bóc mở, kiểm soát, thu giữ trái luật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư của người khác.”

Với quy định trên, mặc dù Hiến pháp năm 2013 sử dụng một số thuật ngữ như “thông tin về đời sống riêng tư”, “thông tin riêng tư”,...nhưng tựu chung lại nội hàm của những thuật ngữ này đều hướng đến “thông tin cá nhân”, đồng thời xác định “thông tin cá nhân” là phạm trù quyền thuộc riêng của cá nhân sở hữu thông tin, là quyền bất khả xâm phạm. Tuy nhiên, cần lưu ý rằng, quyền bất khả xâm phạm này phải được hiểu theo nghĩa “tương đối”. Quyền bất khả xâm phạm về thông tin cá nhân phải được hiểu là khả năng mà cá nhân phải được và chỉ được hưởng lợi ích từ quyền đó. Tuy nhiên trong một số trường hợp như bảo vệ lợi ích của Nhà nước, trật tự, an toàn xã hội thì quyền này “bị xâm phạm” bởi chủ thể mang quyền lực Nhà nước một cách hợp pháp. Chính vì thế, vấn đề bảo vệ thông tin cá nhân của sinh viên không thể không đề cập đến văn bản này.

(ii) Tiếp đến, khi tiếp cận dưới góc độ dân sự, nhóm tác giả đề cập đến hai văn bản chính bao gồm Bộ luật Dân sự năm 2015; Luật An toàn thông tin mạng năm 2015 và Nghị định số 13/2023/NĐ-CP quy định về bảo vệ dữ liệu cá nhân (sau đây gọi là Nghị định số 13/2023/NĐ-CP)⁴¹.

Thứ nhất, Bộ luật Dân sự năm 2015 theo hướng sử dụng thuật ngữ tương tự như Hiến pháp năm 2013, nhóm tác giả cho rằng tại thời điểm ban hành, Bộ luật Dân sự năm 2015 chịu sự ảnh hưởng của Hiến pháp. Cụ thể, Điều 38 quy định Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình với nội dung:

“1. Đời sống riêng tư, bí mật cá nhân, bí mật gia đình là bất khả xâm phạm và được pháp luật bảo vệ.

2. Việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến đời sống riêng tư, bí mật cá nhân phải được người đó đồng ý, việc thu thập, lưu giữ, sử dụng, công khai thông tin liên quan đến bí mật gia đình phải được các thành viên gia đình đồng ý, trừ trường hợp luật có quy định khác.”

⁴¹ Nhóm tác giả đề cập đến Luật An toàn thông tin mạng năm 2015 và Nghị định số 13/2023/NĐ-CP trong phần dân sự là có lý do. Bởi lẽ, hiện nay các văn bản này còn là cơ sở để cơ quan Nhà nước có thẩm quyền xác định làm căn cứ để tiến hành xử phạt vi phạm hành chính, tuy nhiên nhóm tác giả phân tích những quy định có liên quan trong phần này dưới góc độ bảo vệ quyền dân sự của cá nhân về thông tin của họ.

Từ quy định này, nếu cá nhân cho rằng quyền bảo vệ thông tin của mình bị xâm phạm bởi các hành vi như thu thập, lưu trữ, sử dụng... thông tin cá nhân trái pháp luật thì cá nhân đó có quyền sử dụng các phương thức bảo vệ quyền dân sự được quy định tại Điều 11 Bộ luật Dân sự năm 2015. Hiện nay, qua Điều 11 Bộ luật Dân sự năm 2015 ta có thể thấy, khi cá nhân có quyền về đời sống riêng tư bị xâm phạm có thể lựa chọn một trong hai phương thức bao gồm (i) thực hiện quyền tự bảo vệ theo quy định của Bộ luật Dân sự, luật khác có liên quan; hoặc (ii) yêu cầu cơ quan, tổ chức có thẩm quyền thực hiện các phương thức nhất định được liệt kê tại điều này⁴². Và hiện nay, một trong những phương thức được các chủ thể cho rằng quyền của bản thân bị xâm phạm áp dụng nhiều hơn chính là phương thức “bồi thường thiệt hại”.

Thứ hai, Luật An toàn thông tin mạng năm 2015, sửa đổi bổ sung năm 2018 được xem là văn bản có nhiều quy định quan trọng bảo vệ thông tin cá nhân⁴³. Khi xem xét đến Luật này, có thể thấy được một số vấn đề như các hành vi bị nghiêm cấm tại Điều 7, nguyên tắc bảo vệ thông tin cá nhân trên mạng tại Điều 16, thu thập và sử dụng thông tin cá nhân, bảo đảm an toàn thông tin cá nhân trên mạng tại Điều 19 và trách nhiệm của các cơ quan, tổ chức, cá nhân khác được quy định tại Điều 20. Từ những quy định trên, có thể nhận thấy rằng Luật An toàn thông tin mạng năm 2015 đã tạo hành lang pháp lý nhằm bảo vệ quyền của cá nhân trong vấn đề bảo vệ thông tin của cá nhân trên không gian mạng. Điều đáng chú ý ở đây chính là việc cá nhân khi cho rằng thông tin của mình bị sử dụng, khai thác... hoặc bị xâm phạm bởi chủ thể khác thì có quyền yêu cầu “bồi thường thiệt hại”, tương tự như quy định của Bộ luật Dân sự năm 2015, ngoài ra còn có thể tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự (Điều 8 Luật An toàn thông tin mạng năm 2015, sửa đổi bổ sung năm 2018).

Thứ ba, Nghị định số 13/2023/NĐ-CP sử dụng thuật ngữ “dữ liệu cá nhân”, một số quan điểm như nhóm tác giả đã đề cập đồng nhất thuật ngữ “dữ liệu cá nhân” và “thông tin cá nhân”. Nhóm tác giả cho rằng, thông tin cá nhân là dữ liệu cá nhân, tuy nhiên dữ liệu cá nhân là “phân tầng” cao hơn thông tin cá nhân khi đã được tác động bởi bên chủ thể khác, từ đó Nghị định số 13/2023 mới đưa ra những quy định có liên quan đến trách nhiệm của chủ thể xử lý dữ liệu cá nhân. Tuy nhiên, tựu trung lại, Nghị định số 13/2023/NĐ-CP đề cập đến quyền yêu cầu bồi thường thiệt hại, theo đó, chủ thể

⁴² Đào Tấn Anh (2023), *Quyền về đời sống riêng tư của cá nhân trong hoạt động báo chí - một số kiến nghị hoàn thiện luật báo chí*, Hội thảo Khoa học Quốc gia “Cơ sở Khoa học và cơ sở thực tiễn, sửa đổi bổ sung Luật Báo chí 2016”, Viện Đào tạo Báo chí và Truyền thông, Trường ĐHKH & NV phối hợp với Tạp chí Thông tin và Truyền thông (Bộ Thông tin và Truyền thông), <https://hoithao.ictvietnam.vn/quyen-ve-doi-song-rieng-tu-cua-ca-nhan-trong-hoat-dong-bao-chi-mot-so-kien-ngh-i-hoan-thien-luat-bao-chi-181698.html>, truy cập ngày 10/9/2023.

⁴³ Vũ Quỳnh Nga, Lê Thị Ngọc Hà, Nguyễn Quỳnh Trang (2021), *Quyền bảo mật thông tin cá nhân trong hệ thống pháp luật Việt Nam – Thực trạng và giải pháp hoàn thiện pháp luật*, Đề tài sinh viên nghiên cứu khoa học, Trường Đại học Luật Hà Nội, tr. 05.

dữ liệu có quyền yêu cầu bồi thường thiệt hại theo quy định của pháp luật khi xảy ra vi phạm quy định về bảo vệ dữ liệu cá nhân của mình, trừ trường hợp các bên có thỏa thuận khác hoặc luật có quy định khác.

(iii) Trong các lĩnh vực pháp luật khác như Hình sự và Hành chính:

Thứ nhất, trong lĩnh vực hình sự: Theo quy định của Bộ Luật Hình sự năm 2015, sửa đổi bổ sung năm 2017 thì việc xâm phạm thông tin cá nhân khi đủ các yếu tố cấu thành tội phạm sẽ bị xử lý theo Điều 159 về tội xâm phạm bí mật hoặc an toàn thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư khác của người khác có thể bị phạt cải tạo không giam giữ đến 3 năm.

Thứ hai, trong lĩnh vực hành chính. Đối với các hành vi vi phạm khác nhau, các mức phạt hành chính khác nhau được quy định cụ thể. Đơn cử như vấn đề bảo mật thông tin cá nhân thuộc về đời sống riêng tư, bí mật cá nhân, bí mật gia đình. Nghị định 167/2013/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy và chữa cháy; phòng, chống, chống bạo lực gia đình. Nghị định này áp dụng đối với vi phạm của thành viên gia đình tiết lộ hoặc phát tán tư liệu, tài liệu thuộc bí mật đời tư của thành viên gia đình nhằm xúc phạm danh dự, nhân phẩm, sử dụng các phương tiện thông tin, phát tin lừa dối, bài viết...

Nhóm quy định đặc thù về bảo vệ thông tin cá nhân của sinh viên:

Cách phân nhóm này được tác giả sử dụng trong phạm vi bài viết được nhóm tác giả phân tách với mục đích làm rõ vai trò quan trọng trong vấn đề bảo vệ thông tin cá nhân của sinh viên, thực tế quy định của pháp luật Việt Nam không phân tách như thế, bất kỳ chủ thể nào, dù là cơ sở giáo dục, các phòng ban, cá nhân, tổ chức khác khi có hành vi xâm phạm thông tin cá nhân của sinh viên tùy theo tính chất, mức độ mà chủ thể là sinh viên có thể áp dụng các quy định để yêu cầu bồi thường, thực hiện hành vi tố cáo, tố giác, khiếu nại đến các cơ quan Nhà nước có thẩm quyền.

Tại Luật Giáo dục đại học hiện hành mặc dù không minh thị về vấn đề này, tuy nhiên có một số quy định gián tiếp khẳng định các chủ thể có liên quan phải tuân thủ thực hiện các quy định của pháp luật. Đơn cử như Điều 16 quy định về trách nhiệm của Hội đồng trường trường đại học công lập như là “*Giám sát việc thực hiện quyết định của hội đồng trường, việc tuân thủ pháp luật, thực hiện quy chế dân chủ trong hoạt động của trường đại học và trách nhiệm giải trình của hiệu trưởng trường đại học; giám sát việc quản lý, ...*” và “*Tuân thủ pháp luật; chịu trách nhiệm trước pháp luật, trước cơ quan quản lý có thẩm quyền và các bên liên quan về các quyết định của hội đồng trường;...*”

2. Thực trạng rủi ro đối với thông tin cá nhân của sinh viên trong các cơ sở giáo dục

Vấn đề an ninh con người tại Việt Nam lần đầu tiên xuất hiện tại Văn kiện Đại hội XII của Đảng Cộng sản Việt Nam⁴⁴, cho đến Văn kiện Đại hội XIII của Đảng, vấn đề an ninh con người vẫn tiếp tục được đề cập và căn cứ theo 07 thành tố của an ninh con người do Liên hợp quốc đề ra⁴⁵. Theo quan điểm của tác giả, hoàn toàn có thể tiếp cận vấn đề an ninh sinh viên dựa trên an ninh con người, từ đó nhận thấy vấn đề an toàn thông tin cá nhân của sinh viên có sự liên quan mật thiết đến vấn đề an ninh sinh viên hiện nay. Bởi lẽ thông tin cá nhân của sinh viên đang được tác giả nghiên cứu dưới hai góc độ gồm:

- i) Thông tin cá nhân là đối tượng của quyền về đời sống riêng tư, bí mật cá nhân;
- ii) Thông tin cá nhân là đối tượng của tội phạm.

Trong khi đó, an ninh cá nhân và an ninh chính trị là hai thành tố giúp bảo vệ cá nhân tránh khỏi sự đe dọa của tội phạm và xâm phạm các quyền con người⁴⁶. Vì vậy, bảo vệ thông tin cá nhân của sinh viên là một hoạt động trong công tác bảo đảm an ninh sinh viên nói riêng và trong công tác đảm bảo an ninh con người nói chung tại Việt Nam hiện nay.

Thông tin cá nhân của sinh viên bao gồm họ tên, ngày sinh, nghề nghiệp, chức danh, địa chỉ liên hệ, địa chỉ thư điện tử, số điện thoại, số chứng minh nhân dân (căn cước công dân), số hộ chiếu, số tài khoản ngân hàng,... là những thông tin quan trọng và có sự ảnh hưởng trực tiếp đến quá trình học tập và sinh sống của sinh viên. Thực tế, sinh viên trong quá trình học tập và rèn luyện tại các cơ sở giáo dục đều phải ít nhất một lần cung cấp các thông tin cá nhân của mình, nhất là các thông tin như số điện thoại, địa chỉ thư điện tử hoặc số tài khoản ngân hàng nhằm phục vụ các công tác quản lý và hoạt động của Nhà trường, đoàn - Hội, Câu lạc bộ, Đội, Nhóm,... (xem Hình 01).

⁴⁴ Đảng Cộng sản Việt Nam (2016), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội, tr. 135.

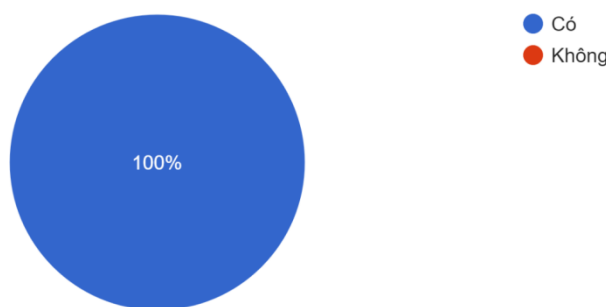
⁴⁵ Đảng Cộng sản Việt Nam (2021), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Tập 1, Nxb. Chính trị quốc gia Sự thật, Hà Nội, tr. 116.

⁴⁶ Nguyễn Viết Thông (2021), *An ninh con người trong văn kiện Đại hội XIII của Đảng*, Trang Thông tin điện tử Hội đồng Lý luận Trung ương, <https://hdl.vn/vi/nghien-cuu---trao-doi/an-ninh-con-nguoi-trong-van-kien-dai-hoi-xiii-cua-dang.html>, truy cập vào 13/9/2023.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Câu hỏi 02. Trong quá trình học tập và rèn luyện tại Trường, bạn có từng cung cấp thông tin cá nhân (số điện thoại, địa chỉ email,...) cho các đơn vị tron..., Đoàn - Hội, Câu lạc bộ, Đội, Nhóm,... trong trường)

93 câu trả lời



Hình 01

Liệu rằng công tác quản lý các thông tin cá nhân của sinh viên tại các cơ sở giáo dục hiện nay đã bảo vệ tốt các thông tin cá nhân của sinh viên hay chưa? Có xuất hiện tình trạng mua bán thông tin cá nhân của sinh viên tại các cơ sở giáo dục hay không? Và liệu rằng vấn đề quản lý, lưu trữ thông tin cá nhân của sinh viên tại các cơ sở giáo dục đã được đảm bảo và tuân thủ nghiêm ngặt các quy định của pháp luật hiện nay hay không?

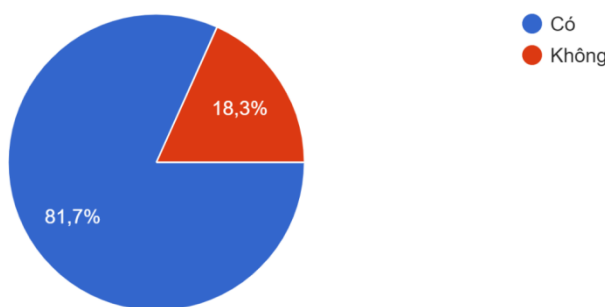
Tại Việt Nam cũng như trên toàn thế giới, rò rỉ thông tin cá nhân của sinh viên không còn là vấn đề mới, tuy nhiên điều này lại tiềm ẩn nhiều rủi ro lớn đối với sinh viên trong thời đại kỹ nguyên số hiện nay. Bên cạnh việc bị quấy rối và làm phiền, sinh viên còn phải đối mặt với những rủi ro lớn về tài sản và nhân thân khi thông tin cá nhân bị xâm phạm. Bởi lẽ những nguồn thông tin cá nhân đặc biệt quan trọng như họ và tên, ngày tháng năm sinh, số điện thoại, địa chỉ thư điện tử, số tài khoản ngân hàng là công cụ, phương tiện để sử dụng các nền tảng công nghệ số hiện nay như ngân hàng, tài khoản mạng xã hội, thương mại điện tử,... Trong thời gian qua, tại Việt Nam và trên thế giới đã có không ít các vụ việc do vô ý hoặc có chủ đích đã gây rò rỉ thông tin cá nhân của sinh viên ra bên ngoài, thậm chí dẫn đến tình trạng sinh viên bị làm phiền bởi các cuộc gọi, thư điện tử của bên thứ ba có được nguồn thông tin cá nhân của sinh viên. Đơn cử như vụ việc hồ sơ của hơn 300.000 sinh viên từ mười trường đại học Việt Nam bị một hacker rao bán, gói dữ liệu này gồm nhiều hình ảnh, thông tin nhạy cảm của sinh viên⁴⁷.

Thực hiện khảo sát trong sinh viên với 93 câu trả lời, nhận thấy có đến 76 sinh viên bị làm phiền bởi các cuộc gọi, thư điện tử từ bên thứ ba và đồng thời nghi ngờ về việc thông tin cá nhân mà bản thân cung cấp tại trường đã bị rò rỉ, phát tán ra bên ngoài, chiếm tỷ lệ đến 81.7% (xem Hình 02).

⁴⁷ Báo điện tử VietNamNet (2021), *Hacker rao bán hồ sơ của 300.000 sinh viên các trường đại học Việt Nam*, <https://vietnamnet.vn/hacker-rao-ban-ho-so-cua-300000-sinh-vien-cac-truong-dai-hoc-viet-nam-766192.html>, truy cập vào 13/9/2023.

Câu hỏi 03. Bạn có bị làm phiền bởi các cuộc gọi, thư điện tử từ bên thứ ba không xác định và đồng thời nghi ngờ về việc thông tin cá nhân mà bản thân...ường đã bị rò rỉ, cung cấp ra bên ngoài hay không?

93 câu trả lời



Hình 02

Có quan điểm nghiên cứu cho rằng thông tin cá nhân là một dạng hàng hóa có giá trị⁴⁸, do đó đây là mục tiêu hướng đến của tội phạm, đặc biệt là tội phạm lừa đảo công nghệ cao. Đồng thời, thông tin cá nhân cũng trở thành mục tiêu mua bán, trao đổi trên thị trường. Điển hình sau kỳ thi tuyển sinh đại học năm 2022, cán bộ tuyển sinh của một trường đại học được gợi ý bán dữ liệu thí sinh dự thi với giá 10.000 đồng mỗi người. Sau khi bị từ chối, người này lại tiếp tục liên hệ trực tiếp với phòng đào tạo trường và ra giá cao hơn⁴⁹. Với số lượng sinh viên trong các cơ sở giáo dục hiện nay, thông tin cá nhân của sinh viên sẽ trở thành mục tiêu thu hút các hành vi tìm kiếm, mua bán trái phép thông tin cá nhân nhằm phục vụ các mục đích bất hợp pháp, xâm phạm quyền riêng tư hoặc thậm chí xâm phạm đến tài sản và nhân thân của sinh viên.

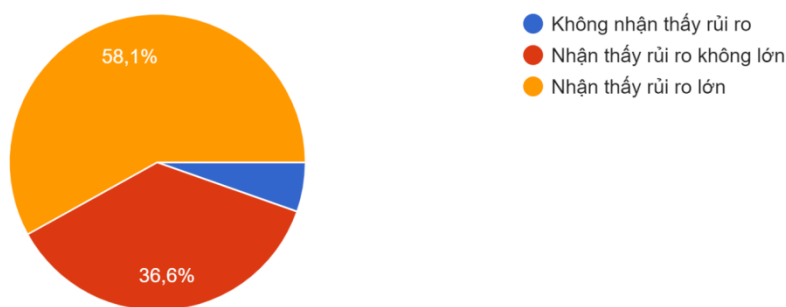
Bên cạnh đó, nhận thức và thái độ của sinh viên hiện nay khi đối mặt với hành vi xâm phạm bí mật thông tin cá nhân cũng đang trở thành một thực trạng đáng báo động trong công tác phòng chống tội phạm xâm phạm thông tin cá nhân của sinh viên. Thực hiện khảo sát trong sinh viên với 93 câu trả lời về việc tự đánh giá mức độ rủi ro đối với bản thân khi thông tin cá nhân tại trường học bị xâm phạm, phát tán bất hợp pháp, có đến 39 sinh viên đánh giá mức độ rủi ro không lớn hoặc không có rủi ro, chiếm tỷ lệ 41.9% (xem Hình 03). Bên cạnh đó, khi được hỏi về biện pháp giải quyết trong trường hợp phát hiện thông tin cá nhân của bản thân bị phát tán, sử dụng vào các mục đích trái phép không được sự đồng ý của bản thân thì có đến 42 sinh viên sẽ bỏ qua, không giải quyết vụ việc, chiếm tỷ lệ 45.2% (xem Hình 04).

⁴⁸ Vũ Công Giao, Lê Trần Như Tuyên (2020), *Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam*, Tạp chí Nghiên cứu Lập pháp số 09 (409), tháng 5/2020, tr. 55.

⁴⁹ Hoài Anh (2023), *Dữ liệu học sinh được chào mua với giá vài nghìn đồng*, <https://vnexpress.net/du-lieu-hoc-sinh-duoc-chao-mua-voi-gia-vai-nghin-dong-4582011.html>, truy cập ngày 14/9/2023.

Câu hỏi 04. Bạn hãy đánh giá về mức độ rủi ro đối với bản thân khi thông tin cá nhân của mình (bao gồm số điện thoại, địa chỉ email) bị rò rỉ, cung cấp trái phép cho bên thứ ba?

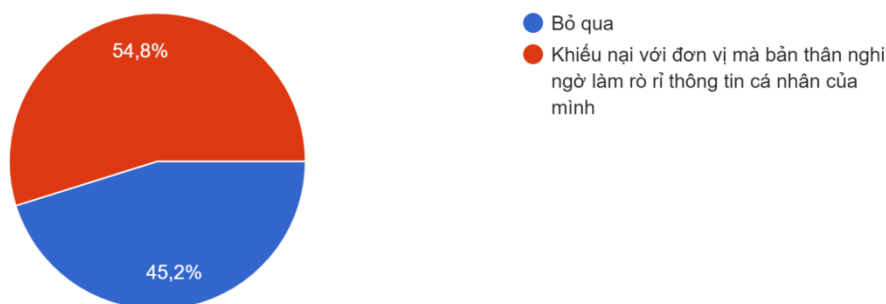
93 câu trả lời



Hình 03

Câu hỏi 05. Hãy cho biết biện pháp giải quyết của bạn khi gặp trường hợp trên?

93 câu trả lời



Hình 04

Qua đó, ta có thể nhận thấy được thực trạng bảo vệ thông tin cá nhân của sinh viên trong các cơ sở giáo dục hiện nay. Bên cạnh các rủi ro lớn về tài sản, nhân thân đối với sinh viên khi thông tin cá nhân bị xâm phạm thì nhận thức và thái độ của sinh viên trong việc bảo vệ quyền, lợi ích của bản thân khi đối mặt với hành vi xâm phạm bí mật thông tin cá nhân cũng đang trở thành một thách thức lớn trong công tác bảo vệ bí mật thông tin cá nhân của sinh viên trong các cơ sở giáo dục nói riêng và trong công tác đảm bảo an ninh sinh viên nói chung.

3. Kiến nghị hoàn thiện pháp luật và nâng cao hiệu quả bảo vệ thông tin cá nhân của sinh viên trong các cơ sở giáo dục tại Việt Nam

Trên cơ sở nghiên cứu về bảo vệ thông tin cá nhân của sinh viên với 03 nguồn thông tin cá nhân bao gồm họ tên, số điện thoại và địa chỉ thư điện tử, tác giả đề xuất một số kiến nghị hoàn thiện pháp luật bảo vệ thông tin cá nhân của sinh viên trong các cơ sở giáo dục tại Việt Nam hiện nay như sau:

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thứ nhất, Nghị định số 13/2023/NĐ-CP cần nghiên cứu bổ sung quy định ghi nhận địa chỉ thư điện tử và số tài khoản ngân hàng là một nguồn dữ liệu cá nhân cơ bản nhằm ghi nhận sự bảo vệ của pháp luật đối với nguồn thông tin cá nhân này. Bởi lẽ thông qua nghiên cứu thực trạng có thể nhận thấy địa chỉ thư điện tử và số tài khoản ngân hàng là hai nguồn thông tin cá nhân quan trọng, có sự ảnh hưởng trực tiếp đến cá nhân sinh viên. Đồng thời, hai nguồn thông tin này cũng đã được xác định là thông tin cá nhân theo quy định tại Nghị định số 64/2007/NĐ-CP. Tuy nhiên, quy định về xác định các nguồn dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm được bảo vệ tại Nghị định số 13/2023/NĐ-CP lại chưa xác định cụ thể về hai nguồn dữ liệu này. Do đó, tác giả kiến nghị bổ sung địa chỉ thư điện tử và số tài khoản ngân hàng thuộc nhóm dữ liệu cá nhân cơ bản tại khoản 3 Điều 2 Nghị định số 13/2023/NĐ-CP nhằm đảm bảo hai nguồn thông tin cá nhân này được bảo vệ theo tinh thần của Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.

Thứ hai, Luật Giáo dục đại học hiện hành cần bổ sung quy định có liên quan đến trách nhiệm của các cơ sở giáo dục trong việc ban hành những quy chế/quy định nhằm bảo vệ thông tin cá nhân của sinh viên. Cụ thể, cần quy định rõ trách nhiệm của cơ sở giáo dục trong việc ban hành quy chế nội bộ quy định nhiệm vụ, quyền hạn của các phòng/ban chuyên môn, phòng/ban chức năng trong việc quản lý, sử dụng thông tin cá nhân của sinh viên.

Cùng với việc kiến nghị hoàn thiện quy định của pháp luật về bảo vệ thông tin cá nhân của sinh viên, theo nhóm tác giả, chính những chủ thể có quyền cụ thể là sinh viên cần phải có trách nhiệm tự bảo vệ thông tin cá nhân của chính bản thân mình. Như khảo sát mà nhóm tác giả đã thực hiện, có 5,4% không nhận thấy rủi ro và 36,6% nhận thấy rủi ro không quá lớn khi thông tin cá nhân bị rò rỉ hoặc cung cấp trái phép bởi bên thứ ba (xem Hình 03). Từ đó, có thể nhận thấy mức độ nhận thức của sinh viên đối với vấn đề thông tin cá nhân này còn đơn giản, tuy nhiên như đã phân tích ở trên, thông tin cá nhân giúp xác định cụ thể được sinh viên đó, đồng thời trong thời đại kỷ nguyên số việc xác định được các thông tin có liên quan đến thông tin cá nhân sẽ ảnh hưởng rất lớn đến các vấn đề về an ninh, trật tự xã hội, đồng thời sẽ là “điểm yếu” để chủ thể xấu lợi dụng nhằm trục lợi một cách phi pháp. Tóm lại, dưới góc độ nâng cao hiệu quả bảo vệ thông tin cá nhân của sinh viên, theo nhóm tác giả, cần nâng cao nhận thức của chính những “người trong cuộc” và chính những chủ thể này phải tự trang bị những kiến thức, kỹ năng và tư tưởng nhằm phòng và chống những hành vi xâm phạm đến thông tin cá nhân của chính mình. Pháp luật chỉ được thực thi một cách đúng đắn và hiệu quả khi chính “người trong cuộc” hiểu và áp dụng đúng.

DANH MỤC TÀI LIỆU THAM KHẢO

- Bộ luật Dân sự năm 2015;
- Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018);
- Nghị định số 64/2007/NĐ-CP của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;
- Nghị định số 13/2023/NĐ-CP của Chính phủ về bảo vệ dữ liệu cá nhân;
- Nghị định 167/2013/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy và chữa cháy; phòng, chống, chống bạo lực gia đình;
- Bạch Thị Nhã Nam (2022), *Hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân*, Tạp chí Nghiên cứu Lập pháp số 05 (453), tháng 03/2022;
- Báo điện tử VietNamNet (2021), *Hacker rao bán hồ sơ của 300.000 sinh viên các trường đại học Việt Nam*, <https://vietnamnet.vn/hacker-rao-ban-ho-so-cua-300000-sinh-vien-cac-truong-dai-hoc-viet-nam-766192.html>;
- Đào Tấn Anh (2023), *Quyền về đời sống riêng tư của cá nhân trong hoạt động báo chí - một số kiến nghị hoàn thiện luật báo chí*, Hội thảo Khoa học Quốc gia “Cơ sở Khoa học và cơ sở thực tiễn, sửa đổi bổ sung Luật Báo chí 2016”, Viện Đào tạo Báo chí và Truyền thông, Trường ĐHKH & NV phối hợp với Tạp chí Thông tin và Truyền thông (Bộ Thông tin và Truyền thông);
- Hoài Anh (2023), *Dữ liệu học sinh được chào mua với giá vài nghìn đồng*, <https://vnexpress.net/du-lieu-hoc-sinh-duoc-chao-mua-voi-gia-vai-nghin-dong-4582011.html>;
- Vũ Quỳnh Nga, Lê Thị Ngọc Hà, Nguyễn Quỳnh Trang (2021), *Quyền bảo mật thông tin cá nhân trong hệ thống pháp luật Việt Nam – Thực trạng và giải pháp hoàn thiện pháp luật*, Đề tài sinh viên nghiên cứu khoa học, Trường Đại học Luật Hà Nội;
- Vũ Công Giao, Lê Trần Như Tuyên (2020), Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế, pháp luật ở một số quốc gia và giá trị tham khảo cho Việt Nam, Tạp chí Nghiên cứu Lập pháp số 09 (409), tháng 5/2020;
- Nguyễn Viết Thông (2021), *An ninh con người trong văn kiện Đại hội XIII của Đảng*, Trang Thông tin điện tử Hội đồng Lý luận Trung ương;
- Đảng Cộng sản Việt Nam (2016), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XII*, Nxb. Chính trị quốc gia Sự thật, Hà Nội;
- Đảng Cộng sản Việt Nam (2021), *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, Tập 1, Nxb. Chính trị quốc gia Sự thật, Hà Nội.

MÔ HÌNH CỘNG TÁC PHÁT HIỆN TẤN CÔNG MẠNG VÀ SĂN TÌM MỐI ĐE DỌA DỰA TRÊN PHƯƠNG PHÁP HỌC LIÊN KẾT

A FEDERATED LEARNING APPROACH FOR COLLABORATIVE INTRUSION DETECTION AND CYBER THREAT HUNTING

Trần Đức Lương, Huỳnh Thái Thi, Nguyễn Hữu Quyền,

Vương Minh Tiên, Ngô Đức Hoàng Sơn

Trường Đại học Công nghệ Thông tin, ĐHQG-HCM

Email: 19521815@gm.uit.edu.vn

THÔNG TIN	TÓM TẮT
Từ khóa: <i>Trung tâm điều hành an ninh, phương pháp học liên kết, trình phát hiện xâm nhập mạng, săn tìm mối đe dọa, mạng khả lập trình, chống tấn công nhiễm độc.</i>	Trong bối cảnh các cuộc tấn công có chủ đích ngày càng trở nên tinh vi, nhu cầu hợp tác giữa các Trung tâm điều hành an ninh (SOC) ở các doanh nghiệp, tổ chức ngày càng trở nên cần thiết. Bằng việc tham gia vào quá trình huấn luyện các trình phát hiện xâm nhập mạng (IDS) theo phương pháp học liên kết, các tổ chức này có thể tận dụng các nguồn thông tin dữ liệu phân tán để huấn luyện mô hình IDS học máy phát hiện các cuộc tấn công mạng mà không xâm phạm đến quyền riêng tư của tổ chức khác; đồng thời làm giàu thông tin trong quá trình săn tìm mối đe dọa nhằm phòng chống các cuộc tấn công 0-day trong tương lai. Bên cạnh đó, cơ chế chống tấn công nhiễm độc hệ thống học liên kết cũng được đề xuất trong đề tài. Kết quả thực nghiệm trên tập dữ liệu Kitsune và triển khai hệ thống làm giàu thông tin trong môi trường mạng khả lập trình cho thấy tính khả thi của bộ giải pháp trong quá trình liên kết các SOC nhằm phát hiện các cuộc tấn công mạng và săn tìm mối đe dọa.

ABSTRACT

Keywords: Witnessing the increasing sophistication of SOC, Federated Learning, Advanced Persistent Threat (APT), the need for IDS, Threat Hunting, SDN, cooperation among Security Operations Centers (SOCs) is becoming more and more imperative. Thus, this work introduces a federated learning (FL) approach for intrusion detection systems (IDS) and cyber threat hunting in the

context of SOC by leveraging the data privacy assurance from collaborative parties. Not only do these SOC teams take advantage of distributed data sources in training machine learning-based IDS (ML-based IDS), but they also enrich the outcome of ML-based IDS in recognizing malicious indicators and the threat hunting process. Additionally, an anti-poisoning mechanism called Local Outlier Factor (LOF) is carried out in order to prevent poisoning attacks against our FL-based system. The experiment results on the Kitsune dataset and the implementation of a knowledge enrichment system in a Software Defined Network (SDN) context have demonstrated the feasibility of the proposed architecture in detecting and hunting network-based threats by collaborative SOC teams.

TỔNG QUAN

Trong những năm gần đây, săn tìm mối đe dọa (Threat Hunting) đang được sử dụng rộng rãi bởi các tổ chức SOC trong việc đảm bảo sự an toàn của hệ thống trước các cuộc tấn công APT. Tuy nhiên, đây là một quá trình phụ thuộc nhiều vào kinh nghiệm, công sức và thời gian của các chuyên gia. Trong khi đó, nhiều nhà nghiên cứu đã tiến hành nghiên cứu các giải pháp săn tìm chủ động kết hợp với trí tuệ nhân tạo (Artificial Intelligence - AI) mà đặc biệt là hệ thống IDS sử dụng AI. Mặt khác, dữ liệu đầu ra của các hệ thống này thường không phù hợp cho quá trình Threat Hunting nên cần được làm giàu một cách tự động để tăng cường hiệu quả cho cuộc săn tìm. Vì thế, việc thiết kế một hệ thống có khả năng làm giàu thông tin [1] cho các hệ thống IDS sử dụng AI là hết sức cần thiết.

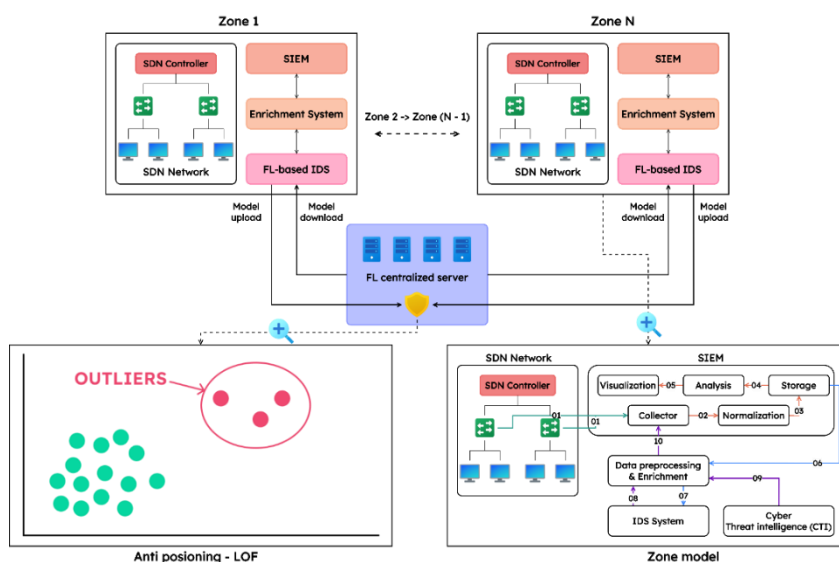
Mặt khác, các mô hình IDS này cũng đòi hỏi khối lượng dữ liệu rất lớn dẫn đến các quan ngại về tính riêng tư của dữ liệu trong quá trình thu thập. Bên cạnh đó, việc sử dụng dữ liệu nội tại của tổ chức hoặc các nguồn dữ liệu được chia sẻ là không đủ để huấn luyện tốt các mô hình IDS nhằm phát hiện các dạng tấn công tinh vi mới. Trong bối cảnh đó, phương pháp học liên kết [2] xuất hiện như một giải pháp đầy hứa hẹn để xây dựng mô hình học cộng tác phát hiện tấn công mạng, cho phép các tổ chức cùng nhau huấn luyện mà vẫn đảm bảo quyền riêng tư giữa các chủ sở hữu dữ liệu. Mặc dù vậy, phương pháp học liên kết vẫn tồn tại một số lỗ hổng khi mà nó có thể bị tấn công đầu độc (poisoning attack) bởi các tổ chức không thiện chí. Để khắc phục điều đó, nhóm đề xuất giải pháp phòng chống tấn công đầu độc (anti-poisoning) [3] sử dụng thuật toán

LOF nhằm xác thực các cập nhật cục bộ trước khi tổng hợp thành mô hình toàn cục hoàn chỉnh.

PHƯƠNG PHÁP NGHIÊN CỨU

Hệ thống huấn luyện mô hình IDS máy học dựa trên phương pháp học liên kết với cơ chế anti-poisoning

Trong mô hình tổng quan được đề xuất, từng trung tâm SOC tham gia vào quá trình huấn luyện liên kết được xem như một vùng (zone). Trong mỗi vùng, hệ thống IDS sẽ đóng vai trò giao tiếp trực tiếp với máy chủ FL trung tâm và cũng là nơi thực hiện quá trình huấn luyện cục bộ (local training). Ngoài ra, cơ chế anti-poisoning sẽ được áp dụng nhằm kiểm tra các mô hình cục bộ trước khi được tổng hợp vào mô hình chung. Các mô hình cục bộ sẽ được xác định là Outlier hay không dựa vào điểm lân cận (Score) được tính bởi thuật toán LOF.



Hình 1: Mô hình tổng quan

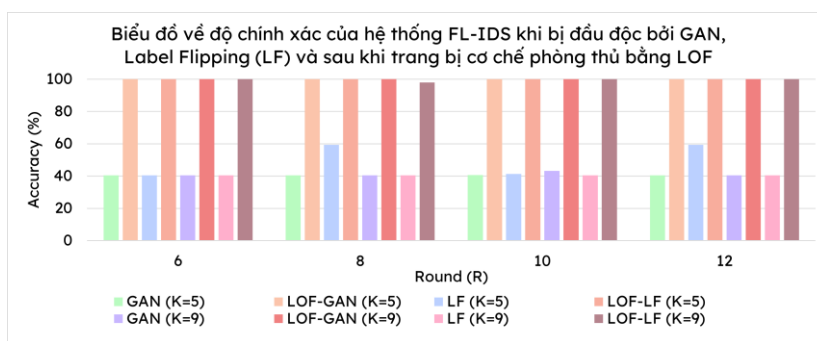
Hệ thống tự động phát hiện tấn công mạng và làm giàu thông tin phục vụ săn tìm mối đe dọa.

Hệ thống IDS sau khi được huấn luyện thông qua học liên kết sẽ được sử dụng trong hệ thống tự động phát hiện tấn công mạng và làm giàu thông tin (zone model trong **Hình 1**). Cách thức hoạt động của nó được mô tả như sau: Đầu tiên, các dữ liệu mạng được từ mạng SDN sẽ được thu thập, chuẩn hóa và lưu trữ bởi SIEM. Sau đó, dữ liệu từ nơi lưu trữ được chuyển tiếp đến hệ thống tiền xử lý và làm giàu thông tin (Data preprocessing and enrichment system - DPE). Ở đây, các thuộc tính cần thiết cho quá trình huấn luyện các trình phát hiện xâm nhập sẽ được trích xuất và gửi đến hệ thống IDS. Đồng thời, hệ thống DPE cũng sẽ thực hiện trích xuất các thông tin làm giàu từ cả dữ liệu nội tại của tổ chức SOC và dữ liệu được chia sẻ ngoài cộng đồng thông qua hệ thống CTI. Cuối cùng, kết quả dự đoán từ hệ thống IDS và thông tin làm giàu sẽ được lưu lại dưới dạng log. Sau đó, log này sẽ được thu thập, phân tích và sử dụng bởi hệ thống SIEM nhằm phục vụ cho quá trình săn tìm mối đe dọa.

KẾT QUẢ THỰC NGHIỆM

Độ hiệu quả của giải pháp anti-poisoning bằng LOF

Để xem ảnh hưởng của các tấn công đầu độc lên phương pháp học liên kết với mô hình đề xuất, chúng tôi tiến hành thực hiện hai cuộc tấn công: tấn công lật nhãn và tấn công bằng mô hình mạng sinh đối kháng trên zone thứ hai kể từ lần cập nhật thứ năm trở đi. Kết quả ở **Hình 2** cho thấy Accuracy của mô hình cộng tác giảm đáng kể xuống còn mức xấp xỉ 40% khi bị tấn công đầu độc. Tuy nhiên, bằng việc ứng dụng cơ chế xác thực bằng LOF để loại bỏ các thành phần tấn công, hiệu quả của mô hình đã được hồi phục và ổn định ở ngưỡng 99% đối với Accuracy. Kết quả này một phần đã chứng minh tính hiệu quả của giải pháp anti-poisoning nhằm mang lại tính bảo mật và chính xác cho quá trình huấn luyện mô hình phát hiện tấn công mạng trong thực tế.

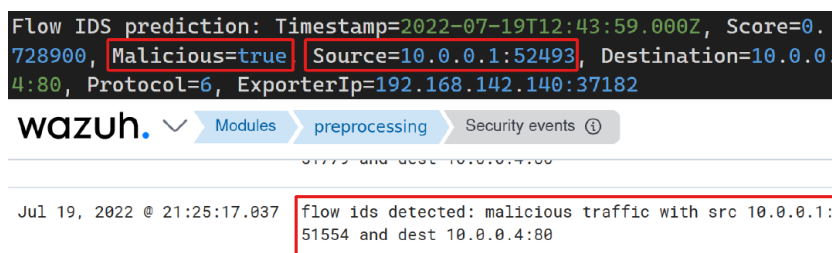


Hình 2: Kết quả chống tấn công đầu độc bằng LOF

Xây dựng hệ thống phát hiện và làm giàu thông tin của trung tâm SOC phục vụ sẵn tìm mối đe dọa

Hệ thống phát hiện bất thường và làm giàu thông tin được chúng tôi triển khai theo mô hình của một SOC zone tại **Hình 1**. Mạng SDN được triển khai sử dụng Containernet. Đối với SIEM, chúng tôi ứng dụng các công cụ mã nguồn mở Wazuh cùng với ELK stack. Ngoài ra, chúng tôi đã viết một chương trình để hiển thị hệ thống DPE. Trong mạng SDN, chúng tôi thực hiện tấn công DOS từ một máy có IP là 10.0.0.1 đến một máy khác trong mạng có IP là 10.0.0.4. Ngay sau đó, hệ thống sẵn tìm đã phát hiện và trực quan hóa cuộc tấn công như

Hình 3.



Hình 3: Log tại các trung tâm SOC khi phát hiện cuộc tấn công kèm theo thông tin làm giàu

KẾT LUẬN

Đề tài đã đề xuất một bộ khung giải pháp an toàn ứng dụng FL trong quá trình phát hiện tấn công và săn tìm mối đe dọa. So với các mô hình săn tìm mối đe dọa trước, chúng tôi đã ứng dụng học liên kết trong việc huấn luyện các hệ thống IDS máy học nhằm phục vụ săn tìm mối đe dọa trên mạng. Tuy nhiên, mô hình đề xuất còn tồn tại một số hạn chế như: xác thực mô hình chưa phi tập trung, độ trễ khi truy vấn dữ liệu trong quá trình làm giàu thông tin, chưa có cơ chế khuyến khích, ...

TÀI LIỆU THAM KHẢO

- [1] H. T. Thi, N. D. H. Son, P. T. Duy and P. Van-Hau, "Federated learning-based cyber threat hunting for APT attack detection in SDN-enabled networks," in *21st International Symposium on Communications and Information Technologies (ISCIT 2022)*, Xi'an, China, 2022.
- [2] T. D. Luong, V. M. Tien, H. T. Anh, N. V. Luyen, N. C. Vy, P. T. Duy and P. Van-Hau, "FedChain: A Collaborative Framework for Building Artificial Intelligence Models using Blockchain and Federated Learning," in *2021 8th NAFOSTED Conference on Information and Computer Science (NICS)*, 2021.
- [3] N. C. Vy, N. H. Quyen, P. T. Duy and P. Van-Hau, "Federated Learning-Based Intrusion Detection in the Context of IIoT Networks: Poisoning Attack and Defense," in *Network and System Security (NSS 2021)*, 2021.

NÂNG CAO NĂNG LỰC CỦA SINH VIÊN TRONG VIỆC ỨNG PHÓ VỚI CÁC RỦI RO TỪ CÔNG NGHỆ DEEPPFAKE ENHANCING STUDENTS’ CAPACITY TO COPE WITH RISKS FROM DEEPPFAKE TECHNOLOGY

Trần Lê Trọng Văn*

Trường Đại học Kinh tế - Luật, ĐHQG-HCM

*Tác giả liên hệ: vantlt21503@st.uel.edu.vn

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> Deepfake, an ninh sinh viên, chuyển đổi số, năng lực số.	Trong thời đại số hóa ngày nay, hình ảnh và âm thanh cũng có thể bị biên tập, chỉnh sửa hoặc làm giả một cách dễ dàng bằng các công cụ kỹ thuật số. Một trong những công cụ đó là Deepfake với khả năng tạo ra các video hoặc hình ảnh giả mạo rất thật bằng cách thay thế chân dung của người này từ chân dung của người khác. Vì vậy, việc nâng cao năng lực của sinh viên trong việc ứng phó với các rủi ro từ công nghệ Deepfake là một vấn đề cấp thiết và quan trọng. Bài tham luận này sẽ trình bày về khái niệm và cơ chế hoạt động của Deepfake, những rủi ro mà công nghệ này gây ra đối với sinh viên, cũng như một số giải pháp để nâng cao năng lực của sinh viên trong việc ứng phó các rủi ro từ công nghệ Deepfake.
<i>Keywords:</i> Deepfake, student security, digital transformation, digital capacity.	ABSTRACT In today’s digital age, images and sounds can be easily edited, altered, or falsified using digital tools. One such tool is Deepfake, which has the ability to create very realistic fake videos or images by replacing one person’s portrait with another’s. Therefore, enhancing students’ capacity to cope with risks from Deepfake technology is an urgent and important issue. This paper will present the concept and mechanism of Deepfake, the risks this technology poses to students, as well as some solutions to enhance students’ capacity in dealing with risks from Deepfake technology.

1. Đặt vấn đề

Trí tuệ nhân tạo (AI) là một trong những lĩnh vực công nghệ số có tốc độ phát triển nhanh chóng và ảnh hưởng sâu rộng đến nhiều khía cạnh của cuộc sống con người. AI không chỉ mang lại những tiện ích cho con người trong các lĩnh vực mà còn tiềm ẩn nhiều nguy cơ và thách thức cho xã hội, đặc biệt là trong việc bảo vệ quyền riêng tư, an toàn thông tin của người dùng Internet. Một trong những công nghệ AI gây ra nhiều tranh cãi và lo ngại nhất là công nghệ Deepfake. Deepfake là sự kết hợp giữa thuật ngữ deep learning (học sâu) và fake (giả mạo). Đây là một dạng thức của trí tuệ nhân tạo (AI), sử dụng các thuật toán “học máy” để chỉnh sửa hoặc tạo ra các hình ảnh, video, âm thanh giả mạo, sao cho chúng trông giống như thật⁵⁰.

Công nghệ Deepfake xuất hiện từ năm 2017, khi một người dùng Reddit có biệt danh Deepfakes đăng tải các video khiêu dâm có sử dụng khuôn mặt của các nữ diễn viên nổi tiếng được ghép vào bằng phần mềm AI⁵¹. Từ đó, công nghệ này đã được phát triển và ứng dụng trong nhiều lĩnh vực khác nhau, chẳng hạn như giải trí, giáo dục, y tế, bảo mật, chính trị... Công nghệ Deepfake có thể mang lại những ứng dụng tích cực, như việc hoán đổi khuôn mặt để tạo ra các hiệu ứng hài hước, lồng tiếng để tạo ra các video song ngữ, tạo ra những video giả lập để huấn luyện hoặc kiểm tra kỹ năng giao tiếp... Tuy nhiên, công nghệ này cũng có thể được sử dụng với những mục đích tiêu cực hoặc xấu xa, như việc xâm phạm quyền riêng tư, tạo ra những tin tức giả mạo, lừa đảo trực tuyến, phá hoại danh tiếng, ảnh hưởng đến niềm tin và an toàn của người dùng Internet.

Trong bối cảnh công nghệ Deepfake ngày càng phát triển và tiềm ẩn nhiều nguy cơ cho xã hội, sinh viên là một trong những đối tượng dễ bị ảnh hưởng bởi công nghệ này. Sinh viên là những người thường xuyên tiếp xúc với các nội dung trực tuyến, có nhu cầu giải trí và học tập cao, cũng như có ít kinh nghiệm và kiến thức về công nghệ. Do đó, sinh viên có thể bị lợi dụng hình ảnh và giọng nói để tạo ra những video khiêu dâm, bạo lực hoặc phỉ báng; bị lừa đảo trực tuyến bằng cách mạo danh người thân, bạn bè hoặc cấp trên để yêu cầu chuyển tiền; bị ảnh hưởng đến uy tín và danh tiếng khi bị tung ra những video giả mạo có nội dung xấu xa hoặc sai sự thật; bị mất niềm tin vào các nguồn thông tin trên Internet khi gặp phải những tin tức giả mạo do Deepfake tạo ra.

Vì vậy, việc nâng cao năng lực của sinh viên trong việc ứng phó với các rủi ro từ công nghệ Deepfake là một vấn đề cấp thiết và quan trọng, đòi hỏi sự quan tâm và đóng góp của cả xã hội nói chung và các cơ quan, tổ chức, cá nhân liên quan nói riêng. Bài

⁵⁰ Hern, A. (2020, January 13). What are deepfakes – and how can you spot them? The Guardian. Retrieved from <https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them>

⁵¹ Laura Payne (2020, August 27). Deepfake. Encyclopedia Britannica. Retrieved from <https://www.britannica.com/technology/deepfake>

tham luận này sẽ trình bày về khái niệm và cơ chế hoạt động của Deepfake, những rủi ro mà công nghệ này gây ra đối với sinh viên, cũng như một số giải pháp để nâng cao năng lực của sinh viên trong việc ứng phó các rủi ro từ công nghệ Deepfake.

2. Khái niệm và cơ chế hoạt động của Deepfake

Deepfake là một kỹ thuật nâng cao để tổng hợp hình ảnh và âm thanh của con người, dựa trên học máy (machine learning - ML) và trí tuệ nhân tạo (artificial intelligence - AI). Công nghệ Deepfake cho phép người sản xuất đặt hình ảnh và/hoặc giọng nói của bất kỳ ai vào một hình ảnh, video hoặc đoạn âm thanh đã có sẵn, và thậm chí có thể được sử dụng để tạo ra những bức ảnh hoàn toàn giả tạo từ đầu.

Cơ chế hoạt động của Deepfake dựa trên công nghệ học sâu, một nhánh của học máy, là một phần của AI. Học sâu mô tả ứng dụng hiện đại của mạng nơ-ron nhân tạo (artificial neural network) vào các bộ dữ liệu lớn. Mạng nơ-ron nhân tạo là một hệ thống máy tính được thiết kế để mô phỏng quá trình học xảy ra trong bộ não sinh học. Khi một người học hoặc phản ứng với thế giới bên ngoài, các kết nối giữa các tế bào não của họ sẽ thay đổi. Chúng tạo thành các mạch và cấu trúc logic, tăng cường một số kết nối và làm yếu các kết nối khác. Khi bạn đã thành thạo một thứ gì đó, chẳng hạn như lái xe, những mạch não này sẽ phản hồi nhanh hơn và hiệu quả hơn.

Về cơ bản, điều này cũng xảy ra tương tự với hệ thống học sâu. Nó sẽ nhìn vào hàng đồng ví dụ về một thứ, lĩnh vực gì đó và dần trở nên hiểu biết về lĩnh vực đó hơn. Trong trường hợp của Deepfake, phần mềm sẽ quét video và ảnh chân dung của một người nào đó và gán khuôn mặt của một người này sang cho một người khác trong video. Để tạo ra Deepfake, người ta sử dụng các công cụ phần mềm và các mô hình học sâu đã được huấn luyện trước. Các công cụ này có thể được tải về từ internet hoặc sử dụng trực tuyến. Các mô hình học sâu là các hệ thống máy tính được thiết kế để bắt chước cách học của não bộ con người. Chúng có thể nhận diện các đặc điểm và quy luật từ các dữ liệu đầu vào, ví dụ như các hình ảnh hoặc âm thanh⁵².

Một trong những kỹ thuật phổ biến để tạo ra Deepfake là sử dụng Mạng Đối sinh (Generative Adversarial Network - GAN). Đây là một loại mạng nơ-ron nhân tạo, gồm hai phần: Mạng Sinh (Generative Network) và Mạng Phân biệt (Discriminative Network). Mạng Sinh có nhiệm vụ tạo ra các hình ảnh mới từ các hình ảnh đã có. Mạng Phân biệt có nhiệm vụ kiểm tra xem các hình ảnh mới có giống với các hình ảnh gốc hay không. Hai phần này sẽ cùng nhau học và cải thiện qua quá trình tranh đấu với nhau. Kết quả cuối cùng là Mạng Sinh có thể tạo ra các hình ảnh Deepfake chân thực và khó phát hiện⁵³.

⁵² Jye Sawtell-Rickson (2023, January 23). What Is a Deepfake? Built In. Retrieved from <https://builtin.com/machine-learning/Deepfake>

⁵³ Megan Ellis (2022, December 8). What Are Deepfakes and How Are They Made? MakeUseOf. Retrieved from <https://www.makeuseof.com/tag/what-are-deepfakes-explained/>

Ví dụ, để tạo ra một video Deepfake, trong đó khuôn mặt của người A được chèn vào khuôn mặt của người B, người ta sẽ cần hai bộ dữ liệu: Một bộ gồm các video của người A và một bộ gồm các video của người B. Sau đó, người ta sẽ cho Mạng Sinh quét qua các video của người A để học được các đặc điểm của khuôn mặt của người A. Tương tự, Mạng Sinh cũng quét qua các video của người B để học được các đặc điểm của khuôn mặt của người B. Sau khi đã học xong, Mạng Sinh sẽ thử tạo ra các video mới, trong đó khuôn mặt của người A được ghép vào khuôn mặt của người B. Những video này sẽ được gửi cho Mạng Phân biệt để kiểm tra xem chúng có giống với video gốc hay không. Nếu Mạng Phân biệt nhận ra rằng video mới là giả, nó sẽ gửi lại cho Mạng Sinh một thông báo lỗi và yêu cầu Mạng Sinh cải thiện. Nếu Mạng Phân Biệt không nhận ra rằng video mới là giả, nó sẽ gửi lại cho Mạng Sinh một thông báo thành công và khuyến khích Mạng Sinh tiếp tục. Quá trình này sẽ lặp đi lặp lại cho đến khi Mạng Sinh tạo ra được các video Deepfake hoàn hảo.

3. Những rủi ro mà công nghệ Deepfake gây ra đối với sinh viên

Công nghệ Deepfake là một công nghệ trí tuệ nhân tạo tiên tiến, có thể tạo ra những video, âm thanh, hay hình ảnh giả mạo một cách chân thực, khiến cho người xem khó phân biệt được thật và giả. Công nghệ này có thể mang lại nhiều lợi ích cho các lĩnh vực như giải trí, nghệ thuật, hay giáo dục. Tuy nhiên, công nghệ này cũng tiềm ẩn nhiều rủi ro và nguy cơ đối với xã hội, đặc biệt là đối với sinh viên. Sinh viên là một nhóm đối tượng có nhu cầu cao về thông tin, có hoạt động tích cực trên mạng xã hội và có vai trò quan trọng trong việc xây dựng, phát triển đất nước trong tương lai. Nếu sinh viên bị lợi dụng và xâm phạm quyền riêng tư bởi công nghệ Deepfake, họ sẽ phải đối mặt với những hậu quả nghiêm trọng về mặt học tập, đời sống và tâm lý.

3.1. Rủi ro về an toàn cá nhân

Một trong những rủi ro của công nghệ Deepfake đối với sinh viên là ảnh hưởng đến an toàn cá nhân. Sinh viên là đối tượng rất dễ bị lừa đảo bởi các cuộc gọi video hoặc tin nhắn giả mạo từ người thân, bạn bè, hoặc cấp trên yêu cầu chuyển tiền cho họ⁵⁴. Công nghệ Deepfake cho phép các kẻ lừa đảo tạo ra những video với hình ảnh và giọng nói giống hệt người được làm giả. Đây là một hình thức lừa đảo mới và rất nguy hiểm vì người nhận cuộc gọi rất khó phân biệt được thật giả và có thể tin tưởng vào những gì họ nhìn thấy và nghe được. Bằng chứng là đã có nhiều vụ việc được ghi nhận trên thế giới và tại Việt Nam liên quan đến việc sử dụng công nghệ Deepfake để thực hiện các hành vi trên. Một ví dụ điển hình là trường hợp của một doanh nhân ở Đức bị mất 220.000 euro (khoảng 5,8 tỷ đồng) vào năm 2019, khi ông nhận được một cuộc gọi từ

⁵⁴ PCBB (2022, February 28). Deepfakes Are Increasing - Top Three Scams To Watch. PCBB. Retrieved from <https://www.pccb.com/bid/2022-02-28-deepfakes-are-increasing-top-three-scams-to-watch>

người giả danh là cấp trên của ông ở Anh, yêu cầu ông chuyển tiền cho một nhà cung cấp ở Hungary⁵⁵. Đây được cho là vụ lừa đảo sử dụng công nghệ Deepfake đầu tiên trên thế giới⁵⁶. Sinh viên cũng có thể gặp phải những trường hợp tương tự, ví dụ như bị người giả danh là cha mẹ, người yêu, hoặc giáo viên yêu cầu chuyển tiền khẩn cấp cho họ vì lý do này hay lý do khác.

Theo các chuyên gia an ninh mạng, công nghệ Deepfake có thể tạo ra các video giả mạo rất khó phát hiện bằng mắt thường. Các kẻ lừa đảo có thể thu thập thông tin cá nhân, hình ảnh, video có giọng nói của nạn nhân hoặc người thân của nạn nhân từ các tài khoản mạng xã hội, rồi sử dụng các phần mềm hoặc ứng dụng Deepfake để tạo ra các video giống hệt người thật. Các video này có thể được gửi qua các ứng dụng nhắn tin hoặc gọi video như Zalo, Messenger, Viber, Telegram... để thực hiện kịch bản lừa đảo. Về khía cạnh tâm lý, công nghệ Deepfake tận dụng sự tin tưởng của con người vào những gì họ nhìn thấy và nghe được. Khi người nhận cuộc gọi video nhìn thấy khuôn mặt và nghe được giọng nói quen thuộc của người thân, người quen, sếp... chúng sẽ có xu hướng tin rằng đó là người thật và không nghi ngờ gì. Đặc biệt khi người gọi yêu cầu chuyển tiền hoặc làm việc gấp với lý do khẩn cấp hoặc thiết tha, người nhận cuộc gọi sẽ bị áp lực tâm lý và không có thời gian để suy nghĩ kỹ. Đặc điểm chung của những cuộc gọi video như vậy thường có âm thanh, hình ảnh không rõ nét, tín hiệu chập chờn giống như trong khu vực phủ sóng di động hoặc wifi yếu để nạn nhân khó phân biệt⁵⁷. Hơn nữa, khi cuộc gọi video chỉ diễn ra trong vài giây, người nhận cuộc gọi sẽ không có cơ hội để kiểm tra hay hỏi thêm những câu hỏi để xác minh thông tin. Do đó, người nhận cuộc gọi sẽ dễ dàng bị lừa đảo mà không hay biết.

Tại Việt Nam, theo chuyên gia tại Trung tâm Giám sát an toàn không gian mạng quốc gia cho biết, thời gian qua, Trung tâm thường xuyên nhận được báo cáo về những vụ việc lừa đảo qua videocal⁵⁸. Trên thực tế đã có nhiều trường hợp tại TP. Hà Nội, Thái Nguyên, Tuyên Quang bị lừa mất hàng trăm triệu đồng bởi các cuộc gọi video Deepfake. Một số nạn nhân đã kể lại rằng, khi nhận được cuộc gọi video từ người thân yêu cầu chuyển tiền gấp, họ đã không để ý kỹ đến chi tiết âm thanh và hình ảnh của người gọi.

⁵⁵ Damiani, J. (2019, September 3). A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000. Forbes. Retrieved from <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=3d21732f2241>

⁵⁶ Margi Murphy (2023, August 25). Deepfake Video Phone Calls Could Be a Dangerous AI-Powered Scam. Bloomberg.com. Retrieved from <https://www.bloomberg.com/news/articles/2023-08-25/deepfake-video-phone-calls-could-be-a-dangerous-ai-powered-scam>

⁵⁷ Dave J. et Alexander J. (2020, June 15). What is a deepfake? Everything you need to know about the AI-powered fake videos that can make anyone say anything. Business Insider India. Retrieved from <https://www.businessinsider.com/guides/tech/what-is-deepfake>

⁵⁸ Đức Thiện (2023, March 30). Cuộc gọi video Deepfake để lừa đảo ra sao? Tuổi Trẻ Online. Retrieved from <https://tuoitre.vn/cuoc-goi-video-deepfake-de-lua-dao-ra-sao-20230330094147252.htm>

Họ chỉ thấy khuôn mặt và giọng nói của người thân rất giống với thực tế, nên đã tin tưởng và làm theo yêu cầu. Sau khi chuyển tiền xong, họ mới liên lạc lại với người thân để xác minh và phát hiện ra sự thật.

Về khía cạnh pháp lý, công nghệ Deepfake cũng gây ra nhiều vấn đề và thách thức cho việc xử lý và phòng ngừa các hành vi lừa đảo. Một trong những vấn đề là việc xác định danh tính và trách nhiệm của các kẻ lừa đảo. Do công nghệ Deepfake cho phép giả mạo hình ảnh và giọng nói của người khác, nên việc nhận diện khuôn mặt hoặc giọng nói của người gọi không còn là cách để xác minh danh tính của họ. Các kẻ lừa đảo cũng có thể sử dụng các biện pháp để che giấu hoặc thay đổi địa chỉ IP, số điện thoại, tài khoản mạng xã hội... để tránh bị truy tìm. Do đó, việc thu thập bằng chứng và xác minh danh tính của các kẻ lừa đảo sẽ rất khó khăn và tốn nhiều thời gian và công sức. Một vấn đề khác là việc thiếu hụt các quy định pháp luật về công nghệ Deepfake và các hành vi lừa đảo sử dụng công nghệ này. Hiện tại, ở Việt Nam chưa có luật nào quy định rõ về công nghệ Deepfake và các hành vi liên quan. Việc xử lý các trường hợp lừa đảo bằng công nghệ Deepfake sẽ phải căn cứ vào các quy định chung về tội lừa đảo chiếm đoạt tài sản hoặc tội xâm phạm quyền riêng tư của người khác. Tuy nhiên, các quy định này có thể không phản ánh được tính chất và mức độ nguy hiểm của công nghệ Deepfake và các hành vi lừa đảo sử dụng công nghệ này.

3.2. Rủi ro về danh dự và uy tín cá nhân

Sinh viên là một đối tượng dễ bị xâm phạm danh dự bằng cách bị tạo ra những video khiêu dâm giả mạo, trong đó khuôn mặt của họ được ghép vào những người khác đang có hành vi gợi dục. Những video này có thể được lan truyền trên mạng xã hội hoặc các trang web khiêu dâm, gây tổn thương tinh thần và uy tín cho nạn nhân. Một ví dụ nổi tiếng là trường hợp của nữ diễn viên Gal Gadot, người đã bị ghép khuôn mặt vào một video khiêu dâm và được chia sẻ rộng rãi trên internet vào năm 2017⁵⁹. Đây là một trong những vụ việc đã gây chú ý đến công nghệ Deepfake và những nguy hiểm của nó. Deepfake có thể xâm phạm quyền riêng tư của sinh viên bằng cách sử dụng hình ảnh hoặc video của họ mà không có sự đồng ý để tạo ra những nội dung giả mạo, nhục mạ hoặc khiêu dâm. Sinh viên cũng có thể bị làm nhục bằng cách bị tạo ra những video khiêu dâm giả mạo từ những hình ảnh cá nhân của họ, ví dụ như những hình ảnh tự sướng, chụp chung với bạn bè, hoặc tham gia các hoạt động xã hội. Theo thống kê của Deeptrace - Công ty có trụ sở tại Amsterdam (Hà Lan) chuyên nghiên cứu về những nội

⁵⁹ Kirsti Melville (2019, August 30). ‘I felt violated’: The woman who took on the ‘ultimate form of victim blaming’. ABC News Australia. Retrieved from <https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774>

dung được tạo ra bởi AI, 96% video Deepfake có nội dung đồi trụy⁶⁰. Hầu hết nạn nhân là ca sĩ, diễn viên nữ nổi tiếng bị ghép mặt vào các bộ phim khiêu dâm. Sinh viên cũng có thể bị làm nhục bằng cách bị tạo ra những video khiêu dâm giả mạo từ những hình ảnh cá nhân của họ, ví dụ như những hình ảnh tự sướng, chụp chung với bạn bè, hoặc tham gia các hoạt động xã hội. Với sự phát triển của công nghệ trí tuệ nhân tạo, việc tạo ra Deepfake không còn đòi hỏi kỹ năng chuyên môn cao hay phần mềm chuyên dụng. Chỉ cần có vài bức ảnh của người muốn ghép khuôn mặt, bất kỳ ai cũng có thể sử dụng các ứng dụng hoặc trang web miễn phí để tạo ra video Deepfake⁶¹.

Công nghệ Deepfake cũng có thể được sử dụng để tạo ra các video gây tranh cãi hoặc phỉ báng về sinh viên, trong đó họ được cho là nói hoặc làm những điều không phù hợp với đạo đức, văn hóa hoặc chính trị. Ví dụ, một sinh viên có thể bị giả giọng hoặc giả mạo hình ảnh để nói những lời lăng mạ, sỉ nhục hoặc vu khống người khác; hoặc để thể hiện những quan điểm cực đoan, phân biệt hoặc xúc phạm đến một nhóm người, một tổ chức hoặc một quốc gia. Những video này có thể được tung ra trên các kênh truyền thông xã hội để gây ra sự phẫn nộ, chỉ trích hoặc bạo lực trong cộng đồng. Hậu quả của tất cả việc này là những tổn thương nghiêm trọng cho hình ảnh cá nhân, danh tiếng của sinh viên, ảnh hưởng đến sự phát triển cá nhân và nghề nghiệp của họ trong tương lai. Một số nạn nhân của đã phải chịu đựng những áp lực tâm lý và thể chất khủng khiếp, thậm chí có người đã tự tử.

3.3. Rủi ro về quyền riêng tư khi sử dụng các ứng dụng công nghệ Deepfake

Sinh viên là một nhóm người có nhu cầu cao về việc sử dụng các ứng dụng Deepfake để thỏa mãn nhu cầu giải trí, học tập, hoặc giao tiếp. Ví dụ, ứng dụng có tên “Zao” cho phép người dùng chèn khuôn mặt của mình vào các cảnh trong các bộ phim nổi tiếng. Hay ứng dụng có tên “FaceApp” cho phép người dùng biến đổi khuôn mặt của mình theo nhiều kiểu khác nhau như già đi, trẻ lại, hoặc thay đổi giới tính. Điều này có thể giúp người dùng có được những trải nghiệm thú vị và độc đáo. Tuy nhiên, khi sử dụng các ứng dụng Deepfake, sinh viên cũng phải cung cấp các thông tin cá nhân nhạy cảm, như hình ảnh chân dung, video, hoặc âm thanh của mình. Điều này có thể tạo ra những rủi ro bị lợi dụng các thông tin cá nhân. Một số ứng dụng Deepfake yêu cầu người dùng đồng ý cho phép nhà phát triển sử dụng, chia sẻ, và thương mại hóa các thông tin cá nhân của họ. Điều này có nghĩa là nhà phát triển có thể sử dụng các thông tin này để tạo ra các sản phẩm mới hoặc bán cho bên thứ ba mà không có sự đồng ý của người dùng. Đây là một việc làm

⁶⁰ Aasha Shaik (2021, July 20). Deepfake Pornography: Beyond Defamation Law? Cyber Forum at Yale Law School. Retrieved from <https://www.cyber.forum.yale.edu/blog/2021/7/20/deepfake-pornography-beyond-defamation-law>

⁶¹ Chris Von Wilpert (2023, September 6). Best Deepfake Software: Top 14 Video & Voice Tools In 2022! Content Mavericks Blog. Retrieved from <https://contentmavericks.com/best-deepfake-software/>

trái với quyền riêng tư của người dùng đối với các thông tin cá nhân của họ. Một số sản phẩm có thể được tạo ra từ các hình ảnh này là các video quảng cáo, các video khiêu dâm, hoặc các video giả mạo. Bên cạnh đó, nhà phát triển hoàn toàn có thể sử dụng các hình ảnh chân dung đó để xây dựng các cơ sở dữ liệu khuôn mặt và sử dụng chúng cho các mục đích khác mà không có sự đồng ý của người dùng.

3.4. Rủi ro về việc tiếp cận thông tin

Sinh viên là một đối tượng dễ bị ảnh hưởng bởi những nội dung Deepfake, bởi vì họ thường tiếp xúc với nhiều nguồn thông tin trên mạng và có thể không có đủ kỹ năng để kiểm tra và phân tích thông tin. Những nội dung Deepfake có thể liên quan đến các vấn đề chính trị, xã hội, kinh tế, y tế, v.v., ảnh hưởng đến quan điểm và hành vi của người xem. Một ví dụ nổi bật là trường hợp của cựu Tổng thống Mỹ Barack Obama, người đã bị tạo ra một video Deepfake trong đó ông phát biểu những lời lẽ thô tục và chỉ trích Tổng thống Mỹ Donald Trump vào năm 2018. Video này được tạo ra bởi nhà làm phim Jordan Peele với mục đích cảnh báo về nguy cơ của công nghệ Deepfake⁶².

Sinh viên cũng có thể bị ảnh hưởng bởi những video Deepfake khác, ví dụ như những video về các nhân vật lịch sử, các nhà lãnh đạo, hoặc các ngôi sao nổi tiếng nói những điều không phù hợp với sự thật hoặc có ý định xấu. Những video này có thể gây ra nhầm lẫn, hiểu lầm, hoặc thiếu kiến thức cho sinh viên khi họ tìm hiểu về các sự kiện hay con người quan trọng. Ví dụ:

- Một video Deepfake cho thấy Tổng thống Ukraine Volodymyr Zelensky dường như sẽ đầu hàng Nga. Đoạn clip lan truyền trên mạng xã hội Nga vào năm 2020. Đoạn video có cảnh Zelensky từ bục giảng kêu gọi quân đội của ông hạ vũ khí và đầu quân cho lực lượng của Tổng thống Nga Vladimir Putin⁶³. Đây là một video giả mạo nhằm gây áp lực chính trị và làm suy yếu uy tín của Zelensky trong cuộc chiến tranh Donbass.

- Một video Deepfake cho thấy Bộ trưởng chính phủ Malaysia Azmin Ali xuất hiện trong một video quan hệ tình dục với người đồng giới vào năm 2019. Hành vi này là bất hợp pháp ở Malaysia, dù những người ủng hộ ông tin rằng hình ảnh đó là giả mạo nhưng các chuyên gia lại không tìm thấy bằng chứng video bị cắt ghép⁶⁴. Đây là một video giả mạo nhằm phá hoại sự nghiệp chính trị và danh tiếng của Ali.

⁶² Kaylee Fagan (2018, April 17). A deepfake video of Barack Obama shows the disturbing future of fake news - Business Insider India. Business Insider India. Retrieved from <https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4>

⁶³ Matthew Holroyd (2020, October 14). Deepfake video of Ukraine's president Zelensky 'surrendering' to Russia goes viral | Euronews. Euronews.com. Retrieved from <https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war>

⁶⁴ Petaling Jaya (2019, June 17). Azmin's office insists videos are fake, refuting foreign reports. Head Topics Malaysia. Retrieved from <https://headtopics.com/my/azmin-s-office-insists-videos-are-fake-refuting-foreign-reports-6437924>

- Một video Deepfake cho thấy nữ diễn viên Scarlett Johansson tham gia vào các cảnh quay khiêu dâm. Đây là một trong số nhiều video Deepfake sử dụng khuôn mặt của các ngôi sao nổi tiếng để tạo ra các nội dung nhạy cảm. Johansson đã phản đối và lên tiếng về sự xâm phạm quyền riêng tư và bản quyền của cô, nhưng cũng thừa nhận rằng không có cách nào để ngăn chặn những video này. Đây là một video giả mạo nhằm lợi dụng hình ảnh của các ngôi sao để kiếm tiền hoặc thỏa mãn nhu cầu bệnh hoạn của một số người⁶⁵.

Những video Deepfake như trên có thể gây ra những ảnh hưởng xấu cho sinh viên theo nhiều cách. Chúng có thể làm sinh viên không biết được đâu là sự thật, đâu là giả mạo, và đâu là ý kiến cá nhân. Từ đó, sinh viên có thể bị cuốn vào những tranh luận không có căn cứ hoặc bị lôi kéo vào những phe phái chính trị hoặc xã hội khác nhau; bị mất niềm tin vào các nguồn thông tin uy tín hoặc bị lừa bởi các nguồn thông tin không minh bạch. Hơn nữa, những video Deepfake có thể làm sinh viên bị sai lầm về các sự kiện hay con người quan trọng trong lịch sử, văn hóa, hoặc xã hội. Chúng ảnh hưởng đến thái độ và sự tôn trọng của sinh viên đối với các nhân vật lịch sử, các nhà lãnh đạo, hoặc các ngôi sao nổi tiếng. Gây cho sinh viên cảm giác lo lắng, sợ hãi, hoặc e ngại khi biết rằng họ cũng có thể trở thành nạn nhân của công nghệ Deepfake. Sinh viên có thể bị mất lòng tin vào bản thân hoặc vào người khác.

4. Một số giải pháp để nâng cao năng lực của sinh viên trong việc ứng phó các rủi ro từ công nghệ Deepfake

Công nghệ Deepfake là một công nghệ sử dụng trí tuệ nhân tạo để tạo ra các hình ảnh, video, hoặc âm thanh giả mạo của người thật. Công nghệ này có ích cho sinh viên trong việc giải trí, học tập hoặc giao tiếp. Nhưng công nghệ này cũng rủi ro cho sinh viên về an toàn cá nhân, danh dự và uy tín cá nhân, quyền riêng tư khi sử dụng các ứng dụng công nghệ Deepfake và việc tiếp cận thông tin. Để đối phó với các rủi ro này, sinh viên cần nâng cao năng lực của mình trong việc sử dụng và phản biện công nghệ Deepfake.

(1) Tăng cường nhận thức và kiến thức về công nghệ Deepfake và các hậu quả tiêu cực của nó

Một trong những biện pháp quan trọng để phòng ngừa và bảo vệ bản thân khỏi các rủi ro do công nghệ Deepfake gây ra là tăng cường nhận thức và kiến thức về công nghệ này và các hậu quả tiêu cực của nó. Điều này giúp sinh viên có thể nhận biết và phòng tránh các nội dung Deepfake có ý định xấu, cũng như bảo vệ quyền và lợi ích của bản thân và người khác.

⁶⁵ Zack S. (2018, December 31). Scarlett Johansson on Fake AI Porn: ‘Nothing Can Stop Someone From Cutting and Pasting My Image’. IndieWire. Retrieved from <https://www.indiewire.com/features/general/scarlett-johansson-deepfakes-face-porn-videos-1202031678/>

Để làm được điều này, sinh viên cần được cập nhật về các xu hướng, ứng dụng và nguy cơ của công nghệ này thông qua các kênh thông tin chính thống và tin cậy, như các trang web, tạp chí, sách hoặc chương trình khoa học, giáo dục, pháp luật... Sinh viên cũng cần được trang bị các kỹ năng phân tích và đánh giá thông tin một cách kỹ lưỡng và khách quan, để có thể phát hiện và phòng tránh các nội dung Deepfake có ý định xấu. Các kỹ năng này bao gồm: xác định nguồn gốc, tác giả, mục đích và độ tin cậy của thông tin; so sánh và kiểm tra thông tin với các nguồn khác; nhận biết các dấu hiệu bất thường hoặc mâu thuẫn trong hình ảnh, video, âm thanh hoặc giọng nói; đặt câu hỏi và tìm kiếm bằng chứng cho thông tin⁶⁶.

Ngoài ra, sinh viên cũng cần được hướng dẫn cách sử dụng các công cụ kiểm tra và xác minh thông tin, như Google Reverse Image Search⁶⁷, InVID Verification Plugin⁶⁸, Microsoft Video Authenticator⁶⁹ hay Sensity⁷⁰, để có thể kiểm tra nguồn gốc, tính xác thực và độ tin cậy của các hình ảnh, video, âm thanh hoặc giọng nói mà họ tiếp xúc. Các công cụ này hoạt động bằng cách sử dụng các thuật toán AI để phát hiện các dấu vết của sự can thiệp hoặc thay đổi trong các nội dung truyền thông, như các vết nối, biến dạng, mờ nhòe, sai màu hay sai ánh sáng.

(2) Tăng cường bảo mật thông tin cá nhân trên các kênh truyền thông và mạng xã hội

Một biện pháp bảo vệ bản thân khác để ứng phó với rủi ro do công nghệ Deepfake gây ra là tăng cường bảo mật thông tin cá nhân trên các kênh truyền thông và mạng xã hội. Điều này giúp sinh viên có thể ngăn chặn hoặc giảm thiểu khả năng bị lợi dụng hình ảnh cá nhân để tạo ra các nội dung Deepfake có hại cho danh tiếng, quyền riêng tư hoặc tài chính của họ.

Để làm được điều này, sinh viên cần chú ý đến việc thiết lập các cài đặt bảo mật và quyền riêng tư cho các tài khoản, ứng dụng và thiết bị của họ. Cụ thể, sinh viên nên:

- Sử dụng các mật khẩu mạnh, khác nhau cho mỗi tài khoản và thay đổi thường xuyên.
- Kích hoạt xác minh hai yếu tố.
- Chỉ cho phép những người tin tưởng truy cập vào thiết bị.

⁶⁶ Sally Adey (2020, April 29) IEEE Spectrum: Technology, Engineering, and Science News (2020, April 29). What Is a Deepfake? IEEE Spectrum: Technology, Engineering, and Science News. Retrieved from <https://spectrum.ieee.org/what-is-deepfake>

⁶⁷ Johannes Langguth (2021, May 21). Don't Trust Your Eyes: Image Manipulation in the Age of DeepFakes. Media Governance and the Public Sphere, 5-2021. Retrieved from <https://www.frontiersin.org/articles/10.3389/fcomm.2021.632317/full>

⁶⁸ John Villasenor (2019, February 14). Artificial intelligence, deepfakes, and the uncertain future of truth. Brookings Institution. Retrieved from <https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/>

⁶⁹ Rabia Noureen (2020, September 2). Microsoft Video Authenticator aims to detect deepfakes by using AI and Azure. OnMSFT.com. Retrieved from <https://www.onmsft.com/news/microsoft-video-authenticator-aims-to-detect-deepfakes-by-using-ai-and-azure/>

⁷⁰ Sensity.ai (n.d.). Deepfake Detection. Sensity.ai. Retrieved from <https://sensity.ai/deepfake-detection/>

Kỹ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- Chỉ sử dụng các ứng dụng từ các nhà phát triển uy tín.
- Chỉ kết nối với các mạng wifi an toàn và có mật khẩu.
- Không tải về hoặc mở các tệp tin đính kèm đáng ngờ.
- Không nhấp vào các liên kết lạ hoặc không rõ nguồn gốc.

Bên cạnh đó, sinh viên cũng cần hạn chế việc chia sẻ các thông tin cá nhân nhạy cảm, như hình ảnh, video, âm thanh hoặc giọng nói của bản thân hoặc người thân, với những người không quen biết hoặc không tin tưởng. Cách làm này giúp sinh viên tránh bị thu thập dữ liệu để huấn luyện các mô hình Deepfake. Sinh viên nên:

- Kiểm tra lại các quyền truy cập của các ứng dụng đến máy ảnh, microphone, bộ nhớ hoặc vị trí của thiết bị.
- Chỉ chia sẻ các nội dung cá nhân với những người được cho phép và thiết lập chế độ riêng tư cho các bài đăng.
- Không để lộ các thông tin cá nhân trên các trang cá nhân, hồ sơ hoặc tiểu sử.

Sinh viên cũng cần thận trọng khi tiếp xúc với những người lạ hoặc những thông điệp đáng ngờ trên mạng, để tránh bị lừa đảo hoặc bị lấy cắp thông tin cá nhân. Sinh viên nên:

- Kiểm tra lại danh tính và thông tin của người liên lạc.
- Không tiết lộ các thông tin cá nhân, tài khoản, mật khẩu, mã xác minh hoặc số thẻ ngân hàng cho bất kỳ ai.
- Không gửi tiền hoặc quà cho những người không rõ lai lịch.
- Không tham gia vào các cuộc trò chuyện hay cuộc gọi có nội dung nhạy cảm hoặc bất thường.

Nếu nhận thấy có dấu hiệu bị tấn công hoặc lừa đảo bằng công nghệ Deepfake, sinh viên cần báo cáo ngay cho các cơ quan chức năng và yêu cầu hỗ trợ. Sinh viên có thể liên hệ với các cơ quan pháp luật, an ninh mạng, bảo vệ quyền riêng tư hoặc quản lý nội dung truyền thông để trình báo về các trường hợp vi phạm pháp luật, xâm phạm quyền riêng tư, lừa đảo hay phỉ báng liên quan đến công nghệ Deepfake. Sinh viên cũng có thể yêu cầu các cơ quan này hỗ trợ trong việc xóa bỏ, khóa hoặc gỡ bỏ các nội dung Deepfake có hại cho mình.

(3) Phát triển kỹ năng nhận thức và phản biện các nguồn thông tin sử dụng công nghệ Deepfake

Trước những rủi ro do công nghệ Deepfake gây ra, việc nâng cao năng lực phân tích và đánh giá các nguồn thông tin sử dụng công nghệ này là một biện pháp quan trọng. Điều này giúp sinh viên có thể phòng ngừa và chống lại các hành vi lợi dụng công nghệ Deepfake để tuyên truyền, đánh lừa hoặc xuyên tạc thông tin.

Để có được năng lực này, sinh viên cần chủ động trang bị cho mình kiến thức về công nghệ Deepfake, bao gồm cách thức hoạt động, ứng dụng và hậu quả của nó. Tất nhiên, các tổ chức giáo dục, các tổ chức khoa học và các nhà nghiên cứu trong lĩnh vực

cần hỗ trợ sinh viên bằng cách cung cấp các nguồn thông tin chất lượng, chính xác về công nghệ này cũng như các rủi ro và cách ứng phó rủi ro của Deepfake thông qua các bài báo, sách, tạp chí, video hoặc podcast,... Các chuyên gia, nhà nghiên cứu hoặc tổ chức có uy tín trong lĩnh vực này cũng cần tổ chức các khóa học, workshop, webinar hoặc hội thảo về công nghệ Deepfake để cập nhật cho sinh viên các kiến thức mới nhất.

Ngoài ra, sinh viên cũng cần phát triển kỹ năng phê bình và đánh giá các nguồn thông tin sử dụng công nghệ Deepfake. Sinh viên không nên tin tưởng một cách mù quáng vào bất kỳ thông tin nào mà không kiểm tra lại nguồn gốc, tính xác thực và độ tin cậy của nó. Một bộ tiêu chí được gợi ý sử dụng để đánh giá tính xác thực của thông tin có thể là:

1. Ai là tác giả hoặc người phát ngôn của thông tin?
2. Thông tin được đăng tải ở đâu và khi nào?
3. Thông tin có được trích dẫn từ các nguồn khác không và nguồn đó là gì?
4. Thông tin có bị thiếu sót, sai lệch hoặc thiên vị không?
5. Thông tin có mục đích gì và hướng đến ai?

Bên cạnh đó, sinh viên cũng có thể sử dụng các công cụ kiểm tra sự thật hoặc phát hiện Deepfake để xác minh tính chính xác của các nguồn thông tin. Nếu nhận thấy có những nguồn thông tin sai lệch hoặc gây hiểu lầm về công nghệ Deepfake, sinh viên cần phản bác, làm rõ hoặc báo cáo cho các cơ quan có thẩm quyền. Sinh viên tuyệt đối không sử dụng công nghệ này để tạo ra hoặc lan truyền các nội dung sai trái, xuyên tạc hoặc xâm hại đến quyền lợi của người khác. Sinh viên cũng không nên chia sẻ hay lan truyền các nguồn thông tin mà mình không chắc chắn về tính xác thực hoặc không kiểm tra lại nguồn gốc. Cuối cùng, sinh viên cần có trách nhiệm trong việc sử dụng và chia sẻ các nguồn thông tin sử dụng công nghệ Deepfake.

(4) Cần có sự hỗ trợ và hợp tác của các tổ chức, cá nhân, các tổ chức giáo dục, và cơ quan chức năng

Việc các tổ chức, cá nhân, các tổ chức giáo dục, cơ quan chức năng hỗ trợ và hợp tác với nhau giúp tạo ra một môi trường an toàn, minh bạch và có trách nhiệm trong việc sử dụng và phát triển công nghệ Deepfake.

Đối với các tổ chức và cá nhân sử dụng công nghệ Deepfake, việc tuân thủ các nguyên tắc đạo đức và pháp lý trong việc tạo ra, sử dụng và chia sẻ các nội dung sử dụng công nghệ này là một trách nhiệm không thể thiếu. Bằng cách làm như vậy, họ không chỉ bảo vệ quyền lợi của bản thân mà còn góp phần duy trì uy tín và niềm tin của cộng đồng đối với công nghệ này. Họ cũng nên ghi rõ nguồn gốc, mục đích và phương thức của các nội dung này, không sử dụng chúng để gây hại hoặc xâm phạm đến quyền lợi của người khác. Hơn nữa, họ cũng nên tham gia vào các hoạt động giáo dục, tuyên truyền và nâng cao nhận thức về công nghệ Deepfake cho cộng đồng.

Đối với các tổ chức giáo dục, việc đào tạo cho sinh viên về công nghệ Deepfake, bao gồm kiến thức, kỹ năng và thái độ liên quan đến công nghệ này là một nhiệm vụ quan trọng. Bằng cách làm như vậy, họ không chỉ giúp người học tiếp cận và ứng dụng công nghệ này một cách hiệu quả mà còn giáo dục cho người học những giá trị xã hội trong thời đại số. Họ cần tích hợp công nghệ Deepfake vào các chương trình giảng dạy, khuyến khích người học sáng tạo và khám phá các ứng dụng tích cực của công nghệ này. Họ cũng cần hướng dẫn người học về các nguyên tắc đạo đức và pháp lý trong việc sử dụng công nghệ Deepfake, giáo dục người học về trách nhiệm xã hội và nhân quyền trong thời đại số.

Đối với các cơ quan chức năng, việc ban hành và thực thi các điều luật, quy định và chính sách liên quan đến công nghệ Deepfake là một biện pháp thiết yếu. Bằng cách làm như vậy, họ không chỉ bảo vệ quyền lợi của người dân trước những tác động tiêu cực của công nghệ này, như vi phạm bản quyền, xâm phạm danh dự, uy tín hoặc riêng tư của cá nhân hoặc tổ chức mà còn khuyến khích và hỗ trợ các hoạt động nghiên cứu, phát triển và ứng dụng công nghệ Deepfake cho mục đích xã hội hóa.

5. Kết luận

Deepfake là một công nghệ tiên tiến và đầy tiềm năng trong nhiều lĩnh vực khác nhau. Nếu được sử dụng một cách hợp lý và có trách nhiệm, Deepfake có thể mang lại nhiều lợi ích cho xã hội và con người. Tuy nhiên, Deepfake cũng có những mặt trái và nguy cơ gây ra những hậu quả tiêu cực nếu bị lạm dụng. Đặc biệt, trong bối cảnh an ninh sinh viên đang bị đe dọa bởi những hình ảnh Deepfake giả mạo, xuyên tạc hay phỉ báng, sinh viên cần có những kiến thức và kỹ năng để phòng tránh và bảo vệ bản thân khỏi những tác động tiêu cực từ công nghệ này. Bên cạnh đó, sinh viên cũng cần có tinh thần sáng tạo và khám phá để khai thác những ứng dụng tích cực của Deepfake trong các lĩnh vực học thuật, giải trí hay xã hội. Hy vọng tham luận này sẽ góp phần nâng cao nhận thức và năng lực của sinh viên trong việc ứng phó với các rủi ro từ công nghệ Deepfake, cũng như khuyến khích các nghiên cứu về việc kiểm soát và phát huy tối ưu lợi ích từ công nghệ này trong tương lai.

TÀI LIỆU THAM KHẢO

Tạp chí (*bản online*):

- Hern, A. (2020, January 13). What are deepfakes – and how can you spot them? The Guardian. Retrieved from <https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them>
- Laura Payne (2020, August 27). Deepfake. Encyclopedia Britannica. Retrieved from <https://www.britannica.com/technology/deepfake>

- Jye Sawtell-Rickson (2023, January 23). What Is a Deepfake? Built In. Retrieved from <https://builtin.com/machine-learning/Deepfake>
- Megan Ellis (2022, December 8). What Are Deepfakes and How Are They Made? MakeUseOf. Retrieved from <https://www.makeuseof.com/tag/what-are-deepfakes-explained/>
- PCBB (2022, February 28). Deepfakes Are Increasing - Top Three Scams To Watch. PCBB. Retrieved from <https://www.pcbb.com/bid/2022-02-28-deepfakes-are-increasing-top-three-scams-to-watch>
- Damiani, J. (2019, September 3). A Voice Deepfake Was Used To Scam A CEO Out Of \$243,000. Forbes. Retrieved from <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=3d21732f2241>
- Margi Murphy (2023, August 25). Deepfake Video Phone Calls Could Be a Dangerous AI-Powered Scam. Bloomberg.com. Retrieved from <https://www.bloomberg.com/news/articles/2023-08-25/deepfake-video-phone-calls-could-be-a-dangerous-ai-powered-scam>
- Dave J. et Alexander J. (2020, June 15). What is a deepfake? Everything you need to know about the AI-powered fake videos that can make anyone say anything. Business Insider India. Retrieved from <https://www.businessinsider.com/guides/tech/what-is-deepfake>
- Đức Thiện (2023, March 30). Cuộc gọi video Deepfake để lừa đảo ra sao? Tuổi Trẻ Online. Retrieved from <https://tuoitre.vn/cuoc-goi-video-deepfake-de-lua-dao-ra-sao-20230330094147252.htm>
- Kirsti Melville (2019, August 30). ‘I felt violated’: The woman who took on the ‘ultimate form of victim blaming’. ABC News Australia. Retrieved from <https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774>
- Aasha Shaik (2021, July 20). Deepfake Pornography: Beyond Defamation Law? Cyber Forum at Yale Law School. Retrieved from <https://www.cyber.forum.yale.edu/blog/2021/7/20/deepfake-pornography-beyond-defamation-law>
- Chris Von Wilpert (2023, September 6). Best Deepfake Software: Top 14 Video & Voice Tools In 2022! Content Mavericks Blog. Retrieved from <https://contentmavericks.com/best-deepfake-software/>
- Kaylee Fagan (2018, April 17). A deepfake video of Barack Obama shows the disturbing future of fake news - Business Insider India. Business Insider India. Retrieved from <https://www.businessinsider.com/obama-deepfake-video-insulting-trump-2018-4>

- Matthew Holroyd (2020, October 14). Deepfake video of Ukraine’s president Zelensky ‘surrendering’ to Russia goes viral | Euronews. Euronews.com. Retrieved from <https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war>
- Petaling Jaya (2019, June 17). Azmin’s office insists videos are fake, refuting foreign reports. Head Topics Malaysia. Retrieved from <https://headtopics.com/my/azmin-s-office-insists-videos-are-fake-refuting-foreign-reports-6437924>
- Zack S. (2018, December 31). Scarlett Johansson on Fake AI Porn: ‘Nothing Can Stop Someone From Cutting and Pasting My Image’. IndieWire. Retrieved from <https://www.indiewire.com/features/general/scarlett-johansson-deepfakes-face-porn-videos-1202031678/>
- Sally Adey (2020, April 29) IEEE Spectrum: Technology, Engineering, and Science News (2020, April 29). What Is a Deepfake? IEEE Spectrum: Technology, Engineering, and Science News. Retrieved from <https://spectrum.ieee.org/what-is-deepfake>
- Johannes Langguth (2021, May 21). Don't Trust Your Eyes: Image Manipulation in the Age of DeepFakes. Media Governance and the Public Sphere, 5-2021. Retrieved from <https://www.frontiersin.org/articles/10.3389/fcomm.2021.632317/full>
- John Villasenor (2019, February 14). Artificial intelligence, deepfakes, and the uncertain future of truth. Brookings Institution. Retrieved from <https://www.brookings.edu/articles/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/>
- Rabia Noureen (2020, September 2). Microsoft Video Authenticator aims to detect deepfakes by using AI and Azure. OnMSFT.com. Retrieved from <https://www.onmsft.com/news/microsoft-video-authenticator-aims-to-detect-deepfakes-by-using-ai-and-azure/>
- Sensity.ai (2023). Deepfake Detection. Sensity.ai. Retrieved from <https://sensity.ai/deepfake-detection/>

**PHÁP LUẬT VỀ AN NINH SINH VIÊN TỪ GÓC ĐỘ GIỚI HẠN
QUYỀN TỰ DO NGÔN LUẬN TRÊN KHÔNG GIAN MẠNG -
KINH NGHIỆM QUỐC TẾ VÀ VẬN DỤNG CHO VIỆT NAM
LEGISLATION ON STUDENT SECURITY FROM THE
PERSPECTIVE OF LIMITING FREEDOM OF EXPRESSION
IN CYBERSPACE - INTERNATIONAL EXPERIENCE AND
APPLICATION TO VIETNAM**

Bùi Lê Hiếu*, Nguyễn Thu Hiền

Học viện Tòa án

*Tác giả liên hệ: buihieuvank25thd@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> An ninh sinh viên, quyền tự do ngôn luận, giới hạn quyền, không gian mạng, kinh nghiệm.	Pháp luật về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng là một chủ đề quan trọng và đang được quan tâm rộng rãi. Mục đích là tìm hiểu, phân tích các quy định và chính sách liên quan đến an ninh sinh viên và quyền tự do ngôn luận trên không gian mạng, từ đó đề xuất các giải pháp, khuyến nghị nhằm cải thiện tình hình hiện tại. Phương pháp nghiên cứu bao gồm việc thu thập và phân tích các tài liệu pháp lý, các nghiên cứu quốc tế và kinh nghiệm của các quốc gia khác về vấn đề này. Kết quả đạt được từ nghiên cứu sẽ cung cấp cái nhìn tổng quan về tình hình hiện tại của pháp luật về an ninh sinh viên và quyền tự do ngôn luận trên không gian mạng. Đồng thời đưa ra các khuyến nghị và giải pháp nhằm cải thiện tình hình, bảo vệ quyền lợi và đảm bảo an ninh cho sinh viên trong việc sử dụng không gian mạng. Các kết luận chính của nghiên cứu sẽ tập trung vào việc nhấn mạnh sự cần thiết của việc giới hạn quyền tự do ngôn luận trên không gian mạng để đảm bảo an ninh sinh viên và bảo vệ quyền lợi của các cá nhân và cộng đồng.

ABSTRACT

Student security legislation from the perspective of limiting freedom of expression in cyberspace is an important topic and is receiving widespread attention. The

Keywords:

Student security, freedom of speech, rights restrictions, cyberspace, experience.

aim is to understand and analyze regulations and policies related to student security and freedom of expression in cyberspace, thereby proposing solutions and recommendations to improve the current situation. Research methodology will include the collection and analysis of legal documents, international studies and the experience of other countries in this regard. Findings from the study will provide an overview of the current state of student security legislation and freedom of expression in cyberspace. At the same time, make recommendations and solutions to improve the situation, protect the rights and ensure security for students in the use of cyberspace. The main conclusions of the study will focus on emphasizing the need to limit freedom of expression in cyberspace to ensure student security and protect the rights of individuals and communities. The study will also propose reasonable measures and policies to do this, while respecting the protection of freedom of expression in accordance with the law.

1. Giới thiệu

Quyền tự do ngôn luận là một trong những quyền thiết yếu của con người, được ghi nhận từ lâu đời. Trong bối cảnh công nghệ hiện đại, quyền tự do ngôn luận được thực hiện trên không gian mạng, có nhiều ảnh hưởng tác động đến cuộc sống xã hội. Trong đó, vấn đề sinh viên và an ninh sinh viên là một trong những đối tượng chịu tác động của quyền tự do ngôn luận trên không gian mạng. Việc hoàn thiện khung pháp lý và nâng cao hiệu quả áp dụng pháp luật về bảo đảm an ninh sinh viên bằng phương pháp giới hạn quyền tự do ngôn luận là cần thiết trong bối cảnh chuyển đổi số hiện nay.

2. Cơ sở lý thuyết

2.1. Khái quát về an ninh sinh viên

“An ninh” là một trong những phạm trù quan trọng nhất trong sự tồn tại của con người và xã hội loài người. Quyền được đảm bảo về sự an toàn của con người như là một “*lẽ phải tự nhiên*”. Hay nói cách khác an ninh sẽ được khái quát như sau: về khách quan là không có sự uy hiếp, về chủ quan là không có sự lo sợ. An ninh là trạng thái ổn định, an toàn, không có dấu hiệu nguy hiểm đe dọa sự tồn tại và phát triển bình thường của cá nhân, tổ chức, của từng lĩnh vực hoạt động xã hội hoặc của toàn xã hội. Trên thực tế, bất kể nhìn từ góc độ nào, an ninh cùng với cảm giác và trạng thái tâm lý của con

người đều không tách rời nhau.⁷¹ Việc gắn “*an ninh*” với các thực thể xã hội khác nhau sẽ là rõ các vấn đề, đặc biệt là đối với sinh viên.

“*An ninh sinh viên*” là một khái niệm liên quan đến việc giáo dục và rèn luyện học sinh, sinh viên về nhận thức về an ninh quốc phòng và trách nhiệm bảo vệ Tổ quốc. Công tác an ninh sinh viên được coi là rất quan trọng và cấp thiết trong tình hình hiện nay. Việc tăng cường giáo dục quốc phòng và an ninh cho học sinh, sinh viên là một trong những chủ trương của Đảng và Nhà nước ta. Công tác này được thực hiện thông qua việc ban hành Luật Giáo dục quốc phòng và an ninh, hệ thống các văn bản quy phạm pháp luật, và được triển khai trong hệ thống giáo dục quốc dân.

Tầm quan trọng của an ninh sinh viên đầu tiên là bảo vệ an ninh quốc gia. Sinh viên được coi là nhân tố trẻ, đầy nhiệt huyết và tiềm năng cho tương lai. Việc rèn luyện an ninh sinh viên giúp họ hiểu rõ trách nhiệm của mình đối với đất nước và sẵn sàng tham gia vào các hoạt động bảo vệ an ninh quốc gia. Bên cạnh đó việc trang bị kiến thức về an ninh quốc phòng cho sinh viên đóng vai trò quan trọng trong việc xây dựng lực lượng nòng cốt bảo vệ an ninh Tổ quốc trong tương lai. Sinh viên có thể trở thành những nhân tài trong các lĩnh vực quốc phòng và an ninh, góp phần vào sự phát triển và mạnh mẽ của quốc gia. Cuối cùng tạo động lực học tập và rèn luyện, an ninh sinh viên không chỉ liên quan đến việc bảo vệ Tổ quốc mà còn đóng vai trò quan trọng trong việc tạo động lực học tập, rèn luyện, tạo môi trường thuận lợi để cho họ phát triển tư duy, kỹ năng và phẩm chất cá nhân cho học sinh, sinh viên. Việc có một môi trường an toàn và ổn định sẽ giúp sinh viên tập trung vào việc học tập và phát triển bản thân.

Tuy nhiên, có nhiều nguyên nhân gây ra tình trạng không an toàn cho sinh viên như thiếu đi sự quản lý, thiếu thông tin hoặc tội phạm,... Hậu quả gây ra nếu không kịp thời phát hiện thì việc đảm bảo an ninh sinh viên sẽ rất khó khăn thậm chí là gây ảnh hưởng về mặt tâm lý và thể chất. Từ đó nên có các biện pháp để nâng cao an ninh sinh viên bao gồm cả các biện pháp phòng ngừa và xử lý khi có vụ việc xảy ra, các giải pháp có thể bao gồm tăng cường quản lý, cung cấp thông tin an ninh cho sinh viên, tăng cường hợp tác với lực lượng an ninh, và nâng cao ý thức an ninh của sinh viên.

Tóm lại, an ninh sinh viên là điều kiện rất quan trọng để đảm bảo một môi trường học tập an toàn, lành mạnh và kích thích phát triển cá nhân của sinh viên. Các biện pháp an ninh phải được áp dụng đồng bộ và sự hợp tác từ tất cả các bên liên quan để đạt được hiệu quả tốt nhất. Đặc biệt trong thời kỳ sự phát triển mạnh mẽ của Internet với nhiều vấn đề cần phải lường trước được.

2.2. Khái quát về giới hạn quyền tự do ngôn luận trên không gian mạng

⁷¹ Trần, V. H., Đỗ, T. B., Lương, T. T. H., Nguyễn, T. T. H. (2020). *An ninh con người trong bối cảnh toàn cầu hóa*. Việt Nam: NXB Chính trị Quốc gia.

2.2.1. Quyền tự do ngôn luận trên không gian mạng

Ngay từ thời Hy Lạp cổ đại, tự do ngôn luận đã được thể hiện bằng việc tham gia các buổi thảo luận chính trị xã hội của công dân Athènes. Sokrates - một triết gia Hy Lạp đã tuyên bố mạnh mẽ quyền tự do ngôn luận trước các vị bồi thẩm đoàn rằng: *“If you offered to let me off this time on condition I am not any longer to speak my mind... I should say to you, “Men of Athenes, I shall obey the Gods rather than you”* (nếu bạn đề nghị tôi rời khỏi đây với điều kiện tôi không được nói lên suy nghĩ của mình, thì, tôi sẽ nói rằng *“Hỡi công dân Athenes, hãy tin vào các vị thần thay vì tin nghe theo bạn”*).

Quyền tự do ngôn luận đã sớm được ghi nhận và được soi chiếu từ nhiều góc độ khác nhau. Dưới góc nhìn của triết học. *“Tự do”* được xem là một giá trị cao quý, cơ bản của nhân loại. Dưới góc độ pháp lý, khái niệm tự do ngôn luận được tìm thấy từ các văn bản pháp luật lâu đời như Bộ luật về quyền của Vương quốc Anh (1689), Tuyên ngôn nhân quyền và dân quyền của Pháp (1789). Quyền tự do ngôn luận được ghi nhận tại Điều 11 Tuyên ngôn nhân quyền và dân quyền của Pháp: *“Trao đổi tự do các ý tưởng và quan niệm là một trong những quyền quý giá nhất của con người”*. Nội dung này được tái khẳng định tại Điều 19 UDHR và Điều 19 ICCPR.

Quyền tự do ngôn luận có thể được hiểu là quyền tự do ngôn luận là một quyền cơ bản của con người, đó là quyền tự do thể hiện ý chí, quan điểm của mình và tự do tìm kiếm, tiếp nhận, truyền đạt thông tin, ý tưởng. của con người được bày tỏ ý kiến một cách công khai, bình đẳng, không bị hạn chế trên cơ sở tôn trọng pháp luật, không xâm phạm đến quyền và lợi ích chính đáng của người khác.

Quyền tự do ngôn luận vừa có tính phổ biến, vừa có tính đặc thù. Mọi người trong xã hội không phân biệt màu da, dân tộc, giới tính, tôn giáo, độ tuổi... đều có quyền tự do ngôn luận. Tuy nhiên, mức độ thụ hưởng quyền còn phụ thuộc vào năng lực cá nhân. Quyền tự do ngôn luận mang tính cá nhân và không thể chuyển nhượng, tùy tiện tước bỏ. Quyền tự do ngôn luận được bảo đảm thực hiện bằng pháp luật quốc gia và các thỏa thuận pháp lý quốc tế.

Cách mạng khoa học công nghệ đã đưa cuộc sống hằng ngày lên không gian mạng. Luật An ninh mạng năm 2018 đã định nghĩa *“Không gian mạng”* là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Không gian mạng có một số đặc điểm sau: (i) không gian mạng có phạm vi toàn cầu, không bị giới hạn về mặt không gian địa lý; (ii) khi tham gia vào không gian mạng, danh tính thực sự của người tham gia bị ẩn đi; (iii) không gian mạng còn có tính “mở” và tính tương tác cao tạo môi trường trao đổi, tiếp cận thông tin cởi mở. Chính không

gian mạng thúc đẩy con người thực hiện các quyền tự do căn bản, trong đó có quyền tự do ngôn luận.

Tóm lại, quyền tự do ngôn luận trên không gian mạng là quyền tự do biểu đạt của con người được thực hiện trên hệ thống trực tuyến mà trong đó có sự liên kết và kết nối giữa các cơ sở hạ tầng công nghệ thông tin như mạng máy tính, mạng internet, mạng viễn thông, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu với nhau trên phạm vi toàn cầu.

2.2.2. Giới hạn quyền tự do ngôn luận trên không gian mạng

Giới hạn quyền con người được ghi nhận trong tuyên ngôn quốc tế nhân quyền và một số Điều ước quốc tế về quyền con người mà bản chất của nó là cho phép các quốc gia thành viên áp đặt một số điều kiện với việc thực hiện/thụ hưởng một số quyền con người nhất định. So với các quyền dân sự - chính trị khác, quyền tự do ngôn luận không phải là quyền tuyệt đối. Quyền này sẽ bị giới hạn trong một số trường hợp nhất định, được pháp luật quốc gia và pháp luật quốc tế ghi nhận.

Việc giới hạn quyền con người xuất phát từ các cơ sở sau: (i) bất cứ điều gì vượt quá giới hạn đều không tốt, ngay cả với quyền con người, quyền công dân. Nếu như tất cả các quyền đều là tuyệt đối thì sẽ không hình thành nên xã hội, không hình thành lên những cộng đồng người. Bản chất con người luôn sống và tồn tại trong tổng hòa các mối liên hệ xã hội⁷²; (ii) giới hạn quyền để không xâm phạm đến quyền của người khác, xâm phạm đến trật tự xã hội. Việc sử dụng quyền tự do ngôn luận để bôi nhọ danh dự người khác sẽ không được chấp nhận. Do đó, vấn đề giới hạn quyền được đặt ra; (iii) giới hạn quyền để bảo hài hòa giữa lợi ích cá nhân và lợi ích của chủ thể khác, lợi ích chung của cộng đồng.

Cần phân biệt giữa khái niệm hạn chế quyền và đình chỉ quyền. Điểm chung giữa hạn chế quyền và đình chỉ quyền đó là lý do được viện dẫn áp dụng cho cả 2 trường hợp là “*an ninh quốc gia*”. Bởi an ninh quốc gia là lý do chung nhất để hạn chế quyền và cũng có thể được xác định là sự kiện đó tác động đến an ninh quốc gia, là đe dọa đến sự sống còn của quốc gia. Điểm khác biệt lớn giữa đình chỉ và hạn chế quyền là, đình chỉ quyền chỉ được áp dụng trong thời gian ngắn – thời gian diễn ra tình trạng khẩn cấp, nên được gọi là “*tạm đình chỉ quyền*”, nhưng hạn chế quyền được thực hiện đồng thời với việc thực thi và hưởng thụ quyền.

Giới hạn quyền tự do ngôn luận được ghi nhận tại khoản 2 Điều 29 UDHR: “*Trong khi hành xử những quyền tự do của mình, ai cũng phải chịu những giới hạn do luật pháp đặt ra ngõ hầu những quyền tự do của người khác cũng được thừa nhận và tôn trọng, những đòi hỏi chính đáng về đạo lý, trật tự công cộng và an lạc chung trong*

⁷² Grégoire, W. C.N. (2009). *The Negotiable Constitution - On the Limitation of Rights*.

một xã hội dân chủ cũng được thỏa mãn”; khoản 3 Điều 19 ICCPR: *“Việc thực hiện những quyền quy định tại khoản 2 điều này kèm theo những nghĩa vụ và trách nhiệm đặc biệt. Do đó, việc này có thể phải chịu một số hạn chế nhất định, tuy nhiên, những hạn chế này phải được quy định trong pháp luật và là cần thiết để: a) Tôn trọng các quyền hoặc uy tín của người khác, b) Bảo vệ an ninh quốc gia hoặc trật tự công cộng, sức khỏe hoặc đạo đức của xã hội.”*

Việc giới hạn quyền tự do ngôn luận nhằm mục đích bảo đảm an ninh quốc gia, trật tự công cộng, sức khỏe cộng đồng, đạo đức cộng đồng, quyền và tự do của người khác. Pháp luật Việt Nam cũng quy định việc giới hạn quyền tại khoản 2 Điều 14 Hiến pháp năm 2013: *“Quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng”*. Quyền tự do ngôn luận trên không gian mạng cũng bị giới hạn dựa trên và nguyên tắc và quy định trên.

3. Phương pháp nghiên cứu

Trong từng nội dung nghiên cứu, các phương pháp được sử dụng một cách linh hoạt, bao gồm:

- Phương pháp phân tích để phân chia nội dung đề tài thành các vấn đề nhỏ để phân tích đánh giá một cách chi tiết và toàn diện các quy định pháp luật về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng.

- Phương pháp tổng hợp nhằm khái quát lên thực trạng pháp luật và thực tiễn áp dụng pháp luật về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng trên cơ sở phân tích, đánh giá những vấn đề chi tiết mà nhóm tác giả phân tích.

- Phương pháp so sánh nhằm đối chiếu giữa Việt Nam với một số quốc gia, khu vực về các quy định pháp luật và thực tiễn áp dụng về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng. Từ đó rút ra kinh nghiệm và có định hướng, giải pháp hoàn thiện pháp luật, nâng cao hiệu quả thực thi pháp luật tại Việt Nam.

4. Kết quả nghiên cứu và thảo luận

4.1. Mối quan hệ giữa an ninh sinh viên và giới hạn quyền tự do ngôn luận

An ninh con người và quyền con người có mối quan hệ mật thiết, tác động và hỗ trợ lẫn nhau. Về bản chất, việc bảo đảm bảy dạng an ninh con người cũng chính là bảo đảm các quyền con người tương ứng. Ngược lại, bảo vệ và thúc đẩy các quyền con người tương ứng cũng chính là nhằm thực hiện, bảo đảm bảy dạng an ninh con người. Thêm vào đó, cả an ninh con người và quyền con người đều hướng vào việc thúc đẩy các nguyên tắc dân chủ và sự phát triển về thể chế trong các xã hội như là những điều kiện

để bảo đảm an ninh và các quyền của con người một cách bền vững⁷³.

Từ những khái quát về an ninh sinh viên và giới hạn quyền tự do biểu đạt trên không gian mạng tại cơ sở lý thuyết. Nhóm tác giả nhận thấy giữa hai đối tượng trên có quan hệ mật thiết, tác động và hỗ trợ lẫn nhau.

Thứ nhất, giới hạn quyền tự do ngôn luận trên không gian mạng là biện pháp bảo đảm an ninh sinh viên trong bối cảnh chuyển đổi số hiện nay.

Công nghệ phát triển dẫn đến việc bùng nổ thông tin. Bên cạnh những quan điểm chính thống, thông tin chính xác thì những luồng thông tin giả, tin xấu độc còn tồn tại. Những tin tức trên có ảnh hưởng đến suy nghĩ, lời nói và hành động của thế hệ trẻ. Do đó, việc hạn chế luồng thông tin xấu độc trên không gian mạng là vô cùng cần thiết nhằm bảo đảm an ninh quốc gia, trật tự công cộng, bảo đảm môi trường mạng xã hội trong lành, thích hợp cho sự phát triển của giới trẻ. Giới hạn quyền với những nguyên tắc chặt chẽ, được pháp điển hóa sẽ là phương pháp hiệu quả trong bối cảnh hiện nay. Những hành vi phát tán, lưu truyền những thông tin xấu độc trên không gian mạng sẽ bị xử lý theo pháp luật về giới hạn quyền tự do ngôn luận.

Thứ hai, bảo đảm an ninh sinh viên cũng là điều kiện để sinh viên có thể thụ hưởng quyền tự do ngôn luận một cách tối đa trên không gian mạng, không bị hạn chế. Khi sinh viên được bảo vệ trước những thông tin xấu độc trên mạng xã hội, những suy nghĩ, lời nói và hành động sẽ trở nên tích cực hơn, phù hợp với chuẩn mực của xã hội. Từ đó, không gian mạng được trong lành, sinh viên có cơ hội bày tỏ quan điểm, tìm kiếm thông tin một cách an toàn.

4.2. Thực trạng pháp luật Việt Nam về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng

4.2.1. Quy định pháp luật

Trong sự nghiệp xây dựng và bảo vệ Tổ quốc, Đảng và Nhà nước Việt Nam luôn xác định việc đảm bảo, thực thi quyền tự do ngôn luận là một trong những giải pháp quan trọng khơi dậy phát huy ý chí, nguyện vọng, tinh thần của mọi tầng lớp nhân dân nhằm thực hiện mục tiêu dân giàu, nước mạnh, dân chủ, công bằng, văn minh. Vì vậy, sự phát triển của xã hội hiện đại bên cạnh về sự phát triển về chính trị, kinh tế, văn hóa,... thì Cách mạng 4.0 thật sự đã làm cho con người có được nhiều thứ không tưởng. Tự do ngôn luận, tự do báo chí có ý nghĩa phát triển đối với từng cá nhân và cộng đồng, được coi là sự bình đẳng, dân chủ thúc đẩy sự phát triển của xã hội đặc điểm đối với thời kỳ công nghệ số với sự phát triển của các loại dịch vụ mạng xã hội thông dụng có thể kể đến như Facebook, Twitter, Youtube, Tik Tok,... Thì giới hạn quyền tự do ngôn

⁷³ Khoa Luật - Đại học Quốc gia Hà Nội. (2011). *Giáo trình Lý luận và Pháp luật về Quyền con người*. Hà Nội: NXB Đại học Quốc gia Hà Nội.

luận trên không gian mạng ngày càng được quan tâm.

Hiến pháp năm 2013

Văn bản có giá trị pháp lý cao nhất là Hiến pháp quy định như sau về quyền tự do ngôn luận của công dân tại Điều 25:

“Công dân có quyền tự do ngôn luận, tự do báo chí, tiếp cận thông tin, hội họp, lập hội, biểu tình. Việc thực hiện các quyền này do pháp luật quy định”.

Điều 14 Hiến pháp quy định quyền con người, quyền và nghĩa vụ cơ bản của công dân, trong đó nhấn mạnh:

“1. Ở nước Cộng hòa xã hội chủ nghĩa Việt Nam, các quyền con người, quyền công dân về chính trị, kinh tế, văn hóa, xã hội được công nhận, tôn trọng, bảo vệ, đảm bảo theo Hiến pháp và pháp luật.

2. Quyền con người, quyền công dân chỉ có thể bị hạn chế theo quy định của luật trong trường hợp cần thiết vì lý do quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội, đạo đức xã hội, sức khỏe của cộng đồng”.

Có thể thấy rằng, các mệnh đề chung giới hạn quyền, mặc dù được diễn đạt khác nhau trong các điều ước quốc tế và các hiến pháp, về cơ bản thể hiện ba triết lý. Thứ nhất, nguyên tắc này ghi nhận sự xung đột giữa quyền của người này với quyền của người khác cũng như với lợi ích chung của toàn xã hội. Đây là điều không thể tránh khỏi vì bảo vệ phạm vi tự do chính đáng của người này cũng chính là sự giới hạn tự do của người khác. Thứ hai, việc giới hạn quyền được thực hiện thông các quy phạm pháp luật dưới hiến pháp. Thứ ba, nguyên tắc này đòi hỏi đảm bảo tính cân xứng giữa quyền bị hạn chế với bảo vệ quyền của người khác và lợi ích chung. Tính cân xứng được đảm bảo cũng có nghĩa là biện pháp giới hạn quyền mang tính hợp hiến.⁷⁴

Hay Điều 21 Hiến pháp quy định:

“1. Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình; có quyền bảo vệ danh dự, uy tín của mình. Thông tin về đời sống riêng tư, bí mật cá nhân, bí mật gia đình được pháp luật bảo đảm an toàn.

2. Mọi người có quyền bí mật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư khác.

Không ai được bóc mở, kiểm soát, thu giữ trái luật thư tín, điện thoại, điện tín và các hình thức trao đổi thông tin riêng tư của người khác.”

Theo đó, Hiến pháp đã đảm bảo rằng mọi người có quyền tự do diễn đạt ý kiến, truyền thông và tiếp cận thông tin một cách tự do và công bằng. Tuy nhiên, việc thực

⁷⁴ Bùi, Đ. T. (2015, March 1). *Hiến pháp hóa nguyên tắc giới hạn quyền con người: Cần nhưng chưa đủ*. Tạp chí nghiên cứu lập pháp. Retrieved September 13, 2023, from <http://www.lappphap.vn/Pages/TinTuc/208344/Hien-phap-hoa-nguyen-tac-gioi-han-quyen-con-nguoi--Can-nhung-chua-du.html>

hiện các quyền này cần tuân thủ các quy định pháp luật và không được lạm dụng để gây hại đến lợi ích của quốc gia và cộng đồng.

Luật An ninh mạng năm 2018

Điều 8 quy định các hành vi bị nghiêm cấm về an ninh mạng

“1. Sử dụng không gian mạng để thực hiện các hành vi sau đây:

a) Hành vi quy định tại khoản 1 Điều 18 của Luật này;

b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội.

6. Các hành vi khác theo quy định của Luật này.

Điều 9 quy định về xử lý vi phạm pháp luật về an ninh mạng như sau

“Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử lý vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự, nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật”.

Như vậy, Luật An ninh mạng năm 2018 không cấm người tham gia mạng xã hội lên tiếng, có điều những người sử dụng mạng xã hội phải luôn tuân thủ theo Hiến pháp và pháp luật. Họ hoàn toàn có thể bày tỏ tự do chính kiến, quan điểm của cá nhân; nhưng không được lợi dụng điều đó để xuyên tạc, chống phá Đảng và Nhà nước, kích động lôi kéo gây rối, bôi nhọ xúc phạm danh dự người khác... Nếu vi phạm các hành vi trên thì sẽ có những biện pháp để xử phạt nghiêm chỉnh (xử phạt về vi phạm hành chính hoặc truy cứu trách nhiệm hình sự hay phải bồi thường thiệt hại về vật chất và tinh thần).

Luật báo chí năm 2016

Điều 9 các hành vi bị nghiêm cấm quy định tại các khoản 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13. Có mô tả hành vi chi tiết bị cấm đặc biệt ở đây có thể nói đến báo điện tử, các loại sản phẩm báo chí trên Internet dễ dàng tiếp cận rất nhiều người dùng đặc biệt đối với những thế hệ trẻ, sinh viên cần biết và nên tuân thủ các quy định của nhà trường và pháp luật để tránh những hậu quả khôn lường gây nguy hại cho bản thân và cho xã hội.

Ngoài các loại văn bản Luật trên thì bên cạnh đó còn có những loại văn bản khác như Bộ luật Hình sự năm 2015, Nghị định số 72/2013/NĐ-CP được sửa đổi bổ sung một

số điều tại Nghị định 72/2018/NĐ-CP... Cũng quy định về các hành vi, mức xử phạt theo quy định của pháp luật.

Vì vậy, việc giới hạn quyền tự do ngôn luận trên không gian mạng cần được thực hiện một cách hợp pháp và công bằng, đồng thời phải đảm bảo quyền lợi và sự phát triển của sinh viên. Việc áp dụng các biện pháp giới hạn quyền tự do ngôn luận trên không gian mạng cần được thực hiện theo quy định của pháp luật và phải đảm bảo tính hợp lý, công bằng, và không gây ảnh hưởng tiêu cực đến quyền tự do ngôn luận và quyền lợi của sinh viên.

4.2.2. Thực tiễn áp dụng

Trong bối cảnh vấn đề về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng càng nhận được sự quan tâm của các nhà luật học cũng như của toàn xã hội thì việc áp dụng giới hạn quyền tự do ngôn luận trên không gian mạng đã và đang được thực hiện trên thực tế đảm bảo quyền và lợi ích bị xâm phạm điển hình như vụ án của Nguyễn Lê Tuấn Tài (Sinh năm 2004, quê Đồng Nai) vào ngày 26-7, sau thời gian xét xử, Tòa án Quân sự Quân khu 7 đã tuyên phạt bị cáo Nguyễn Lê Tấn Tài mức án 12 tháng cải tạo không giam giữ về tội “Đưa trái phép thông tin mạng máy tính” theo quy định tại điểm a khoản 1 Điều 288; điểm b, i, s khoản 1 và khoản 2 Điều 51, Điều 36 Bộ luật Hình sự., thời điểm xảy ra hành vi phạm tội là sinh viên năm thứ nhất của Trường Đại học Kinh tế TP Hồ Chí Minh. Theo cáo trạng, khoảng 0 giờ 30 phút ngày 11-1-2023, mặc dù không biết nội dung vụ việc, chưa kiểm chứng nhưng bị cáo Nguyễn Lê Tấn Tài sử dụng máy tính xách tay của mình trực tiếp duyệt, chỉnh sửa bài viết do người không rõ lai lịch gửi đến, có nội dung bịa đặt, sai sự thật, rằng tại Trường Quân sự Quân khu 7 xảy ra vụ hiếp dâm nữ sinh viên học giáo dục quốc phòng an ninh vào lúc 22 giờ 30 phút ngày 10-1-2023 tại Đại đội 6, Tiểu đoàn 3, Trung tâm Giáo dục Quốc phòng và An ninh (Trường Quân sự Quân khu 7) và nhiều vụ việc hiếp dâm trước đây. Tài đã đăng tải bài viết bịa đặt này trên trang fanpage: UEH Confessions (bị cáo Tài là một trong các quản trị viên) vào lúc 19 giờ ngày 11-1-2023. Bài viết đã có hàng trăm nghìn lượt tương tác, chia sẻ, bình luận, gây hoang mang dư luận. Trong phần luận tội, đại diện Viện Kiểm sát Quân sự Quân khu 7 cho rằng: Nguyễn Lê Tấn Tài là sinh viên đại học, có trình độ năng lực về công nghệ thông tin, hiểu biết về mạng xã hội, tự nguyện tham gia làm quản trị viên của fanpage: UEH Confessions không có tính chất vụ lợi, không được trả công, phải có trách nhiệm trong hoạt động trên không gian mạng internet và các nền tảng mạng xã hội, phải đảm bảo đúng theo quy định pháp luật nói chung, cùng các tiêu chí do ban quản trị của trang fanpage này đưa ra: “Không đăng tải các bài liên quan đến việc đả kích, bêu rếu, xúc phạm trực tiếp hoặc gián tiếp đến tôn giáo và kích động các vấn đề chính trị”. Tuy nhiên, trong quá trình duyệt bài viết trên, bị cáo đã không kiểm chứng nội dung, đăng tải công khai thông tin có yếu tố nhạy cảm,

nhiều từ ngữ có tính chất xúc phạm nghiêm trọng liên quan trực tiếp đến Trường Quân sự Quân khu 7. Bị cáo đăng bài với mục đích đăng tải thông tin cộng đồng những việc đăng tin bài này không đúng sự thật, có tính chất bịa đặt. Hành vi phạm tội do bị cáo Nguyễn Lê Tấn Tài thực hiện đã gây ra hậu quả nghiêm trọng trong việc tổn hại uy tín của một nhà trường quân đội, gián tiếp xúc phạm đến các quân nhân đang học tập, công tác tại trường. Hành vi này đã trực tiếp xâm phạm đến quy định về quản lý môi trường mạng, làm giảm uy tín của tổ chức, cụ thể là Trường Quân sự Quân khu 7, gây ảnh hưởng xấu đến tình hình an ninh chính trị, uy tín của quân đội. Bị cáo là người có đầy đủ năng lực trách nhiệm hình sự, vì vậy bị cáo phải chịu trách nhiệm hình sự về hành vi phạm tội và những thiệt hại đã xảy ra⁷⁵. Và nhiều trường hợp khác trên thực tế đã và đang được xử lý.

Tuy nhiên trong nhiều trường hợp các đơn vị thực thi còn khó khăn khi quyết định hình thức xử lý, nhiều trường hợp không dám công khai biện pháp xử lý do có yếu tố nhạy cảm, nên chưa đề cao tính răn đe. Công tác thanh tra, kiểm tra và xử lý sai phạm tuy đã được tăng cường năng lực bộ máy thanh tra, kiểm tra, xử lý vi phạm còn hạn chế, rất thiếu về số lượng thanh tra chuyên ngành; năng lực kỹ thuật xử lý, ngăn chặn thông tin sai phạm từ các máy chủ đặt tại nước ngoài còn nhiều bất cập, trong khi các biện pháp ngăn chặn kỹ thuật mới chỉ tập trung đối với những thông tin sai phạm về an ninh chính trị, còn đối với những sai phạm thông tin khác không có điều kiện quan tâm đúng mức. Ngoài ra, pháp luật cũng chưa đủ sức răn đe đối với một số hành vi ảnh hưởng tới quyền tự do ngôn luận của người dân. Cụ thể là trong Bộ luật Hình sự chưa có một quy định cụ thể nào có thể giải quyết được những phát sinh gần đây như vấn nạn tin giả, tin rác, các xâm phạm giải trí gây phiền nhiễu cho dùng internet. Đối với vấn nạn tin giả, chủ thể rất có thể nhầm lẫn (hoặc cố tình nhầm lẫn) với quyền giữ quan điểm – là một quyền tuyệt đối, không bị hạn chế hay tước bỏ trong mọi hoàn cảnh. Trong khi các quyền tự do ngôn luận có những giới hạn nhất định theo luật. Những hành vi này đang gây ra tác hại xấu cho xã hội ảnh hưởng nghiêm trọng đến đời sống riêng tư, danh dự, nhân phẩm, uy tín của cá nhân, tổ chức, gây ra những tổn thất về vật chất, tinh thần cho cá nhân, pháp nhân, tổ chức. Trong điều kiện xây dựng Nhà nước pháp quyền xã hội chủ nghĩa của nhân dân, do nhân dân, vì nhân dân, lấy việc tôn trọng, bảo vệ quyền con người là trung tâm của mọi hoạt động, nhất là trong quá trình tiến hành cách mạng công nghiệp lần thứ 4 thì tính nguy hiểm của các hành vi phát tán, truyền bá thông tin giả trên internet; hành vi phát tán tin rác trên internet; hành vi phát tán trò chơi giải trí gây phiền nhiễu cho người sử dụng internet ở mức độ nguy hại cao cho xã hội cần phải xử lý bằng

⁷⁵ Vụ án đưa thông tin thất thiệt về Trường Quân sự Quân khu 7 Tuyên phạt Nguyễn Lê Tấn Tài mức án 12 tháng cải tạo không giam giữ. Retrieved September 13, 2023, from <https://www.qdnd.vn/phap-luat/tin-tuc/tuyen-phat-nguyen-le-tan-tai-muc-an-12-thang-cai-tao-khong-giam-giu-736237>.

biện pháp hình sự.⁷⁶

4.3. Kinh nghiệm pháp luật của một số quốc gia về an ninh sinh viên từ góc độ giới hạn quyền tự do ngôn luận trên không gian mạng

4.3.1. Kinh nghiệm pháp luật của Trung Quốc

Trung Quốc là quốc gia châu Á có nét tương đồng về văn hóa và chế độ chính trị với Việt Nam. Do đó, Việt Nam có thể nghiên cứu và áp dụng các quy định về giới hạn quyền tự do ngôn luận trên không gian mạng nhằm bảo đảm an ninh cho sinh viên. Quyền tự do ngôn luận được Trung Quốc ghi nhận tại Điều 35 và Điều 51 Hiến pháp nước Cộng hòa nhân dân Trung Hoa.

Năm 2022, tỷ lệ tuyển sinh trung cấp trung học phổ thông là 91,6%, cao hơn năm trước 0,2 điểm phần trăm. Cả nước có 15.000 trường trung học phổ thông chính quy, tăng 441 trường so với năm trước. Tổng số học sinh mới đăng ký vào các trường này là 9.475.400, tăng 4,71% so với năm trước và số học sinh đăng ký lên tới 27.138.700, tăng 4,18% so với năm trước. Cả nước có 7.201 trường trung cấp nghề, giảm 93 trường so với năm trước. Số sinh viên mới tuyển sinh năm 2022 là 4.847.800, giảm 0,86% so với năm trước. Số học sinh đăng ký học các trường trung cấp nghề đạt tổng cộng 13.392.900, tăng 2,09% so với năm trước⁷⁷. Trung Quốc có số lượng sinh viên đông đảo, bao gồm cả sinh viên trong nước và sinh viên quốc tế. Do đó, việc bảo đảm an ninh sinh viên trong bối cảnh mạng xã hội phát triển như hiện nay luôn được chú trọng.

Chính sách của Chính phủ Trung Quốc đối với mạng internet là kiểm soát rất chặt chẽ về thông tin, cũng như sự phát triển các trang mạng và dịch vụ trong nước và ngăn cản sự thâm nhập của các trang mạng nước ngoài. Trung Quốc đã ban hành 03 văn bản pháp luật về sử dụng internet: (i) Quy chế tạm thời về việc quản lý thông tin mạng máy tính kết nối quốc tế, trong đó quy định “*Không một đơn vị hoặc cá nhân nào được phép tự tạo những kết nối quốc tế trực tiếp. Tất cả những kết nối trực tiếp với internet phải thông qua bốn nhà cung cấp mạng chính của Trung Quốc là: ChinaNet, GBNet, CERNET và CTSNET*”; (ii) Pháp lệnh về bảo vệ an ninh của các hệ thống thông tin máy tính, trong đó quy định việc “*giám sát, kiểm tra và hướng dẫn công tác bảo vệ an ninh*” và “*điều tra và truy tố các trường hợp phạm pháp*”; (iii) Pháp lệnh quy định về thông tin độc hại trên internet, trong đó định nghĩa “*thông tin độc hại*” và chỉ ra 5 loại hoạt động có hại liên quan đến việc sử dụng internet.

Chính phủ Trung Quốc xác định việc quản lý internet với ba cấp độ, trong đó ở

⁷⁶ Nguyễn Minh Vọng (2019), “Quyền tự do ngôn luận trên Internet trong pháp luật và thực tiễn Việt Nam”, Luận văn Thạc sĩ Luật học, Trường Đại học Luật - Đại học Quốc Gia Hà Nội, Hà Nội.

⁷⁷ *Statistical report on China's educational achievements in 2022*. (2023, April 2). Ministry of Education of the People's Republic of China. Retrieved September 13, 2023, from http://en.moe.gov.cn/documents/reports/202304/t20230403_1054100.html

cấp độ một là quản lý các mạng chủ và các nhà cung cấp dịch vụ mạng. Về vấn đề này, một trong những kế hoạch quan trọng là “*Dự án Trường thành lửa*”, được Bộ Công an Trung Quốc khởi xướng vào năm 1988 và đưa vào sử dụng từ tháng 1/2003. Hệ thống này hoạt động dựa trên một số nguyên tắc cơ bản như khóa địa chỉ IP, lọc và dẫn đến một tên miền mới, lọc URL, lọc gói tin và xác lập lại kết nối. Hệ thống này khiến cho không chỉ mạng xã hội mà rất nhiều công ty về internet nổi tiếng thế giới ở Mỹ và phương Tây thất bại khi thâm nhập thị trường rộng lớn này do chính sách kiểm duyệt thông tin trên internet gắt gao của Chính phủ Trung Quốc. Những người dùng internet thông thường ở Trung Quốc hiện tại bị chặn không cho truy cập vào nhiều trang web và dịch vụ web nước ngoài.

Luật An ninh mạng tại Trung Quốc điều chỉnh các hoạt động thành lập, duy trì, sử dụng, quản lý kiểm soát mạng tại Trung Quốc. Bên cạnh đó nhiều văn bản pháp luật các cùng điều chỉnh như: Bộ luật hình sự, Bộ luật dân sự Luật Trừng phạt hành chính... Mục đích của việc giới hạn quyền tự do ngôn luận trên không gian mạng nhằm bảo đảm an ninh quốc gia, trật tự công cộng, bảo vệ quyền và lợi ích hợp của người khác trước những hành vi lợi dụng quyền tự do ngôn luận để xâm hại. Tuy nhiên, các lý do an ninh quốc gia, trật tự công cộng, đạo đức xã hội thường được nêu ra nhưng nội hàm các lý do trên chưa được giải thích một cách rõ ràng.

Việt Nam có vận dụng một số quy định như: thừa nhận quyền này là quyền cơ bản của công dân trong Hiến pháp, ghi nhận các giới hạn của quyền này, có quy định cụ thể về “*thông tin độc hại*”, có cơ quan kiểm soát riêng về vấn đề thông tin trên mạng internet... Tuy nhiên, Việt Nam cũng cần tránh các khung pháp lý quá khắt khe như hạn chế các ứng dụng mạng xã hội nước ngoài hoạt động trong nước như tại Trung Quốc.

4.3.2. Kinh nghiệm pháp luật của Vương quốc Anh

Vương quốc Anh là một quốc gia quân chủ lập hiến ở khu vực châu Âu. Là một đất nước không có Hiến pháp thành văn, quyền tự do ngôn luận tại Anh được ghi nhận tại Luật về quyền (Bill of rights) năm 1689 trước khi Đạo luật Nhân quyền năm 1998 ra đời. Điều 10 đạo luật Nhân quyền năm 1998 là sự thể chế hóa ECHR. Tương tự như ECHR, mục đích giới hạn quyền tự do biểu đạt bao gồm: an ninh quốc gia, toàn vẹn lãnh thổ, an toàn công cộng, ngăn ngừa mất trật tự hay tội phạm, bảo vệ sức khỏe hay đạo đức, bảo vệ nhân phẩm hay quyền của người khác, ngăn ngừa công bố thông tin mật, duy trì tính tôn nghiêm và công tâm của tư pháp.

Dữ liệu cho thấy tổng số 2.862.620 sinh viên đăng ký vào năm học 2021-2022, tăng 4% so với năm học 2020-2021. 1.288.160 sinh viên đang theo học năm đầu tiên của khóa học. 526.645 (41%) trong số những sinh viên này đang bắt đầu khóa học sau đại học, tăng 9% so với năm trước. Số lượng sinh viên bắt đầu khóa học đại học giảm

2%⁷⁸. Số lượng sinh viên tại Anh là vô cùng lớn, có cả số lượng sinh viên quốc tế nên việc bảo đảm an ninh sinh viên được quan tâm thực hiện trong bối cảnh chuyển đổi số hiện nay. Đặc biệt, quyền tự do ngôn luận còn được quy định tại khía cạnh giáo dục. Đạo luật Giáo dục năm 1986 quy định rằng mỗi cá nhân tập thể liên quan đến giáo dục phải thực hiện các biện pháp hợp lý nhằm bảo đảm tự do ngôn luận được bảo vệ trong phạm vi pháp luật đối với người sử dụng và có liên hệ với các cơ sở giáo dục.

Nước Anh không có Bộ luật hình sự như các quốc gia khác, các quy định về hình sự thường nằm rải rác ở các đạo luật của Nghị viện, án lệ của Tòa án. Quyền tự do ngôn luận phải tuân theo một loạt hạn chế trong luật pháp Vương quốc Anh, bao gồm: Đạo luật Truyền thông Độc hại 1988 và Đạo luật Truyền thông 2003, hình sự hóa các tin nhắn và mối đe dọa “không đứng đắn hoặc xúc phạm nặng nề”; Đạo luật Trật tự Công cộng 1986, bao gồm các tội kích động hận thù vì lý do chủng tộc, tôn giáo hoặc phân biệt giới tính; Đạo luật Khủng bố 2006, hình sự hóa việc xuất bản và phổ biến tài liệu có thể được coi là khuyến khích hành động khủng bố.

Pháp luật về quyền tự do ngôn luận tại các nước châu Âu được xem là chuẩn mực để Việt Nam có thể nghiên cứu, vận dụng. Việt Nam cần rà soát, áp dụng kinh nghiệm của pháp luật nước Anh ở các khía cạnh: tiêu chuẩn rõ ràng cho các phát ngôn thù địch, kích động, phỉ báng, bôi nhọ và các hình thức biểu đạt khác.

5. Kết luận & Gợi ý

5.1. Gợi ý giải pháp

Từ thực trạng pháp luật tại mục 4.2. và kinh nghiệm pháp luật của một số quốc gia tại mục 4.3., nhóm tác giả đề xuất một số giải pháp hoàn thiện quy định pháp luật tại Việt Nam như sau:

Thứ nhất, hoàn thiện quy định pháp luật về giới hạn quyền tự do ngôn luận trên không gian mạng. Làm rõ nội hàm của các lý do giới hạn quyền vào quy định pháp luật để tránh trường hợp lạm dụng, vi phạm dẫn đến xâm phạm quyền tự do biểu đạt trên không gian mạng.

Thứ hai, tăng giáo dục, tuyên truyền pháp luật, đa dạng về hình thức, phong phú về nội dung nhằm nâng cao trách nhiệm của sinh viên khi tham gia mạng xã hội cảnh giác trước những thông tin, phát ngôn giả mạo, xấu độc gây ảnh hưởng tiêu cực đến suy nghĩ, lời nói và hành động của giới trẻ.

Thứ ba, thường xuyên các nghiên cứu, khảo sát về thói quen sử dụng mạng xã hội của sinh viên từ đó có những điều chỉnh về mặt pháp lý, áp dụng kịp thời các biện pháp giáo dục để bảo đảm an ninh sinh viên trên không gian mạng.

⁷⁸ *Higher Education Student Statistics: UK 2021/22 released.* (2023, January 19). HESA. Retrieved September 13, 2023, from <https://www.hesa.ac.uk/news/19-01-2023/higher-education-student-statistics-uk-202122-released>

Thứ tư, tạo ra các ứng dụng xã hội dành riêng cho sinh viên để kịp thời thông tin những quy định pháp luật, thực tiễn áp dụng, các vụ việc về giới hạn quyền tự do ngôn luận nhằm bảo đảm an ninh sinh viên.

Thứ năm, xây dựng đội ngũ sinh viên về an toàn, an ninh mạng và thông tin mạng quốc gia có khả năng làm chủ công nghệ, hạn chế và tiến tới không phụ thuộc vào công nghệ và thiết bị của nước ngoài.

5.2. Kết luận

Cuộc sống được đưa dần lên không gian mạng nhờ vào sự phát triển của khoa học công nghệ. Bên cạnh những mặt tích cực thì tồn tại những yếu tố tác động tiêu cực đến an ninh sinh viên. Bằng phương pháp phân tích, tổng hợp và so sánh, nhóm tác giả tiến hành đánh giá mức độ hoàn thiện của pháp luật và hiệu quả áp dụng so với thực tiễn tại Việt Nam, kinh nghiệm pháp luật của Trung Quốc và Vương quốc Anh. Từ đó, nhóm tác giả đề xuất các giải pháp nhằm hoàn thiện hệ thống quy định, nâng cao hiệu quả áp dụng pháp luật trong việc bảo đảm an ninh sinh viên từ góc nhìn giới hạn quyền tự do ngôn luận trên không gian mạng./.

Tài liệu tham khảo

1. Sách/ báo cáo (bản in):

- Trần, V. H., Đỗ, T. B., Lương, T. T. H., Nguyễn, T. T. H. (2020). *An ninh con người trong bối cảnh toàn cầu hóa*. Việt Nam: NXB Chính trị Quốc gia.
- Grégoire, W. C.N. (2009). *The Negotiable Constitution - On the Limitation of Rights*. Khoa Luật - Đại học Quốc gia Hà Nội. (2011). *Giáo trình Lý luận và Pháp luật về Quyền con người*. Hà Nội: NXB Đại học Quốc gia Hà Nội.

2. Sách/ báo cáo (bản online):

- Mạc, T. T. H. (2020). *Quyền tự do ngôn luận theo pháp luật quốc tế và pháp luật một số quốc gia - Một số giá trị cho Việt Nam* [Đề tài nghiên cứu khoa học cấp trường].
- Statistical report on China's educational achievements in 2022*. (2023, April 2). Ministry of Education of the People's Republic of China. Retrieved September 13, 2023, from http://en.moe.gov.cn/documents/reports/202304/t20230403_1054100.html
- Higher Education Student Statistics: UK 2021/22 released*. (2023, January 19). HESA. Retrieved September 13, 2023, from <https://www.hesa.ac.uk/news/19-01-2023/higher-education-student-statistics-uk-202122-released>

3. Tạp chí (bản online):

- Bùi, Đ. T. (2015, March 1). *Hiến pháp hóa nguyên tắc giới hạn quyền con người: Cần nhưng chưa đủ*. Tạp chí nghiên cứu lập pháp. Retrieved September 13, 2023, from <http://www.lapthap.vn/Pages/TinTuc/208344/Hien-phap-hoa-nguyen-tac-gioi-han-quyen-con-nguoi--Can-nhung-chua-du.html>

**PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA
SINH VIÊN TẠI VIỆT NAM - ĐỐI CHIẾU VỚI PHÁP LUẬT
CỦA LIÊN MINH CHÂU ÂU EU (GDPR)**

**LEGAL REGULATIONS ON PERSONAL DATA
PROTECTION OF STUDENTS IN VIETNAM – A
COMPARATIVE ANALYSIS WITH THE LEGAL
PERSPECTIVE OF THE EUROPEAN UNION (GDPR)**

Nguyễn Tiến Đạt*, Hà Thảo Trâm

Trường Đại học Sài Gòn

*Tác giả liên hệ: tiendatsgu2023@gmail.com

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> dữ liệu cá nhân, an ninh sinh viên, xâm phạm dữ liệu, pháp luật liên minh Châu Âu EU, nền tảng số.	Dữ liệu cá nhân là vấn đề được quan tâm đặc biệt trong thời kỳ hội nhập, chuyển đổi số, cách mạng công nghiệp 4.0 đối với con người trong thời kỳ hiện đại nói chung và sinh viên nói riêng. Bài viết nghiên cứu các thực trạng về vấn đề xâm phạm bảo mật dữ liệu cá nhân của sinh viên tại Việt Nam thông qua phương pháp phân tích bản án, nhằm làm sáng tỏ các hành vi xâm phạm dữ liệu cá nhân và áp dụng quy định pháp luật đối với thực trạng trên. Từ đó, đưa ra các nhận xét, đánh giá về tình hình pháp luật tại Việt Nam. Ngoài ra, bài viết cũng nghiên cứu các công trình trong nước và quốc tế để đưa ra các kinh nghiệm học tập cần thiết cho Việt Nam hoàn thiện hệ thống pháp luật, thông qua đối chiếu pháp luật liên minh Châu Âu EU (GDPR)
<i>Keywords:</i> personal data, students' protection, data invasion, digital platform, GDPR.	ABSTRACT Personal data is a matter of particular concern in the era of globalization, digital transformation, and the Fourth Industrial Revolution, affecting people in general and students in particular in modern times. This research article investigates the realities of personal data security breaches protection, data invasion, concerning Vietnamese students. It employs a case analysis method to shed light on these breaches, apply legal regulations, and provide insights into the legal landscape in Vietnam. Additionally, it studies domestic and international literature to extract essential lessons for Vietnam to enhance its legal system, drawing comparisons with the European Union's General Data Protection Regulation (GDPR).

1. Giới thiệu

Việc sử dụng công nghệ số ở các lĩnh vực trong xã hội đang ngày một gia tăng trên khắp thế giới trong vài thập kỷ qua. Cho dù ở dạng thiết bị điện toán cho nội dung phân phối, ứng dụng học tập trực tuyến, lưu trữ đám mây, hệ thống đào tạo và đánh giá giáo dục, giải trí... đã trở thành một phần không thể thiếu trong nhiều hoạt động. Đặc biệt, sự xuất hiện của các ứng dụng mạng xã hội đã giúp cho cuộc sống trở nên thuận tiện, nhanh chóng hơn bao giờ hết. Song song đó, việc bùng nổ các ứng dụng mạng xã hội cũng mang lại những tác động tiêu cực đến xã hội, đặc biệt là sinh viên - đối tượng dành nhiều thời gian cho việc sử dụng mạng xã hội cho các hoạt động trong cuộc sống. Điều này, đẩy lên vấn đề an ninh sinh viên về bảo mật dữ liệu thông tin cá nhân trong nền tảng số. Vì vậy, pháp luật với vai trò là một công cụ điều chỉnh sẽ phải có những giải pháp hoàn thiện giúp khắc phục các lỗ hổng đang còn tồn tại. Bài viết đề cập đến ba khía cạnh chính gồm: lý luận về vấn đề bảo vệ dữ liệu cá nhân của sinh viên, thực trạng bảo vệ dữ liệu tại Việt Nam, kinh nghiệm học tập từ quốc tế.

2. Cơ sở lý thuyết

Hiện nay, vấn đề bảo vệ dữ liệu cho sinh viên chưa nhận được nhiều sự quan tâm và bảo vệ một cách toàn diện tại Việt Nam. Tuy nhiên, vẫn có một số bài báo nhắc đến vấn đề bảo vệ dữ liệu có thể kể đến như:

Bài viết *Bảo vệ dữ liệu cá nhân trong bối cảnh cách mạng công nghiệp 4.0* của TS. Nguyễn Thị Thu Vân trong tạp chí Dân chủ & Pháp luật số 10 (307) - 2017. Bài viết này mô tả sơ lược một số thách thức đối với các nhà làm luật trong việc bảo vệ dữ liệu cá nhân trước bối cảnh phát triển một số xu hướng công nghệ lớn trên thế giới và ở Việt Nam hiện nay.

Bài viết *Bảo vệ quyền đối với dữ liệu cá nhân trong pháp luật quốc tế*, pháp luật ở một số quốc gia và giá trị tham khảo cho việt nam của PGS.TS Vũ Công Giao, khoa Luật, Đại học Quốc gia Hà Nội và Th.S Lê Trần Như Tuyên, khoa Luật, Đại học Quốc gia Hà Nội, tạp chí xuất bản Số 9(409) - T5/2020. Bài viết này phân tích sự tác động của kỹ thuật số đến quyền đối với dữ liệu cá nhân; đánh giá các quy định của pháp luật quốc tế và pháp luật ở một số quốc gia về việc bảo vệ quyền này trong bối cảnh mới và nêu ra một số giá trị mà Việt Nam có thể tham khảo.

Bài viết *Securing higher education against cyberthreats: from an institutional risk to a national policy challenge* của Noran Shafik Fouad xuất bản ngày 11/12/2021. Bài viết này đã nghiên cứu vấn đề xâm phạm dữ liệu cá nhân trên không gian mạng với đối tượng là các sinh viên đại học. Ngoài ra, bài báo đã đưa ra thực trạng và thống kê các vụ việc xâm phạm dữ liệu xảy ra trong thời kỳ Covid 19, đưa ra những giải pháp về mặt chính sách để giảm thiểu việc dữ liệu cá nhân của sinh viên bị xâm phạm.

Các bài viết trong nước và quốc tế đã có đề cập đến vấn đề bảo mật dữ liệu cá nhân cho sinh viên dưới góc độ chính sách nhưng chưa đề cập đến khía cạnh pháp lý. Vì vậy, bài viết này sẽ kết hợp giữa hai góc độ chính sách và pháp luật nhằm đưa ra các giải pháp khắc phục điểm hạn chế trong pháp luật Việt Nam thông qua việc nghiên cứu, học hỏi kinh nghiệm từ các nước phát triển.

3. Phương pháp nghiên cứu

Trong quá trình nghiên cứu, nhóm chúng tôi đã sử dụng các phương pháp sau: phương pháp phân tích, tổng hợp; phương pháp thu thập thông tin, tài liệu; phương pháp nghiên cứu tình huống. Từ đó chọn lọc, sắp xếp, thống kê tài liệu đi đến phân tích, tổng hợp rút ra các nhận định cần thiết để làm rõ thêm nội dung cần truyền tải.

4. Kết quả nghiên cứu và thảo luận

4.1. Bảo vệ dữ liệu sinh viên trong cách mạng công nghiệp 4.0

a) Dữ liệu cá nhân của sinh viên

Theo định nghĩa cơ bản dữ liệu cá nhân (personal data) là bất cứ thông tin nào liên quan đến dữ liệu của một người hay còn gọi là một chủ thể dữ liệu.

GDPR cho rằng dữ liệu được phân loại thành “dữ liệu cá nhân” một cá nhân có thể được nhận diện trực tiếp hoặc gián tiếp, bằng cách sử dụng những số nhận dạng trực tuyến như tên, số căn cước công dân, địa chỉ IP, hoặc là dữ liệu định vị của họ.^[1]

Tại Việt Nam, dữ liệu cá nhân được quy định trong khoản 1 điều 2 Nghị định số 13/2023-NĐ-CP ngày 17/4/2023 của Chính phủ quy định: “*dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.*”

b) Bảo vệ dữ liệu cá nhân

Theo Khoản 5 Điều 2 [Nghị định số 13/2023/NĐ-CP](#) ngày 17/4/2023 của Chính phủ về bảo vệ dữ liệu cá nhân quy định: “*Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật*”.

4.2. Thực trạng xâm phạm dữ liệu cá nhân của sinh viên hiện nay

Bản án thực tế: Bản án số: 08/2020/HS-ST Ngày 17/01/2020^[2] Vụ án này xoay quanh một hành vi phạm tội sử dụng mạng máy tính và mạng viễn thông để thực hiện các hoạt động lừa đảo và chiếm đoạt tài sản. Cụ thể, vào cuối tháng 02 đầu tháng 3 năm 2019, Lê Văn L, do cần tiền chi tiêu, đã tìm cách hack vào tài khoản Facebook cá nhân để giả danh người thân và yêu cầu chuyển tiền vào tài khoản ngân hàng nhằm chiếm đoạt tài sản. Vì L không có tài khoản ngân hàng nên đã hợp tác với Lê Văn Duy C để tìm người có tài khoản để nhận tiền sau khi hack thành công.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Lê Văn L sau đó được thông báo rằng đã có người liên lạc được với một du học sinh tên Phan Tiến A (bạn của Lê Văn Duy C) để lấy số tài khoản ngân hàng. Họ thống nhất ăn chia số tiền chiếm đoạt theo tỷ lệ 20% và 80%.

Lê Văn L tiếp tục hành động của mình bằng cách hack vào tài khoản Facebook của một du học sinh Nhật Bản có tên Đỗ Thị Lan Hương. Anh ta thu thập thông tin cá nhân của chị Hương, bao gồm ngày tháng năm sinh, địa chỉ và số điện thoại, sau đó đoán ra mật khẩu để truy cập vào tài khoản Facebook của chị Hương.

Sử dụng tài khoản của chị Hương, Lê Văn L nhắn tin đến các người thân của chị Hương, bà Hoàng Thị L1 và bà Đỗ Thị Thúy, yêu cầu họ chuyển tiền vào tài khoản ngân hàng mang tên Ngô Văn H, do Phan Tiến A đã cung cấp. Họ đã chuyển tổng cộng 70 triệu đồng vào tài khoản này sau khi bị lừa đảo.

Sau khi nhận được tiền, Lê Văn L và Phan Tiến A tiếp tục chuyển tiền từ tài khoản này sang các tài khoản khác và rút tiền mặt. Tổng cộng, họ đã chiếm đoạt được 56 triệu đồng.

Sau khi hành vi của họ bị phát hiện, Lê Văn L đã đầu thú tại cơ quan an ninh điều tra. Cả hai bị cáo đã thừa nhận hành vi phạm tội của mình, và phiên tòa đã xem xét giảm nhẹ hình phạt dựa trên các yếu tố khác nhau.

Viện kiểm sát đã đề nghị xử phạt Lê Văn L từ 30 đến 36 tháng tù và xử phạt Phan Tiến A từ 24 đến 30 tháng tù, cùng với trách nhiệm dân sự để trả lại số tiền đã chiếm đoạt cho bị hại. Cả hai bị cáo đã đề nghị giảm nhẹ hình phạt.

Tòa án quyết định tuyên bố các bị cáo Lê Văn L và Phan Tiến A phạm tội “Sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản”. Áp dụng điểm b, đ khoản 2 Điều 290, điểm b, s khoản 1, khoản 2 Điều 51; Điều 56; Điều 58; Điều 38 Bộ luật hình sự; khoản 1 Điều 329 Bộ luật tố tụng hình sự, tổng hợp hình phạt với bản án số: 12/2019/HS-ST ngày 30/8/2019 của Tòa án nhân dân huyện T, tỉnh Quảng Trị buộc Lê Văn L phải chấp hành chung hình phạt của hai bản án là 48 tháng tù. Áp dụng điểm b, đ khoản 2 Điều 290, điểm b, s khoản 1, khoản 2 Điều 51; Điều 58; Điều 38 Bộ luật hình sự: Xử phạt bị cáo Phan Tiến A 30 tháng tù. Áp dụng Điều 47, 48 Bộ luật hình sự; Điều 106 Bộ luật tố tụng hình sự: Buộc bị cáo Lê Văn L và Phan Tiến A phải liên đới bồi thường cho bà Hoàng Thị L1 40.000.000 đồng, bà Đỗ Thị Thúy 30.000.000 đồng. Đồng thời tịch thu một số hiện vật khác có liên quan.

Bản án trên chính là một ví dụ minh họa điển hình cho việc bị xâm phạm dữ liệu cá nhân trên nền tảng mạng xã hội của sinh viên. Vụ việc trên đã gây phương hại trực tiếp đến tinh thần, cuộc sống của nạn nhân - cụ thể chị Hương (một du học sinh tại Nhật) và những người xung quanh.

Từ thực tiễn xét xử, Tòa án đã áp dụng điểm b, đ khoản 2 Điều 290, điểm b, s khoản 1, khoản 2 Điều 51, Điều 56, Điều 58, khoản 1 Điều 329 Bộ luật tố tụng hình sự;

điểm b, d khoản 2 Điều 290, điểm b, s khoản 1, khoản 2 Điều 51; Điều 58; Điều 38 Bộ luật hình sự để xử lý hành vi của Lê Văn L và Phan Tiến A phạm tội sử dụng mạng máy tính và mạng viễn thông để thực hiện các hoạt động lừa đảo và chiếm đoạt tài sản.

Qua đó có thể thấy, pháp luật Việt Nam đang ngày một hoàn thiện và khắc khe hơn trong việc bảo vệ dữ liệu cá nhân của người dùng trên mạng xã hội đặc biệt với đối tượng là sinh viên. Những quy phạm pháp luật chặt chẽ về xử lý hành vi xâm phạm dữ liệu cá nhân đã được ban hành ở những ngành luật riêng. Cụ thể, pháp luật hình sự đã tham gia vào việc bảo vệ dữ liệu cá nhân bằng cách cụ thể hóa tội phạm về các hành vi xâm hại đến dữ liệu cá nhân về tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu cá nhân trong môi trường số.

Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 quy định về bảo vệ dữ liệu cá nhân và trách nhiệm bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan. Tại Điều 4 Nghị định 13/2023/NĐ-CP quy định về xử lý vi phạm quy định bảo vệ dữ liệu cá nhân: “*Cơ quan, tổ chức, cá nhân vi phạm quy định bảo vệ dữ liệu cá nhân tùy theo mức độ có thể bị xử lý kỷ luật, xử phạt vi phạm hành chính, xử lý hình sự theo quy định.*” Như vậy, theo quy định trên thì đối với hành vi vi phạm về dữ liệu cá nhân sẽ có các hình thức xử lý khác nhau tùy theo tính chất và mức độ vi phạm mà tổ chức, cá nhân thực hiện hành vi vi phạm về dữ liệu cá nhân sẽ có hình thức xử lý tương ứng..

4.3. Quy định pháp luật quốc tế

Ở cấp độ toàn cầu, các quy định về bảo vệ quyền về sự riêng tư có thể được tìm thấy trong Tuyên ngôn Nhân quyền phổ quát năm 1948 (UDHR)^[3], trong đó có Điều 12 về bảo vệ quyền về sự riêng tư. Từ nội dung Điều 12 UDHR, có thể thấy nội hàm của các giá trị riêng tư cần được bảo vệ không chỉ là cuộc sống riêng tư của mỗi cá nhân, mà còn bao gồm cả những khía cạnh đời sống có sự gắn kết mật thiết với cá nhân, cụ thể như gia đình, nơi ở, thư tín và cả những giá trị định tính như danh dự, uy tín cá nhân...

Tiếp theo UDHR, nhiều công ước quốc tế về quyền con người cũng công nhận quyền về sự riêng tư như một quyền cơ bản, cụ thể như: Công ước quốc tế về các quyền dân sự và chính trị (ICCPR)^[4] (Điều 17); Công ước về quyền của người lao động nhập cư (Điều 14); Công ước về quyền trẻ em (Điều 16); Công ước về quyền của người khuyết tật (Điều 22) ...

Dù vậy, sự phát triển của công nghệ trong cuộc Cách mạng công nghiệp 4.0 mà đi kèm với nó là tiềm năng giám sát ngày càng tinh vi của các hệ thống máy tính đã đặt ra những yêu cầu mới với bảo vệ dữ liệu của cá nhân. Để đáp ứng yêu cầu này, có hai công cụ pháp lý quốc tế đã được phát triển, trong đó đặt ra một số quy tắc cụ thể chi phối việc thu thập và xử lý dữ liệu cá nhân, bao gồm: Công ước năm 1981 của Hội đồng châu Âu về bảo vệ cá nhân liên quan đến việc xử lý dữ liệu cá nhân tự động và Hướng

dẫn của Tổ chức Hợp tác và Phát triển Kinh tế (OECD)^[5] điều chỉnh việc bảo vệ quyền về sự riêng tư và việc chuyển đổi dữ liệu nêu cơ bản là tương đồng, chỉ khác nhau ở mức độ, theo đó tất cả đều yêu cầu đối với thông tin cá nhân thì: i) Chỉ có thể được thu thập một cách công bằng và hợp pháp; ii) Chỉ được sử dụng cho mục đích ban đầu được biết rõ; iii) Bảo đảm tính đầy đủ, phù hợp và không vượt quá mục đích; iv) Bảo đảm tính chính xác và cập nhật; và v) Phải được loại bỏ sau khi mục đích sử dụng đã hoàn thành. Hai văn kiện nêu trên đã có tác động sâu sắc đến việc xây dựng và áp dụng luật pháp về bảo vệ dữ liệu cá nhân trên toàn thế giới, không giới hạn ở các nước châu Âu và các quốc gia thành viên của OECD.

Tuy nhiên, có thể nói rằng, luật pháp quốc tế hiện nay vẫn còn tương đối tụt hậu so với sự phát triển như vũ bão của công nghệ. Điều này đã khiến cho việc bảo vệ quyền đối với dữ liệu cá nhân của con người trong thực tế còn rất khó khăn. Tính đến thời điểm hiện nay, vẫn chưa có điều ước quốc tế toàn cầu nào về bảo vệ quyền đối với dữ liệu cá nhân. Hai văn kiện về bảo vệ dữ liệu cá nhân đã nêu trên (Công ước của Hội đồng châu Âu năm 1981 và Hướng dẫn của OECD) về nguyên tắc chỉ có tác động trong khu vực châu Âu và với các nước thành viên của OECD. Không chỉ vậy, Bản hướng dẫn của OECD chỉ có tính chất khuyến nghị, không có hiệu lực pháp lý ràng buộc.

a) Pháp luật của châu Âu và Hoa Kỳ về bảo vệ quyền đối với dữ liệu cá nhân

Đứng trước yêu cầu bảo vệ quyền về sự riêng tư trước tốc độ phát triển chóng mặt của công nghệ thông tin, nhiều khu vực và quốc gia đã củng cố khung pháp luật về vấn đề này. Mặc dù vậy, mỗi khu vực và quốc gia có những cách thức bảo vệ dữ liệu riêng tư khác nhau. Một số khu vực và quốc gia đã xây dựng thành công một cơ chế bảo vệ dữ liệu riêng tư mạnh mẽ thông qua luật pháp, trong khi nhiều khu vực và quốc gia khác mới đang lên kế hoạch xây dựng pháp luật về vấn đề này.

Luật bảo vệ dữ liệu cá nhân ở châu Âu Quyền về sự riêng tư là một phần của Công ước châu Âu về quyền con người năm 1950, trong đó tuyên bố, mọi người đều có quyền được tôn trọng riêng tư và cuộc sống gia đình, nhà ở và thư từ. Từ cơ sở đó, các nước trong Liên minh châu Âu (EU) đã tìm cách đảm bảo quyền này thông qua việc xây dựng một văn bản pháp luật chung, đặc biệt khi Internet xuất hiện. Vào năm 1995, EU đã thông qua Chỉ thị về bảo vệ dữ liệu châu Âu (95/46/EC), trong đó thiết lập các tiêu chuẩn bảo mật và riêng tư dữ liệu tối thiểu để các quốc gia thành viên thực thi bằng cách đưa vào pháp luật của nước mình. Tuy nhiên, Chỉ thị năm 1995 được soạn thảo vào giai đoạn khi Internet mới chỉ được sử dụng bởi 1% dân số thế giới. Vì vậy, khi Internet bùng nổ, xuất hiện yêu cầu phải có văn bản pháp luật mới để giải quyết các vấn đề nảy sinh về bảo vệ dữ liệu cá nhân từ việc sử dụng Internet và các thiết bị thông minh trên quy mô lớn. Đây là lý do dẫn đến sự ra đời của Quy định chung về bảo vệ dữ liệu (GDPR)^[6] do Ủy ban châu Âu xây dựng, với mục đích vạch ra kế hoạch cải cách bảo vệ

dữ liệu cá nhân trên toàn Liên minh châu Âu. Về bản chất, GDPR là một bộ quy tắc mới, được xây dựng nhằm cung cấp cho công dân EU quyền kiểm soát nhiều hơn đối với dữ liệu cá nhân của họ. Theo các điều khoản của GDPR, không chỉ các tổ chức phải đảm bảo dữ liệu cá nhân được thu thập hợp pháp và trong các điều kiện nghiêm ngặt, mà tất cả những bên thu thập và quản lý dữ liệu có nghĩa vụ bảo vệ dữ liệu khỏi việc bị lạm dụng và khai thác, cũng như tôn trọng quyền của chủ sở hữu dữ liệu. Tiền phạt đối với hành vi trái với quy định của GDPR rất cao. Theo đó có hai cách thức phạt, có thể tối đa là 20 triệu Euro hoặc 4% doanh thu toàn cầu (tùy theo mức nào cao hơn), cộng với việc các chủ thể dữ liệu có quyền yêu cầu bồi thường thiệt hại.

GDPR cũng là một bước tiến pháp lý lớn về xác định dữ liệu cá nhân. Dữ liệu cá nhân và dữ liệu cá nhân nhạy cảm là hai khái niệm nền tảng của GDPR. Dữ liệu cá nhân được định nghĩa là “bất kỳ thông tin nào liên quan đến một thể nhân (‘data subject’) đã được nhận định danh tính, hoặc có thể được nhận định danh tính, dù trực tiếp hay gián tiếp, cụ thể là bằng cách chỉ ra một định danh như tên, số định danh, dữ liệu vị trí, định danh trên mạng, hay một hoặc nhiều yếu tố chỉ định danh tính của một cá nhân mang tính vật lý, sinh lý, di truyền, tâm lý, kinh tế, văn hoá, hoặc xã hội”. Định nghĩa này khá tương đồng với định nghĩa được đưa ra trong Chỉ thị năm 1995 của EU, nhưng có sự mở rộng hơn, bao gồm cả “địa chỉ IP” hay “giả danh tính” (pseudonymisation). Dữ liệu cá nhân nhạy cảm được quy định dưới dạng hạng mục dữ liệu cá nhân đặc biệt trong GDPR, được xem là: “Bất kỳ dữ liệu nào tiết lộ chủng tộc hoặc sắc tộc, tư tưởng chính trị, đức tin tôn giáo, quan niệm triết lý, thành viên công đoàn, và việc xử lý dữ liệu di truyền và sinh trắc nhằm mục đích định danh, hoặc dữ liệu liên quan đến sức khỏe, tình trạng sinh dục, và xu hướng tính dục”.

Việc xử lý và phân tích các dữ liệu nhạy cảm hoàn toàn bị cấm bởi GDPR. Một số trường hợp ngoại lệ cho phép xử lý dữ liệu cá nhân nhạy cảm, bao gồm có sự đồng thuận từ chủ thể dữ liệu, để bảo vệ quyền lợi cá nhân, để phục vụ công tác y tế dự phòng và y tế nghiệp vụ, hoặc vì lợi ích công cộng. Xét trên những điều kiện đó, việc Facebook hoặc Google cùng các đối tác kinh doanh thu thập và xử lý các dữ liệu cá nhân nhạy cảm có khả năng vi phạm GDPR rất cao. Trong những tình huống vi phạm, GDPR cho phép các cá nhân có quyền nộp đơn khiếu nại đến Cơ quan Quản lý Dữ liệu đặt tại các quốc gia thành viên nơi cá nhân đang làm việc hoặc sinh sống, hoặc nơi việc vi phạm đã diễn ra. Các cá nhân sau khi được thẩm định quyền bị xâm hại sẽ được xử lý đền bù theo quyết định của Cơ quan Quản lý Dữ liệu, theo tinh thần của những quyết định đưa ra bởi Hội đồng Bảo vệ Dữ liệu châu Âu (EDPB)^[7]. Tính đến tháng 5/2019, khoản tiền phạt lớn nhất áp dụng theo GDPR là 50 triệu Euro. Ví dụ, Cơ quan giám sát bảo vệ dữ liệu của Pháp (CNIL)^[8], đã quyết định án phạt cho Google vào tháng 1/2019 sau khi đi đến kết luận rằng gã khổng lồ công cụ tìm kiếm này đã phá vỡ các quy tắc của GDPR

về tính minh bạch và cơ sở pháp lý hợp lệ khi xử lý dữ liệu của mọi người cho mục đích quảng cáo.

GDPR thiết lập 7 nguyên tắc cần tuân thủ khi xử lý dữ liệu: 1) Tính hợp pháp, công bằng và minh bạch: Việc xử lý dữ liệu phải hợp pháp, công bằng và minh bạch đối với chủ thể dữ liệu; 2) Giới hạn mục đích: Mục đích xử lý dữ liệu phải hợp pháp và được thể hiện rõ ràng cho chủ thể dữ liệu khi thu thập; 3) Giảm thiểu dữ liệu: Chỉ thu thập và xử lý dữ liệu khi thực sự cần thiết cho các mục đích đã định; 4) Độ chính xác: Phải bảo đảm dữ liệu cá nhân là chính xác và cập nhật; 5) Giới hạn lưu trữ: Chỉ lưu trữ dữ liệu nhận dạng cá nhân trong thời gian cần thiết cho mục đích đã định; 6) Tính toàn vẹn và bảo mật: Việc xử lý dữ liệu phải được thực hiện trên cơ sở đảm bảo tính bảo mật, tính toàn vẹn và bảo mật thích hợp (ví dụ: bằng cách sử dụng mã hóa); 7) Trách nhiệm giải trình: Người kiểm soát dữ liệu có trách nhiệm chứng minh sự tuân thủ GDPR với tất cả các nguyên tắc này. GDPR cũng quy định “quyền được lãng quên” - cụ thể là quyền xóa dữ liệu cho những người muốn xóa dữ liệu cá nhân của họ khi không còn căn cứ để lưu giữ dữ liệu đó. GDPR được áp dụng ở cấp độ trong nước với hiệu lực ngay lập tức, bắt đầu từ ngày nó có hiệu lực và việc áp dụng luật quốc gia sẽ không ảnh hưởng đến hiệu lực của nó. Tuy nhiên, GDPR cho phép các quốc gia thành viên sự linh hoạt đến một mức độ nhất định khi áp dụng một số quy định. Trong thực tế, các nước thành viên EU đã sửa đổi luật bảo vệ dữ liệu của họ để tuân thủ các yêu cầu GDPR. Ví dụ, Pháp đã điều chỉnh luật pháp nước mình theo GDPR với việc ban hành Luật số 2018-493 (FDPA)^[9] ngày 20/6/2018 về bảo vệ dữ liệu cá nhân, trong đó thay thế logic của các thủ tục trước đó (thông báo hoặc ủy quyền trước bởi CNIL) dựa trên triết lý về trách nhiệm giải trình nâng cao của các bên liên quan trong GDPR. Nước Anh cũng đã thông qua Luật Bảo vệ dữ liệu quốc gia mới (DPA)^[10] có hiệu lực vào ngày 25/5/2018, trong đó cho phép tiếp tục áp dụng GDPR kể cả khi nước này rời Liên minh châu Âu. DPA chuyển đổi Chỉ thị thực thi pháp luật ((EU) 2016/680) thành luật pháp của Vương quốc Anh, tạo ra một chế độ bảo vệ dữ liệu dành riêng cho việc xử lý dữ liệu cá nhân của cơ quan thực thi pháp luật, trong đó Phần 4 của DPA cập nhật chế độ bảo vệ dữ liệu để xử lý an ninh quốc gia; các Phần 5 và 6 đưa ra phạm vi nhiệm vụ và quyền hạn của Ủy viên Thông tin, đồng thời quy định một số tội hình sự liên quan đến xử lý dữ liệu cá nhân.

b) Luật Bảo vệ dữ liệu cá nhân ở Hoa Kỳ

Cho đến nay, Hoa Kỳ chưa có bất kỳ đạo luật riêng nào ở cấp liên bang về bảo vệ dữ liệu cá nhân, song vấn đề này đã được nêu trong nhiều văn bản pháp luật ban hành theo từng ngành, từng đối tượng. Ví dụ: Luật Bảo vệ quyền về sự riêng tư trực tuyến của trẻ em (COPPA)^[11] - cung cấp cho phụ huynh quyền kiểm soát đối với những thông tin mà các trang web có thể thu thập từ con cái họ; Luật về Trách nhiệm giải trình và trách nhiệm bảo hiểm y tế (HIPPA)^[12] - đảm bảo tính bảo mật của bệnh nhân đối với tất cả các dữ liệu liên quan đến

chăm sóc sức khỏe; Luật Bảo vệ quyền về sự riêng tư video - ngăn chặn việc tiết lộ sai thông tin của một cá nhân xuất phát từ việc cho thuê hoặc mua tài liệu nghe nhìn của họ... Theo cách tiếp cận của Hoa Kỳ, việc bảo vệ dữ liệu và quyền về sự riêng tư được dựa trên sự kết hợp giữa luật pháp, quy định và tự điều chỉnh, thay vì chỉ có sự can thiệp của nhà nước. Pháp luật thường chỉ được áp dụng cho các tình huống trong đó các cá nhân không thể tự kiểm soát việc sử dụng dữ liệu cá nhân của họ.

Sau khi GDPR được thông qua, một số tiểu bang của Hoa Kỳ đã đề xuất luật bảo vệ dữ liệu của riêng họ, thiết lập một số quyền giống như GDPR. Luật về Sự riêng tư của người tiêu dùng của bang California (CCPA)^[13] được thông qua vào tháng 6/2018 sau vụ bê bối Cambridge Analytica, dự kiến sẽ trở thành luật về quyền về sự riêng tư dữ liệu toàn diện nhất ở Hoa Kỳ. Giống như GDPR, văn bản luật này thiết lập một số quyền nhất định cho người tiêu dùng, bao gồm “quyền được biết”, “quyền được tiếp cận”, “quyền từ chối” và “quyền xóa bỏ”. Ngoài ra, CCPA mở rộng đáng kể định nghĩa về thông tin cá nhân, từ đó đòi hỏi các công ty phải có những thay đổi đáng kể trong cách thức hoạt động của mình. Văn bản luật này, không giống như bất kỳ luật bảo vệ dữ liệu nào được ban hành trước đây ở Hoa Kỳ, yêu cầu có một lựa chọn trên trang web của công ty để cho phép người tiêu dùng từ chối chia sẻ dữ liệu cho bên thứ ba. Văn bản luật này cũng cho phép quyền hành động riêng tư trong trường hợp vi phạm dữ liệu và cho phép Bộ trưởng Tư pháp California áp dụng các hình phạt hành chính lên tới 7.500 đô la cho mỗi lần vi phạm mà không có giới hạn tối đa.

Không chỉ California, 11 bang khác của Hoa Kỳ bao gồm Maryland, New Jersey và Washington... gần đây đã đưa ra dự thảo văn bản pháp luật tương tự. Những dự luật này có các phiên bản riêng về quyền từ chối và các yêu cầu công bố mà khác một chút so với GDPR và CCPA. Nếu được ban hành, các luật này sẽ dẫn đến tăng chi phí đáng kể cho các doanh nghiệp khi phải cố gắng hiểu và đưa ra một khung bảo mật tuân thủ các quy định của luật. Trên thực tế, mức độ phức tạp và không chắc chắn do những thay đổi về khung pháp lý đang khiến các doanh nghiệp kêu gọi Quốc hội Hoa Kỳ ban hành và thực thi luật bảo mật dữ liệu cá nhân áp dụng cho toàn quốc. Đáp ứng lời kêu gọi đó, Quốc hội Hoa Kỳ đã đưa ra một số dự luật về quyền về sự riêng tư dữ liệu để thực hiện tiêu chuẩn bảo mật dữ liệu liên bang tại Hoa Kỳ. Ví dụ, Luật Phổ biến Dữ liệu Hoa Kỳ (S. 142) sẽ áp đặt các yêu cầu về quyền về sự riêng tư đối với các nhà cung cấp dịch vụ Internet tương tự như các yêu cầu áp đặt cho các cơ quan Liên bang theo Luật về quyền về sự riêng tư năm 1974. Luật bảo vệ quyền về sự riêng tư và quyền lợi người tiêu dùng trên phương tiện truyền thông xã hội năm 2019 (S. 189), sẽ yêu cầu các chủ thể: 1) cung cấp cho người dùng một bản sao miễn phí dưới dạng điện tử những dữ liệu cá nhân mà nhà điều hành đã xử lý và 2) thông báo cho người dùng trong vòng 72 giờ sau khi biết rằng dữ liệu của người dùng đã bị truyền đi mà vi phạm nền tảng bảo mật

5. Kết luận và gợi ý

Từ thực trạng pháp luật trong nước, đối chiếu với các quy định trong pháp luật của châu Âu và Hoa Kỳ, có thể gợi mở một số giải pháp nhằm hoàn thiện pháp luật về quyền được bảo vệ bí mật dữ liệu cá nhân ở nước ta như sau:

Thứ nhất, xây dựng một văn bản pháp luật riêng bảo vệ dữ liệu cá nhân. Như đã đề cập, trước bối cảnh Cách mạng công nghiệp 4.0, ở châu Âu đã có văn bản pháp luật chung của EU và nhiều nước trong khu vực đã ban hành văn bản pháp luật riêng bảo vệ quyền về sự riêng tư, đặc biệt là bảo vệ dữ liệu cá nhân. Hoa Kỳ cũng đang xây dựng những đạo luật liên bang riêng về vấn đề này. Trong khi đó, quy định về bảo vệ quyền về dữ liệu cá nhân ở Việt Nam hiện vẫn nằm rải rác ở nhiều văn bản pháp luật khác nhau, dẫn đến tình trạng vừa chồng chéo, vừa thiếu thống nhất và khó khăn cho việc áp dụng pháp luật. Vì thế, Nhà nước cần nghiên cứu xây dựng, ban hành một văn bản pháp luật riêng để bảo vệ dữ liệu cá nhân, trong đó quy định đầy đủ các khái niệm, nguyên tắc, thể chế và thiết chế bảo vệ dữ liệu riêng tư của con người. Luật bảo vệ dữ liệu cá nhân cũng cần quy định rõ những giới hạn của quyền, những điều kiện và hạn chế đặt ra với việc khai thác, sử dụng, phổ biến dữ liệu cá nhân, quy định về cơ quan chuyên trách theo dõi, giám sát, giải quyết các khiếu nại, tố cáo về quyền này trên thực tế.

Thứ hai, sửa đổi, bổ sung các quy định về bảo mật thông tin/dữ liệu trong các luật chuyên ngành như Luật Công nghệ thông tin, Luật An toàn thông tin mạng, Luật An ninh mạng...

Như đã đề cập, các quy định về vấn đề này trong pháp luật của châu Âu và Hoa Kỳ rất cụ thể và chặt chẽ, trong khi các văn bản pháp luật của Việt Nam mới chỉ dừng lại ở mức quy định nguyên tắc chung nên hiệu quả áp dụng trong thực tế thấp. Vì vậy, việc sửa đổi, bổ sung các quy định về vấn đề này là rất cần thiết.

Thứ ba, sửa đổi, bổ sung các quy định về chế tài với những hành vi vi phạm. Như đã phân tích, chế tài xử phạt vi phạm quyền về sự riêng tư nói chung và dữ liệu riêng tư nói riêng tại Việt Nam hiện quá thấp so với chế tài ở châu Âu và các quốc gia khác, chưa tương xứng với mức độ nghiêm trọng của hành vi vi phạm, chưa đảm bảo tính răn đe. Vì vậy, Nhà nước cần sửa đổi các văn bản pháp luật có liên quan để quy định những hình thức chế tài nghiêm khắc hơn, đặc biệt là về hành chính và dân sự, với các cơ quan, tổ chức, doanh nghiệp và cá nhân vi phạm quyền về dữ liệu riêng tư.

Thứ tư, bảo đảm nghĩa vụ tôn trọng, bảo vệ và thúc đẩy quyền về sự riêng tư. Như đã phân tích ở các phần trên, quyền về sự riêng tư là quyền con người cơ bản, có ý nghĩa rất quan trọng, được công nhận và bảo vệ bởi luật nhân quyền quốc tế và pháp luật của hầu hết quốc gia. Sự phát triển của công nghệ đã cải thiện đáng kể đời sống của con người, song cũng là một nguy cơ lớn với quyền về sự riêng tư, do công nghệ có thể

trở thành công cụ để nhiều chủ thể, trong đó có nhà nước, giám sát và can thiệp vào đời sống riêng tư của con người.

Ở Việt Nam, quyền riêng tư được bảo vệ bởi Hiến pháp và nhiều luật chuyên ngành, song trong thực tế sự bảo vệ của Nhà nước với quyền này còn thiếu hiệu quả, những nỗ lực đã được thực hiện chưa tương xứng với tầm quan trọng của nó. Đặc biệt, Luật An ninh mạng hiện còn có những lỗ hổng tiềm ẩn khả năng cơ quan nhà nước tùy tiện can thiệp vào đời tư thông qua việc thu thập dữ liệu riêng tư của cá nhân. Vì vậy, trong thời gian tới, Nhà nước cần tiếp tục xây dựng, hoàn thiện hệ thống pháp luật để thúc đẩy và bảo vệ hiệu quả hơn quyền về sự riêng tư nói chung, quyền về dữ liệu cá nhân nói riêng theo đúng tinh thần của Hiến pháp năm 2013 và các điều ước quốc tế mà Việt Nam đã tham gia.

LỜI CẢM ƠN

Nhóm tác giả xin trân trọng gửi lời cảm ơn đến các tác giả, nhà khoa học đã cho phép chúng tôi được sử dụng nguồn tài liệu vô cùng quý giá này. Với toàn bộ sự chân thành, nhóm tác giả sẽ cố gắng sử dụng một cách thông minh giúp phát huy giá trị của các đề tài nghiên cứu đã tham khảo, góp phần xây dựng hệ thống pháp luật Việt Nam ngày càng hiện đại và chặt chẽ.

Tài liệu tham khảo

- Amber Pariona, “What Was the Digital Revolution?”, 2017, <https://www.worldatlas.com/articles/what-was-the-digital-revolution.html>.
- European Commission, “What is personal data?”, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.
- Cẩm Thi, “Tràn lan tình trạng mua bán thông tin cá nhân”, 2018, <https://kiemsat.vn/tran-lan-tinh-trang-mua-ban-thong-tin-ca-nhan-50866.html>.
- Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Stasbourg, 1981.
- Chính phủ, Dự thảo Nghị định quy định chi tiết một số điều của Luật an ninh mạng, 31/10/2018.
6. Danny Palmer, “What is GDPR? Everything you need to know about the new general data protection regulations”, 2019, <https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/>.
- Global Internet liberty campaign, “Privacy and human rights - An International Survey of Privacy Laws and Practice”, 2004, <http://gilc.org/privacy/survey/intro.html>.
- HG.org, Data Protection Law, <https://www.hg.org/data-protection.html>.
- Hoàng Thị Ngọc Lan, “Những thành tựu cơ bản của các cuộc cách mạng công nghiệp trong lịch sử thế giới”, 2019, http://vtex.edu.vn/index.php?option=com_content&view=article&id=995:nh-ng

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

thanh-t-u-co-b-n-c-a-cac-cu-c-cach-m-ng-cong-nghi-p-trong-l-ch-s-th-gi-i&catid=93&Itemid=492.

John Rose, Christine Barton & Rob Souza, “The Trust Advantage: How to Win with Big Data”, Boston Consulting Group, 2013,
<https://www.bcg.com/publications/2013/marketing-sales-trust-advantage-win-with-big-data.aspx>.

OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data, Paris, 1981.

Chu Hồng Thanh, “Nhận thức pháp lý về quyền riêng tư”, trong Quyền về sự riêng tư, Nxb. Chính trị quốc gia sự thật, Hà Nội, 2018.

Richard Hodson, “Digital revolution: An explosion in information technology is remaking the world, leaving few aspects of society untouched”, 2018,
<https://www.nature.com/articles/d41586-018-07500-z>.

RMIT University, “what is Industry 4.0?”, <https://www.rmit.edu.au/industry/develop-your-workforce/tailored-workforcesolutions/c4de/industry-40>.

Ủy ban Nhân quyền, Bình luận chung số 16 về quyền về sự riêng tư, 1988

[GDPR personal data – what information does this cover? \(gdpreu.org\)](#). Truy cập ngày 14/9/2023.

[Bản án số: 08/2020/HS-ST ngày 17/01/2020 về tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản](#) của Tòa án nhân dân tỉnh Bắc Giang. Truy cập ngày 10/9/2023.

Tuyên ngôn thế giới về quyền con người (tiếng Anh: *Universal Declaration of Human Rights*, viết tắt: UDHR).

Công ước quốc tế về các quyền dân sự và chính trị (tiếng Anh: *International Covenant on Civil and Political Rights*, viết tắt: ICCPR).

Tổ chức Hợp tác và Phát triển Kinh tế ([tiếng Anh](#): *Organization for Economic Cooperation and Development*; viết tắt: OECD).

Quy định chung về bảo vệ dữ liệu cá nhân (tiếng Anh: *General Data Protection Regulation*, viết tắt: GDPR). Có hiệu lực từ ngày 25/5/2018.

Hội đồng Bảo vệ Dữ liệu châu Âu (tiếng Anh: *European Data Protection Board*, viết tắt: EDPB). Thành lập ngày 25/5/2018.

Cơ quan giám sát bảo vệ dữ liệu của Pháp (tiếng Anh: *Commission nationale de l'informatique et des libertés*, viết tắt: CNIL).

Được viết tắt từ *Federal Data Protection Act* (Chương trình hành động bảo vệ dữ liệu chung)

Luật Bảo vệ dữ liệu quốc gia tại Anh (tiếng Anh: *Data Protection Act*, viết tắt: DPA).

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Luật Bảo vệ quyền về sự riêng tư trực tuyến của trẻ em (tiếng Anh: *Children's Online Privacy Protection Act*, viết tắt: COPPA).

Luật về Trách nhiệm giải trình và trách nhiệm bảo hiểm y tế (tiếng Anh: *Federal Health Insurance Portability and Accountability Act*, viết tắt: HIPPA).

Luật về Sự riêng tư của người tiêu dùng của bang California (tiếng Anh: *California Consumer Privacy Act*, viết tắt: CCPA).

QUẢN LÝ ĐÀO TẠO TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ TẠI CÁC TRƯỜNG ĐẠI HỌC

Nguyễn Thị Mỹ Hạnh

Đại học Kinh tế TP. Hồ Chí Minh

Email: hanhnguyen.31211027446@st.ueh.edu.vn

Phone number: 0943972527

THÔNG TIN	TÓM TẮT
Từ khóa: Chuyển đổi số, quản lý giáo dục, kỹ thuật máy học, khai thác dữ liệu	Bài viết thể hiện tính cấp thiết về chuyển đổi số trong giáo dục và quản lý giáo dục, trong đó lĩnh vực khai thác dữ liệu phục vụ quản lý đào tạo ở các trường đại học là vấn đề trọng tâm được đề xuất. Thông qua phân tích chuyên sâu về tính cấp thiết của nhu cầu chuyển đổi số trong giáo dục và quản lý giáo dục, thực tế của một số mô hình quản lý đào tạo trong bối cảnh chuyển đổi số hiện nay và phân tích tổng quan các nghiên cứu về ứng dụng kỹ thuật máy học (machine learning techniques) trong xử lý dữ liệu và trong quản lý giáo dục, chúng tôi đề xuất một số giải pháp tổ chức chuyển đổi số và khai thác dữ liệu trong quản lý đào tạo của một trường đại học ở Việt Nam trong giai đoạn hiện nay.

Giới thiệu

Ngày nay nhân loại đã bước vào một kỷ nguyên mới của sự sáng tạo dựa trên công nghệ. Cách mạng công nghiệp 4.0 được định hình không thể tách rời với dữ liệu và phân tích dữ liệu, đặt ra thách thức cho các tổ chức (bao gồm cả trường đại học) trong việc xử lý dữ liệu nhằm nâng cao hiệu quả, năng lực hoạt động và giảm thiểu rủi ro. Đối với hoạt động đào tạo và quản lý đào tạo, dữ liệu được coi là tài sản, là một phần cốt lõi của hoạt động chiến lược, mang lại giá trị lớn trong quản lý trường đại học và tăng khả năng cạnh tranh. Đặc điểm của dữ liệu trong thời đại số là khối lượng rất lớn, cấu trúc phức tạp, thay đổi nhanh nên các kỹ thuật phải được phát triển hơn nữa để đáp ứng nhu cầu phân tích dữ liệu mới, chuyển đổi dữ liệu thành thông tin và tiếp tục chuyển đổi thông tin thành các hoạt động, chiến lược trợ giúp. Lãnh đạo nhà trường đưa ra những quyết định quan trọng trong công tác quản lý đào tạo, giúp sinh viên xây dựng chiến lược học tập tối ưu, góp phần quan trọng nâng cao chất lượng và hiệu quả đào tạo.

Quản lý và điều hành hoạt động đào tạo là một trong những hoạt động quan trọng nhất của trường đại học. Trước đây, các hoạt động đào tạo chủ yếu được quản lý thủ công. Thông tin được lưu trữ trên giấy (bản cứng), gây nhiều khó khăn, bất lợi cho công

tác quản lý, điều hành, đặc biệt trong thời đại công nghệ hiện nay, đồng thời, tình hình dịch bệnh kéo dài ảnh hưởng đến sự tương tác trực tiếp giữa người quản lý với dữ liệu và giữa người dạy và người học. (chẳng hạn như dịch bệnh Covid-19).

Cùng với sự phát triển của công nghệ thông tin, hoạt động quản lý giáo dục, quản lý đào tạo có nhiều thay đổi. Với việc sử dụng phần mềm quản lý đào tạo, các thông tin về người dạy, người học, kết quả học tập cùng với các yếu tố ảnh hưởng đến việc học tập.

Quá trình được lưu dưới dạng bản mềm trên máy tính, từ đó có thể dễ dàng thực hiện các thao tác phân tích đơn giản.

Sự phát triển của cơ sở hạ tầng công nghệ thông tin trong những năm gần đây cho phép chúng ta thực hiện nhiều hình thức giảng dạy khác nhau. Bên cạnh phương pháp dạy học truyền thống, việc dạy học trực tuyến qua Internet hay qua hệ thống quản lý học tập (LMS) đã được áp dụng rộng rãi. Điều này giúp việc thu thập các nguồn dữ liệu kỹ thuật số trở nên dễ dàng và dễ tiếp cận hơn, đồng thời đẩy nhanh quá trình chuyển đổi kỹ thuật số trong giáo dục.

Trong thời đại công nghệ dựa trên dữ liệu lớn, nhu cầu các trường đại học đổi mới mô hình quản trị và nâng cao hiệu quả quản trị đã trở thành vấn đề cấp thiết đối với các nhà quản lý. Trong quản lý đào tạo, các trường đại học cần số hóa (chuyển đổi số) thông tin quản lý, tạo hệ thống cơ sở dữ liệu lớn liên thông, triển khai các dịch vụ công trực tuyến, ứng dụng công nghệ mới 4.0 (AI, Blockchain, phân tích dữ liệu,...) để quản lý đào tạo, dự báo kết quả học tập của sinh viên, hỗ trợ việc ra quyết định quản lý nhanh chóng và chính xác.

Phạm vi nghiên cứu

Bài viết này sẽ đi sâu phân tích tính cấp thiết của nhu cầu chuyển đổi số trong giáo dục và quản lý giáo dục, thực trạng một số mô hình quản lý đào tạo trong bối cảnh chuyển đổi số hiện nay và phân tích tổng quan các nghiên cứu về ứng dụng kỹ thuật máy học trong xử lý dữ liệu khoa học giáo dục, từ đó đề xuất một số giải pháp tổ chức chuyển đổi số và khai thác dữ liệu trong quản lý đào tạo của một trường đại học tại Việt Nam trong giai đoạn hiện nay.

Ý nghĩa của nghiên cứu

Khai thác những thông tin hữu ích trên để phục vụ quá trình quản lý giáo dục và nâng cao phương pháp, hiệu quả giáo dục. Câu hỏi đặt ra là làm thế nào để xây dựng được nguồn dữ liệu lớn về hoạt động giáo dục, đào tạo trong nhà trường, có nhiều thuộc tính vốn có và phức tạp; đồng thời, làm thế nào để sử dụng, phân tích và khai thác hiệu quả nguồn dữ liệu này phục vụ công tác quản lý giáo dục và nâng cao hiệu quả giáo dục.

Phương pháp nghiên cứu

Để trả lời câu hỏi trên, một lĩnh vực mới đã xuất hiện - khai thác dữ liệu trong giáo dục. Sử dụng các kỹ thuật thống kê toán học, kỹ thuật máy học và mô hình khai thác dữ liệu để trích xuất kiến thức tiềm ẩn trong dữ liệu giáo dục. Ra đời từ những năm đầu thế kỷ 21, đến nay lĩnh vực khai thác dữ liệu trong giáo dục ngày càng phát triển và đạt được nhiều thành tựu đáng ghi nhận.

Kết quả nghiên cứu và thảo luận

Tổng quan về chuyển đổi số trong giáo dục và quản lý giáo dục

Giáo dục là hoạt động nhằm trang bị cho mọi người những kiến thức, kỹ năng về thế giới quan, khoa học, công nghệ và kỹ năng nghề nghiệp từ cơ bản đến nâng cao. Giáo dục và đào tạo trong bối cảnh hiện nay là giáo dục, đào tạo mở, đại chúng, hướng tới người học. Hoạt động giáo dục được thực hiện ở mọi không gian, thời gian bằng nhiều hình thức truyền tải khác nhau, nhằm thực hiện mục tiêu lấy người học làm “trung tâm”. Việc thực hiện yêu cầu tổ chức hoạt động giáo dục trong mọi không gian, thời gian và bằng các phương tiện truyền tải linh hoạt là tiền đề triết học để phát triển ứng dụng công nghệ cũng như chuyển đổi số cho hoạt động giáo dục và tổ chức quản lý giáo dục.

Chuyển đổi số trong giáo dục là quá trình thay đổi cách thức giáo dục và quản lý giáo dục, trong đó việc ứng dụng công nghệ thông tin đáp ứng nhu cầu học tập ngày càng cao của học sinh, sinh viên, giảng viên và quản lý nhà trường nhằm tạo ra môi trường học tập kết nối là vấn đề cốt lõi của bận tâm. Đó là một hệ sinh thái kết hợp công nghệ, dịch vụ và bảo mật để thu hẹp khoảng cách kỹ thuật số và tạo ra trải nghiệm học tập hợp tác, tương tác và cá nhân hóa. Ngày nay chuyển đổi số được áp dụng dưới hai hình thức chính:

Hình thức đầu tiên là ứng dụng công nghệ vào dạy học. Xu hướng công nghệ số khiến không gian dạy và học ngày càng mở rộng. Các thiết bị thông minh được lắp đặt trong lớp học như đầu ghi hình, bàn làm việc thông minh, bảng điện tử thông minh, thiết bị học tập trực tuyến... được sử dụng rộng rãi. Nhiều cơ sở giáo dục còn tạo điều kiện thuận lợi cho sinh viên trải nghiệm, tiếp cận công nghệ cao, thậm chí tham gia các chuyến tham quan thực tế ảo. Các ứng dụng chuyển đổi số trong phương pháp giảng dạy được sử dụng hiện nay như E-learning; Học qua dự án; Học sử dụng ứng dụng thực tế ảo; Các lớp học về Lập trình, STEM, STEAM, v.v.

Hình thức thứ hai là ứng dụng công nghệ vào quản lý. Hiện nay phần mềm quản lý giáo dục đã được nhiều cơ sở giáo dục sử dụng như phần mềm quản lý trường đại học, phần mềm quản lý tài sản, phần mềm quản lý nhân sự, phần mềm quản lý sinh viên, phần mềm quản lý văn bản, phần mềm quản lý thư viện, phần mềm kế toán, cổng thông tin đào tạo, cổng thông tin tuyển sinh trực tuyến, v.v. Những ứng dụng công nghệ này giúp người học dễ dàng tra cứu thông tin; giáo viên, quản trị viên có thể quản lý bảng

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

điểm, thời khóa biểu của học sinh hoặc các thông tin khác trong việc quản lý và điều hành các hoạt động của nhà trường. Mặt khác, việc sử dụng công nghệ để vận hành và quản lý giáo dục cũng được triển khai mạnh mẽ. Ngành Giáo dục đang tích cực đẩy mạnh tái phát triển công nghệ, quy trình làm việc trực tuyến, ứng dụng BigData, IoT, v.v..., đồng thời tăng cường kết nối giữa các phòng ban trên cơ sở quản lý, xử lý các công việc hành chính thông qua Chính phủ điện tử, v.v...

Chuyển đổi số là nền tảng để xây dựng mô hình giáo dục thông minh (SMART Education). Mô hình này được hiểu là “sự tích hợp toàn diện của công nghệ, khả năng truy cập và kết nối mọi thứ qua Internet mọi lúc, mọi nơi”. Cần thực hiện đồng bộ, toàn diện về mọi mặt dựa trên nền tảng ứng dụng CNTT, bao gồm lớp học thông minh (Smart Classroom - SmCl), môi trường thông minh (Smart Environment - SmE), giáo viên thông minh (Smart Teacher - SmT), khuôn viên thông minh (Smart Campus - SmC) và trường học thông minh (Smart School - SmS). Trong các nghiên cứu, việc đánh giá các hoạt động giáo dục thông minh dựa trên các tiêu chí sau: sẵn sàng tiếp nhận và thích ứng với công nghệ, các chỉ số xác định về ứng dụng công nghệ, mức độ “thông minh” của các nhiệm vụ, hoạt động trong lớp học, trường học và thiết bị.

Trong mô hình “Giáo dục THÔNG MINH” các yếu tố được thiết lập theo hệ thống tổng thể, có tác động lẫn nhau, phát huy chất lượng, hiệu quả của quá trình giáo dục. Nó bao gồm các yếu tố sau: S (tự định hướng); M (có động cơ); A (thích ứng); R (tài nguyên): tài nguyên, tài liệu học tập phong phú; T (công nghệ); E (đánh hôn); R (mức độ liên quan). Mô hình này có thể tác động mạnh mẽ đến quá trình giáo dục theo những cách sau:

- Những thay đổi trong kỳ vọng của người học và khả năng đáp ứng của trường học (khả năng thích ứng, khả năng tuyển dụng, và tự tạo việc làm sau khi tốt nghiệp; khả năng duy trì và phát triển chuyên môn chuyên môn; cơ hội học tập suốt đời...);
- Đa dạng hóa “sản phẩm giáo dục”, quá trình đảm bảo và nâng cao chất lượng giáo dục nhờ cơ sở dữ liệu lớn, trí tuệ nhân tạo, chuỗi giá trị trong giáo dục;
- Những thay đổi về mối quan hệ, vai trò, vị trí của người dạy và người học trong quá trình dạy học, trong hệ sinh thái giáo dục;
- Sự thay đổi môi trường dạy học, khuôn viên học tập với học liệu đa chức năng.
- Thay đổi mô hình quản lý, điều hành trong giáo dục và giảng dạy trên nền tảng số mới.

Về bản chất, với sự trợ giúp của công nghệ mới, giáo dục thông minh cần tạo ra một phương pháp hoàn toàn khác với giáo dục đại chúng, hướng tới sự khác biệt, cá nhân hóa và cá nhân hóa cao. Hệ thống kết nối con người - thông tin - vật thể (máy móc)

tạo thành chuỗi liên kết trong đào tạo, nghiên cứu và chuyển giao công nghệ, thúc đẩy quá trình chuyển đổi cơ sở giáo dục thành hệ sinh thái đổi mới sáng tạo. và sự sáng tạo. Như vậy, thay vì cung cấp kiến thức, nội dung giảng dạy, “đào tạo nhân lực, bồi dưỡng nhân tài” theo chương trình cứng nhắc, nhà trường nên đào tạo các kỹ năng (sử dụng thông tin, sáng tạo kiến thức và ra quyết định), bồi dưỡng nhân tài, phát triển tầm nhìn cho người học, theo mô hình “một người học, nhiều chương trình, nhiều cơ sở”.

Trong bối cảnh đó, có thể coi giáo dục là một quá trình công nghệ, là sản phẩm công nghệ có thể đóng gói, chuyển giao và là quá trình ứng dụng, tiếp thu thành tựu của các lĩnh vực công nghệ khác.

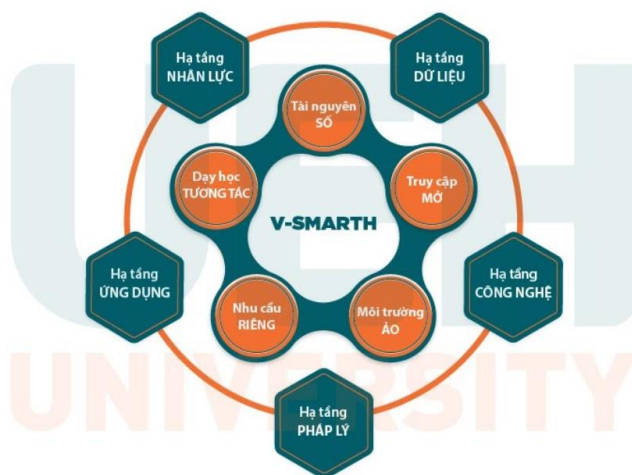
Một số mô hình quản lý đào tạo trong bối cảnh chuyển đổi số ở Việt Nam

Ở Việt Nam đã có một số nghiên cứu về mô hình đại học cũng như mô hình quản lý đào tạo và đánh giá hoạt động đào tạo ở các trường đại học. Tác giả Nguyễn Thị Ngọc Anh (2019) đã hệ thống hóa cơ sở lý luận, đánh giá thực trạng quản lý đào tạo nhằm thực hiện quyền tự chủ, trách nhiệm xã hội của một số trường đại học ở địa phương. Trong nghiên cứu của mình Nguyễn Thị Ngọc Anh đã tiếp cận mô hình quản lý đào tạo CIPO. Cách tiếp cận theo CIPO là cách tiếp cận khi nghiên cứu và xem xét chất lượng của toàn bộ hệ thống giáo dục, bao gồm các yếu tố: Bối cảnh, Đầu vào, Quá trình và Đầu ra. Tác giả đã vận dụng cách tiếp cận này để đề xuất các giải pháp quản lý đào tạo nhằm thực hiện quyền tự chủ, trách nhiệm xã hội phù hợp với điều kiện của các trường đại học ở địa phương.

Trong nghiên cứu “Quản lý đào tạo ở các trường đại học Việt Nam theo cách tiếp cận quản lý dựa trên kết quả (RBM)” (2013), tác giả Trần Văn Tùng đã hệ thống hóa các vấn đề lý luận về quản lý đào tạo ở các trường đại học theo cách tiếp cận quản lý dựa trên kết quả và đề xuất các quy trình và biện pháp dựa trên kết quả để nâng cao chất lượng đào tạo. Theo tác giả, Quản lý dựa trên kết quả (RBM) là phương pháp phân loại các loại hình quản lý với những đặc điểm khác nhau của sự kết hợp khác nhau của các yếu tố quản lý như mục tiêu quản lý, tổ chức mạng lưới quản lý, triết lý quản lý và hiệu quả quản lý.

Tác giả Nguyễn Hữu Đức (2019) đã nghiên cứu đặc điểm, yêu cầu của Cách mạng công nghiệp 4.0, xác định những đặc điểm cơ bản của mô hình đại học 4.0 - đại học công nghiệp thông minh, xây dựng bộ tiêu chuẩn, tiêu chí của mô hình đại học 4.0 theo cách tiếp cận giáo dục đảm bảo chất lượng và xếp hạng đại học, xây dựng cơ sở dữ liệu thống kê các trường đại học từ nguồn quốc tế và trong nước, xác định bộ chỉ số phù hợp và phần mềm làm công cụ đánh giá mức độ tiếp cận mô hình đại học 4.0.

Ngoài ra, tác giả đã đề xuất mô hình chuyển đổi số của trường đại học thông minh (V-SMARTH) hướng tới đổi mới sáng tạo. Theo mô hình này, trường đại học VSmarTH có 6 đặc điểm.



Hình 1: Mô hình đại học thông minh V-SMARTH: Nội dung giáo dục SMART trên nền tảng hạ tầng H.

- **Tài nguyên Số:** là yếu tố cơ bản của đại học thông minh và dạy – học trực tuyến. Tài nguyên số đề cập đến việc sử dụng giáo trình số (digital textbook) với nhiều tính năng vượt trội hơn so với giáo trình truyền thống và giáo trình điện tử (e-textbook) như có thể trực tiếp theo dõi, quản lý quá trình và kết quả học tập, đánh giá và kiểm tra; cho phép kết nối với nguồn học liệu bên ngoài. Đặc biệt, người dạy và người học đều có thể phát triển tài nguyên số này.
- **Nội dung giáo dục Mở:** là đặc điểm quan trọng để thực hiện sứ mệnh của đại học thông minh về đào tạo linh hoạt và cá nhân hóa. Nội dung giáo dục mở bao gồm: Học liệu mở; thông tin mở, bài giảng trực tuyến MOOC, chương trình đào tạo mở và nội dung di động... Ngoài ra, tài nguyên số còn đề cập đến việc kết nối với các tài nguyên giữa những trường đại học khác với nhau và văn hóa chia sẻ như là một tiêu chí để đánh giá chất lượng và hiệu quả của tài nguyên số.
- **Môi trường giáo dục Ảo:** là môi trường cho phép kết hợp các hoạt động giảng dạy và đánh giá trên nền tảng trực tuyến với nhiều mô hình lớp học khác nhau (lớp học chung, lớp học đặc biệt, lớp học tích hợp và lớp học trải nghiệm sáng tạo) với nhiều phương pháp khác nhau dạy – học khác nhau (dạy-học dựa trên vấn đề, dạy-học theo dự án, thảo luận, tích hợp liên ngành, dạy – học qua trải nghiệm) và nhiều tiện ích khác như phòng thí nghiệm ảo, thư viện ảo và các thiết bị học tập ảo. Ngoài ra, môi trường giáo dục ảo còn cung cấp việc giám sát, kiểm tra đánh giá trực tuyến giúp đánh giá người học linh hoạt và toàn diện hơn.
- **Nhu cầu học tập Riêng:** củng cố tính linh hoạt của hệ thống giáo dục và xây dựng chương trình học tùy biến gắn với sở thích cá nhân và nghề nghiệp định hướng trong tương lai. Việc dạy và học có thể theo lộ trình cố định với nhiều hình thức (trực tuyến hoặc trực tiếp) hay một chương trình theo định hướng của mỗi cá nhân tùy sở thích, nhu cầu, năng lực.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

- **Môi trường giáo dục có Tương tác:** đề cập đến việc học tập giảng dạy thông qua nền tảng web có sự tương tác. Tương tác này bao gồm tương tác giữa người học và người dạy, tương tác người học với nhau và tương tác giữa người học và tài nguyên số. Việc học tập như vậy có thể diễn ra mọi nơi với đầy đủ nội dung. Sự tương tác này thúc đẩy sự chia sẻ và văn hóa chia sẻ nhưng cũng mang lại mặt trái liên quan đến vấn đề bản quyền, sở hữu trí tuệ, đạo đức và liêm chính học thuật.
- **Hạ tầng số:** đề cập đến việc đảm bảo các hạ tầng pháp lý số, hạ tầng nhân lực số, hạ tầng dữ liệu số, hạ tầng công nghệ kỹ thuật số cho việc phát triển ĐHTM.

Để đánh giá mức độ thông minh của một ĐHTM, nhóm tác giả Nguyễn Hữu Đức và cộng sự cũng đề xuất các mức độ thông minh của đại học thông minh bao gồm 5 cấp độ: Connection – thu nhận và kết nối thông tin, Conversion – chuyển đổi thông tin và số hóa, Cyber – phân tích và chẩn đoán, Cognition – nhận diện và dự báo, Configuration – tối ưu hóa.



Hình 2: Cấu trúc 5C của các hệ thống CPS và các mức độ thông minh của đại học thông minh

- **Cấp độ 1 – Thu nhận và kết nối thông tin (Connection):** Các hệ thống trong trường có khả năng thu thập thông tin và kết nối các bên liên quan trong các vấn đề liên quan đến học tập như môi trường học tập, phương pháp giảng dạy, đối tượng học tập, phong cách giảng dạy của giảng viên, các hệ thống này có thể tùy chỉnh để thích ứng với những thiết bị khác nhau như máy tính, máy tính bảng, điện thoại hay hệ điều hành khác nhau như iOS và Android. Ngoài ra, các hệ thống có thu nhận và quản lý thông tin thông tin về tất cả đối tượng, sự kiện, quá trình trong khuôn viên trường. Ví dụ: các cảm biến được sử dụng để ghi nhận dữ liệu về môi trường xung quanh như sử dụng điện, đèn, nhiệt độ, độ ẩm... Đầu đọc thẻ thông minh để mở cửa vào giảng đường, phòng máy tính, lớp học và kích hoạt các tính năng/phần mềm/phần cứng. Hệ thống nhận dạng khuôn mặt, giọng

nói, cử chỉ và các thiết bị tương ứng để truy xuất và xử lý dữ liệu như điểm danh, các hoạt động trong lớp...

- **Cấp độ 2 – Khả năng chuyển đổi thông tin và số hóa (Conversion):** Từ những thông tin được thu thập và quản lý ở cấp độ 1, các hệ thống trong cấp độ 2 có khả năng kết nối chúng lại với nhau và đưa ra những kết quả thống kê. Ví dụ: mức độ chuyên cần của sinh viên, kết quả học tập của sinh viên, số giờ giảng của giảng viên, đánh giá của sinh viên về giảng viên, mức độ đăng ký của sinh viên theo từng giảng viên, tình hình sử dụng phòng học, phòng thí nghiệm...
- **Cấp độ 3 – Phân tích và chẩn đoán (Cyber):** Từ những kết quả phân tích ở cấp độ 2, các hệ thống trong cấp độ 3 này có khả năng phân tích, đưa ra những chẩn đoán và học hỏi từ những kết quả đó để hoàn thiện hệ thống. Ví dụ: sau khi thu thập dữ liệu về kết quả học tập của sinh viên, hệ thống có khả năng phân tích lý do những sinh viên không đạt kết quả tốt như học quá nhiều môn trong học kỳ, vắng quá nhiều buổi học hay từ việc thu thập thông tin những lớp có quá ít sinh viên đăng ký, hệ thống có thể phân tích được các lý do như chất lượng giảng viên, thời gian không phù hợp với sinh viên...
- **Cấp độ 4 – Nhận diện và dự báo (Cognition):** Sau khi có được kết quả phân tích từ cấp độ 3, hệ thống ở cấp độ 4 sẽ dùng những kết quả này để dự báo những kết quả có thể xảy ra và đưa ra giải pháp. Ví dụ: hệ thống trong cấp độ 4 có khả năng dự báo kết quả học tập của sinh viên, dự báo chất lượng giảng dạy của giảng viên (mức độ tham gia của sinh viên, mức độ hiểu bài của sinh viên), hệ thống quản lý tuyển sinh để dự đoán, và kiểm soát các thay đổi về số lượng sinh viên hàng năm, dự báo những tài nguyên nào mà sinh viên dành nhiều thời gian nhất và yêu cầu người hướng dẫn cung cấp thêm các tài nguyên có tính chất tương tự hay hệ thống an toàn khuôn viên (Campus-wide Safety System) để dự đoán, nhận biết và hành động phù hợp và không phù hợp trong khuôn viên trường.
- **Cấp độ 5 – Tối ưu hóa (Configuration):** ĐHTM có khả năng tự thay đổi cấu trúc nội bộ, tối ưu hóa và tự duy trì một cách có chủ đích. Ví dụ: hệ thống tự động xác định hệ thống, thông số, cảm biến, và các tính năng trong một lớp học thông minh phù hợp với môn học, đặc điểm của lớp học, người giảng dạy như các cảm biến xác định xem học sinh có đang ở trong lớp học hay không, đèn có sáng không... và điều chỉnh lại cho phù hợp, hệ thống tự động xác định lại hệ thống, phần cứng, phần mềm và các tính năng trong một lớp học thông minh phù hợp với từng giảng viên, những hệ thống tự phục hồi khi xảy ra sự cố như máy chủ tự động khóa và phục hồi lại khi có virus xâm nhập...

Tổng quan các nghiên cứu ứng dụng kỹ thuật máy học trong xử lý dữ liệu khoa học giáo dục

Khai thác dữ liệu là quá trình khám phá thông tin có giá trị hoặc đưa ra dự đoán từ dữ liệu. Đây là một vấn đề bao trùm nhưng cơ sở dữ liệu hiện nay ở dạng Bigdata với nguồn dữ liệu rất lớn sẽ rất khó khăn cho người học cũng như người dạy trong lĩnh vực giáo dục nếu không có kỹ năng khai thác dữ liệu thành thạo nên sẽ rất khó để tìm được dữ liệu phù hợp.

Trong giáo dục, bài toán trích xuất thông tin (Information Extraction) là bài toán vận dụng các thuật toán được người dạy và người học sử dụng nhiều nhất. Từ một cơ sở dữ liệu cụ thể, thao tác này có thể giúp người dạy và người học trích xuất thông tin, tìm kiếm các trường phù hợp với lĩnh vực, kiến thức mà người dạy và người học cần cung cấp.

Xu hướng giáo dục của thế kỷ 21 là giáo dục mở và giáo dục đại chúng, vì vậy bên cạnh những kiến thức lý thuyết được truyền đạt mang tính hàn lâm cần có sự tham gia của hình ảnh, góp phần hỗ trợ cho những kiến thức lý thuyết cần truyền tải cũng có liên quan đến vấn đề đặt ra. giáo dục mở và giáo dục đại chúng trong bối cảnh hiện nay. Kỹ thuật máy học có thể xử lý hình ảnh dựa trên các phương pháp và ứng dụng sau như phân tích thông tin từ hình ảnh, ngoài hình ảnh cần xử lý, công nghệ kỹ thuật máy học có thể xử lý các vấn đề sau:

Đầu tiên là thao tác gắn thẻ hình ảnh (Image Tagging). Đây là thao tác hết sức quen thuộc xuất hiện trên các mạng xã hội phổ biến như Facebook, Instagram, Tiktok. Đây là chức năng dựa trên thuật toán phát sóng phát hiện và tự nhận dạng khuôn mặt của cá nhân phù hợp với hình ảnh, khuôn mặt của cá nhân đó được lưu trữ trong cơ sở dữ liệu. Thuật toán này được xử lý dựa trên cơ sở dữ liệu được cung cấp và tự động tìm ra những bức ảnh tương tự của một cá nhân đã được sử dụng trước đó. Việc sử dụng chức năng tag hình ảnh này rất khả thi trong lĩnh vực giáo dục dựa trên các công việc bổ sung cho giáo viên như điểm danh, quản lý danh sách lớp, cũng như thuận tiện cho người học khi được tiếp nhận cũng như nắm bắt thông tin của lớp.

Thứ hai là thao tác nhận dạng ký tự (Optical Character Reviews) cũng là thao tác rất quen thuộc. Hiện nay có rất nhiều ứng dụng trên smartphone giúp người dùng lưu trữ các tài liệu sau với định dạng file jpg hoặc pdf. Thuật toán nhận dạng ký tự từ máy học tập là sự nâng cấp của công nghệ, đây là lĩnh vực rất quan trọng trong giáo dục, đặc biệt trong bối cảnh giáo dục đang đẩy mạnh số hóa, chuyển đổi số, có kỹ thuật máy học với khả năng nhận dạng ký tự, tài liệu dưới dạng ký tự được trình bày, được thuật toán này nhận diện và chuyển sang dạng số hóa để sử dụng và lưu trữ. Đây là thuật toán góp phần rất lớn cho cả người học và người dạy trong bài toán lưu trữ thông tin, truyền đạt kiến thức giữa người dạy và người học trong cả tương tác trực tiếp và trực tuyến.

Kỹ thuật máy học để khai thác dữ liệu được áp dụng trong nhiều lĩnh vực trong đó có khoa học giáo dục. Đặc biệt trong bối cảnh giáo dục có nhiều thay đổi dưới tác

động của CMCN 4.0, công nghệ đã trở thành một phần phương tiện sản xuất của quá trình giáo dục. Mặt khác, nhu cầu học tập của cá nhân cũng được chú trọng. Vì vậy, nghiên cứu sư phạm đang được chuyển hướng sang nghiên cứu chuyên sâu về hành vi của người học để xây dựng chương trình học tập cá nhân; đồng thời khai thác dữ liệu lớn của người học để chẩn đoán và định hướng lại quá trình học tập của người học nói riêng và quản lý điều hành quá trình giáo dục nói chung. Đó cũng chính là nội dung mà kỹ thuật máy học có thể ứng dụng vào nghiên cứu khoa học giáo dục.

Có nhiều thuật toán thường xuyên được áp dụng trong kỹ thuật máy học để giải quyết các vấn đề trong khoa học giáo dục: (1) thuật toán phát hiện điểm bất thường, đây là phương pháp thuật toán phát hiện những điểm bất thường, ví dụ như gian lận trong quá trình học tập, hay rộng hơn là phát hiện điểm bất thường trong hoạt động nghiên cứu và phát triển (R&D) của một hoạt động khoa học và công nghệ trong trường đại học. Để có thể phát hiện các dị thường cần khai thác dữ liệu có thuộc tính dị thường và so sánh với các giá trị tiêu chuẩn, từ đó tổng hợp và đưa ra đánh giá về thao tác, đây là thuật toán cần thiết cho người dạy và người học; (2) Thuật toán phát hiện luật (Association Rules), trong bài toán khai thác dữ liệu của người dạy và người học thường diễn ra nhiều lần, từ đó xây dựng mới cơ sở dữ liệu về các xu hướng khoa học công nghệ để tìm kiếm, từ đó thuật toán sẽ tổng hợp tìm kiếm. các quy tắc, cũng như các lĩnh vực tìm kiếm thường xuyên của người dạy hoặc người học, chủ đề từ đó, công nghệ AI sẽ đưa ra dự đoán về xu hướng tìm kiếm cũng như gợi ý các lĩnh vực khoa học, kiến thức cần thiết phù hợp với xu hướng tìm kiếm của người dạy và người học; (3) thuật toán phân nhóm, phân nhóm cũng là một thuật toán quan trọng, là thao tác thường được giáo viên sử dụng trong việc chia học sinh trong lớp thành các nhóm dựa trên đặc điểm chung cũng như lĩnh vực học tập phù hợp, với nền tảng công nghệ AI & cơ sở dữ liệu về người học, việc phân nhóm sẽ dễ dàng hơn cho giáo viên thao tác và phù hợp với đặc điểm của người học; (4) thuật toán dự đoán, đây là thuật toán dự đoán của sinh vật. Trong lĩnh vực khoa học công nghệ, có thể khẳng định nghiên cứu dự đoán là một loại hình nghiên cứu khó, hoặc đối với hoạt động dạy học cần làm thí nghiệm để có thể kiểm chứng phản ứng của các thông số đó trong điều kiện thực tế. Việc sử dụng AI và thuật toán này góp phần dự đoán kết quả nghiên cứu, đảm bảo chi phí và an toàn cho người dạy và người học.

Giải pháp tổ chức chuyển đổi số và khai thác dữ liệu trong quản lý đào tạo của trường đại học tại Việt Nam trong giai đoạn hiện nay

Triển khai chuyển đổi số trong trường đại học

Với mục tiêu xây dựng hệ thống quản trị đại học thông minh, tăng cường ứng dụng công nghệ thông tin trong giảng dạy, quản lý nhà trường, quản lý sinh viên và xây dựng cơ sở vật chất hiện đại, đồng bộ, việc nghiên cứu ứng dụng chuyển đổi số và khai

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

thác dữ liệu trong giáo dục vào thực tế giảng dạy đào tạo và nghiên cứu khoa học của các trường đại học cần sớm được triển khai. Tùy theo điều kiện thực tế, mỗi trường đại học cần có định hướng chung trong việc xây dựng lộ trình ứng dụng chuyển đổi số và khai thác dữ liệu lớn vào hoạt động đào tạo, nghiên cứu và giảng dạy. Một số hướng dẫn cơ bản như sau:

Thứ nhất, hình thành hệ thống big data của trường từ hai nguồn: (1) số hóa toàn bộ dữ liệu của trường (dữ liệu nội sinh) và (2) liên kết, trao đổi, hợp tác trong nước và quốc tế để khai thác, xử lý, khai thác dữ liệu nhằm xây dựng nền tảng của trường. dữ liệu lớn (dữ liệu ngoại sinh). Phát triển nguồn tài nguyên số và môi trường học tập số, bổ sung kho dữ liệu số của trường, ngân hàng câu hỏi trực tuyến dùng chung trong nhà trường, kho bài giảng e-learning kết nối Hệ tri thức Việt Nam số hóa.

Thứ hai, khai thác dữ liệu lớn (bao gồm dữ liệu lớn của Trường và dữ liệu lớn trong nước và quốc tế) để sử dụng trong các hoạt động của trường.

Thứ ba, nghiên cứu, xây dựng các đề án chi tiết đảm bảo thu thập, quản lý, vận hành dữ liệu lớn, tổ chức khai thác dữ liệu trong đào tạo, nghiên cứu khoa học trong trường học. Đẩy mạnh triển khai dịch vụ công trực tuyến trong quản trị đại học, ưu tiên triển khai dịch vụ công trực tuyến phục vụ tuyển sinh đại học; thanh toán học phí không dùng tiền mặt; các loại hồ sơ, sổ sách, tài liệu điện tử; tiếp tục sử dụng có hiệu quả hệ thống quản lý hành chính điện tử để trao đổi văn bản điện tử, chữ ký số giữa các đơn vị và tổ chức, cá nhân có liên quan.

Thứ tư, nâng cao kỹ năng dạy học trực tuyến, kỹ năng chuyển đổi số, kỹ năng tham gia hoạt động dạy và học trực tuyến cho giảng viên và sinh viên; hình thành hệ sinh thái học tập trong môi trường số hóa.

Nghiên cứu và xây dựng lộ trình ứng dụng dữ liệu lớn trong hoạt động giáo dục ở các trường đại học cần thực hiện các giải pháp sau:

Thứ nhất, nâng cao nhận thức về ứng dụng công nghệ thông tin, số hóa và ứng dụng dữ liệu lớn, khai thác dữ liệu trong hoạt động quản lý đào tạo, nghiên cứu và giảng dạy.

Thứ hai, thực hiện một số bước trong quy trình chuẩn hóa dữ liệu để hình thành dữ liệu lớn từ nguồn nội sinh của trường.

Thứ ba, nghiên cứu, lựa chọn các mô hình dữ liệu lớn, truy cập dữ liệu lớn và sử dụng khai thác dữ liệu phù hợp với đặc điểm, chức năng, nhiệm vụ của trường.

Thứ tư, tăng cường quản trị dữ liệu và sử dụng các công cụ phân tích và khai thác dữ liệu lớn để mang lại lợi ích thông tin góp phần đổi mới phương pháp giảng dạy và nghiên cứu khoa học.

Thứ năm, tăng cường đầu tư hạ tầng công nghệ thông tin phục vụ thời đại số chuyển đổi cũng như ứng dụng dữ liệu lớn, khai thác dữ liệu trong quản lý và giảng dạy.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thứ sáu, nâng cao chất lượng nguồn nhân lực để có thể xây dựng dữ liệu lớn và làm chủ năng lực khai thác dữ liệu của Trường, trong đó việc tăng cường nguồn nhân lực trong các lĩnh vực công nghệ thông tin, khai thác dữ liệu, kỹ thuật máy học và các vấn đề liên quan là cấp thiết.

Chương trình chuyển đổi số quốc gia đến năm 2025 và giải pháp chuyển đổi số tại Đại học Trường Đại học Kinh tế TP. Hồ Chí Minh

Tháng 6-2020, Thủ tướng Chính phủ phê duyệt Chương trình Chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030; trong đó, giáo dục và đào tạo (GD-ĐT) là một trong 8 lĩnh vực được ưu tiên hàng đầu trong triển khai thực hiện.

Trên thực tế, việc chuyển đổi số đã được các trường thực hiện từng bước từ nhiều năm trước và đẩy mạnh trong thời gian gần đây. Tại Trường ĐH Kinh tế TP.HCM (UEH), quá trình số hoá đã bắt đầu từ năm 2009 khi lần đầu tiên triển khai hệ thống đào tạo tín chỉ. Từ năm 2013 đến nay, liên tục các hệ thống thông tin được xây dựng để phục vụ công tác giảng dạy, nghiên cứu, quản trị nhà trường. Đặc biệt, hệ thống e-learning được đưa vào vận hành năm 2016 theo mô hình giảng dạy kết hợp với quy mô toàn trường, đến nay 100% các lớp học đều có triển khai các công cụ trực tuyến hỗ trợ. Nhờ đó, trong đợt dịch bệnh Covid-19 nhiều biến động vừa qua, toàn bộ hoạt động của trường đã nhanh chóng thay đổi để thích ứng và vẫn đảm bảo chất lượng và tiến độ.

Đến hết năm 2020, hầu hết các hoạt động của nhà trường từ quản lý đến giảng dạy, nghiên cứu khoa học đều đã được chuyển đổi số; từ việc theo dõi quá trình học tập, nghiên cứu, hoạt động đoàn thể của sinh viên, giảng viên đến các công cụ quản trị đại học thông minh như quản trị nhân sự, lịch giảng, thời khóa biểu, quản lý khoa học, đánh giá KPI cho viên chức. Sinh viên còn được trải nghiệm hệ thống chăm sóc người học, thực hiện các dịch vụ công của nhà trường hoàn toàn trực tuyến.

Trong năm 2021, trường tiếp tục thực hiện theo đề án Chuyển đổi số, UEH tiến hành rà soát, nhìn lại quá trình phát triển để định hướng cho việc chuyển đổi số phù hợp sự phát triển công nghệ trong tương lai như ứng dụng các công nghệ mới trí tuệ nhân tạo, điện toán đám mây, di động hóa, phân tích dữ liệu tối ưu hóa nguồn lực, phát triển những ứng dụng tiện ích sáng tạo nhằm tạo sự trải nghiệm tiện nghi, định hướng phát triển công dân số toàn cầu trong tương lai.

Hệ thống thi trực tuyến

Kể từ tháng 10/2022, hình thức thi trực tuyến (online) đã trở thành hình thức chủ yếu trong hoạt động khảo thí tại UEH. Các công tác tổ chức thi, kiểm tra đánh giá kết quả học tập của thí sinh, người học ở các bậc, hệ (như yêu cầu kỹ thuật về thiết bị làm bài, thiết bị giám sát, quy định bố trí không gian thi, quy trình ra đề, quy định làm bài thi...) được xây dựng và trình bày chi tiết trong Quy định tổ chức theo hình thức thi trực tuyến tại UEH nhằm đảm bảo tính hiệu quả và đồng bộ, đánh giá công bằng, chất lượng

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

trong công tác đào tạo của Nhà trường [<https://huongdanthi.ueh.edu.vn/>]. Đây là trang thi trực tuyến chính thức của UEH với các đường link tương ứng các ca thi, hướng dẫn cụ thể cách thức dự thi và các yêu cầu nhằm đảm bảo tính nghiêm túc của kỳ thi.

HƯỚNG DẪN THI TRỰC TUYẾN

ÁP DỤNG TẠI UEH TỪ THÁNG 10/2022



Nhằm đảm bảo quyền lợi của thí sinh tham dự thi trực tuyến, Nhà trường luôn có đội ngũ túc trực để giải quyết những sự cố mà thí sinh gặp phải. Đặc biệt, trong trường hợp thí sinh không đáp ứng yêu cầu kỹ thuật để thi trực tuyến có thể đăng ký thi tại trường ở link dangkythi.ueh.edu.vn.

Dịch vụ hồ sơ điện tử có xác thực

Trong thời gian qua, hàng ngày UEH tiếp nhận từ 50 - 200 đơn đăng ký cấp các giấy tờ, hồ sơ để phục vụ cho mục đích cá nhân trên Cổng giao dịch điện tử <https://es.ueh.edu.vn/>. Nhằm đáp ứng nhu cầu ngày càng tăng cao của người học và cựu sinh viên, UEH đã ứng dụng công nghệ số và cung cấp dịch vụ hồ sơ điện tử có xác thực thông qua hệ thống Portal sinh viên của Trường. Theo đó, người dùng chỉ cần truy cập vào tài khoản cá nhân để tự in hồ sơ hoặc gửi email trực tiếp đến địa chỉ cá nhân/đơn vị một cách nhanh chóng, thuận tiện, tiết kiệm được thời gian và chi phí so với yêu cầu dịch vụ có đóng dấu xác nhận như trước đây. Các cá nhân, đơn vị khi sử dụng các hồ sơ điện tử có xác thực của UEH có thể tra cứu và xác thực thông tin trên trang <https://student.ueh.edu.vn/e-confirm>.

UEH triển khai dịch vụ hồ sơ điện tử có xác thực với các loại giấy tờ, như: Giấy xác nhận người học các bậc/hệ để bổ túc hồ sơ cá nhân; Giấy xác nhận người học hoàn thành chương trình đào tạo; Giấy xác nhận người học đang trả nợ học phần; Bảng điểm học tập các Khóa/hệ bằng Tiếng Việt/Tiếng Anh; Giấy giới thiệu người học thực tập - Khảo sát thu thập dữ liệu; Giấy chứng nhận tốt nghiệp tạm thời; Bảng điểm rèn luyện sinh viên song ngữ; Giấy xác nhận học bổng sinh viên song ngữ. Ngoài ra, trong thời gian tới tùy theo nhu cầu của người học, UEH sẽ theo dõi và bổ sung thêm nhiều sản phẩm khác liên quan nhiều đến quá trình học tập, rèn luyện tại trường.

Cấp chứng chỉ/chứng nhận điện tử các khóa ngắn hạn

Nhằm tạo sự thuận tiện cho người học, cựu sinh viên, cựu học viên trong việc nhận Chứng chỉ/Giấy chứng nhận điện tử UEH các khóa đào tạo ngắn hạn một cách nhanh chóng; đồng thời giúp các đơn vị, cá nhân tra cứu trực tuyến và xác minh các Chứng chỉ/Giấy chứng nhận do UEH cấp, Nhà trường đã ứng dụng công nghệ số và chính thức triển khai cấp Chứng chỉ/Giấy chứng nhận điện tử UEH các khóa đào tạo ngắn hạn từ tháng 11/2022. Việc này giúp đảm bảo sự thống nhất, hiệu quả trong công tác quản lý, lưu trữ các Chứng chỉ/Giấy chứng nhận điện tử các khóa đào tạo ngắn hạn do UEH cấp.

Theo đó, các Chứng chỉ/Giấy chứng nhận điện tử UEH được cấp online miễn phí, người dùng chỉ cần truy cập vào trang web chungchinganhan.ueh.edu.vn, đăng nhập bằng mã học viên để tự tải Chứng chỉ/Giấy chứng nhận điện tử và gửi trực tiếp đến các cá nhân/đơn vị một cách nhanh chóng, thuận tiện, tiết kiệm được nhiều thời gian và chi phí. Khi nhận được Chứng chỉ/Giấy chứng nhận điện tử UEH, các cá nhân, đơn vị có thể dễ dàng kiểm tra tính xác thực trực tuyến.

Trong trường hợp có nhu cầu sử dụng bản giấy, người học, cựu sinh viên, cựu học viên có thể đề nghị và sẽ được cấp Bản sao từ sổ gốc (cấp không giới hạn và có tính phí). Đối với các khóa ngắn hạn dành cho sinh viên đại học chính quy, UEH cấp Giấy chứng nhận điện tử cho khóa học hoặc từng môn học tùy theo nội dung chương trình đào tạo và quy định hiện hành của UEH.

Tích hợp hệ thống quản lý, chăm sóc người học/đối tác, kho tri thức trên hệ thống CRM

Kho tri thức UEH <https://hotro.ueh.edu.vn/> được xây dựng như một nơi tập hợp và lưu trữ tất cả các thông tin hỗ trợ cần thiết liên quan đến quá trình học tập, sinh hoạt và nghiên cứu của các sinh viên, học viên tại UEH. Ví dụ như các thông tin giới thiệu tổng quan về UEH (sứ mệnh, thành tựu, văn hóa...); các cơ sở trực thuộc; đội ngũ viên chức; thông tin các bậc/hệ (Đại học chính quy, Vừa làm vừa học, Sau đại học...); thông tin về các dịch vụ thông minh tại UEH; thông tin của UEH - Phân hiệu Vĩnh Long;...

Tại đây, người học có thể tìm kiếm thông tin từ các cây thư mục dữ liệu được phân theo các loại hình đào tạo của UEH. Đặc biệt, dễ dàng tra cứu thông tin bằng cách nhập các từ khóa (keyword) ở mục tìm kiếm để lọc tìm thông tin phù hợp. Ngoài ra, Kho tri thức còn giới thiệu nhiều nội dung hữu ích như: Cổng thông tin, Chứng chỉ và Tài khoản hỗ trợ người học. Như vậy, người học tại UEH sẽ chủ động trong việc tìm kiếm thông tin cần thiết một cách nhanh chóng trên môi trường mạng (internet).

Với việc số hóa các hoạt động của Nhà trường, Kho tri thức đã được kết nối trực tiếp với Hệ thống quản lý, chăm sóc và hỗ trợ đối tác/người học - CRM (Customer Relationship Management) của UEH. Do đó, người học có thể dùng tính năng “Quản lý

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

yêu cầu” trên Kho tri thức để gửi các yêu cầu hỗ trợ/thắc mắc cho các đơn vị chức năng tại UEH, hệ thống sẽ tự động đưa thông tin vào CRM và chuyển cho các bộ phận chức năng phản hồi giải quyết cho người học theo thời gian cam kết thay vì phải trực tiếp tới các đơn vị chức năng để được hỗ trợ giải đáp thông tin như trước đây. Người học sẽ nhận được kết quả phản hồi từ UEH qua email cá nhân.

Hệ thống Quản lý, chăm sóc và hỗ trợ đối tác/người học CRM

UEH đã xây dựng và chính thức đưa vào vận hành Hệ thống quản lý, chăm sóc và hỗ trợ đối tác/người học CRM dành cho các đơn vị chức năng thuộc trường. Sự ra đời của CRM nhằm nâng cao chất lượng công tác hỗ trợ và chăm sóc người học, đồng hành, đảm bảo cho người học có trải nghiệm tốt nhất tại UEH.

Toàn bộ các kênh tiếp nhận thông tin của Nhà trường (Email, Điện thoại, Mạng xã hội, Kho tri thức UEH, Ứng dụng UEH student, trực tiếp tại văn phòng...) thông qua đầu mối tiếp nhận là Phòng Chăm sóc và hỗ trợ người học (DSA) được tích hợp vào hệ thống CRM. Người học, đối tác liên hệ khi có yêu cầu hỗ trợ, thắc mắc từ các kênh thông tin này sẽ tự động được tiếp nhận và phân công cho các đơn vị chức năng để xử lý. Với mỗi yêu cầu hỗ trợ của đối tác/người học, hệ thống sẽ mở ra một yêu cầu hỗ trợ (ticket). Toàn bộ quá trình tiếp nhận thông tin và xử lý yêu cầu sẽ có email thông báo cho người học, đối tác liên hệ để theo dõi. Hệ thống CRM kết nối trực tiếp với dữ liệu người học, người học tiềm năng, đối tác tạo thành 01 cơ sở dữ liệu chung trong toàn UEH. Lịch sử yêu cầu, hỗ trợ của đối tác/người học từ tất cả các kênh tiếp nhận được lưu trữ tập trung tạo thuận lợi trong giải quyết yêu cầu một cách tối ưu nhất.

Với những tiện ích trên hệ thống, đối tác/người học có thể hoàn toàn yên tâm vì các vấn đề thắc mắc sẽ luôn được tiếp nhận, xử lý và phản hồi một cách nhanh chóng, chính xác. Bên cạnh đó, nhằm nâng cao chất lượng dịch vụ và lắng nghe ý kiến đóng góp cho hoạt động tại UEH, mỗi ticket trên hệ thống khi thực hiện xong sẽ có 01 bản khảo sát chất lượng dịch vụ để đối tác/người học liên hệ đánh giá và góp ý.

Trang giao dịch bán hàng trực tuyến vì cộng đồng

Năm 2022, UEH lần đầu tiên ra mắt trang giao dịch bán hàng trực tuyến UEH Community Shop với các sản phẩm phục vụ cho cộng đồng và vì cộng đồng. Tại đây, các UEHer có thể dễ dàng tìm kiếm các nguồn sách kinh tế hữu ích cũng như các sản phẩm sáng tạo, mang màu sắc thương hiệu của cộng đồng UEH. Đặc biệt, UEH Community Shop hoạt động với chủ trương bán hàng phi lợi nhuận, khoản chênh lệch thu chi sẽ được đóng góp vào Quỹ Giving to UEH nhằm tái đầu tư vào các hoạt động ươm mầm tài năng, đầu tư vươn tầm quốc tế, lan tỏa tri thức, và các dự án hành động bền vững của nhà trường.

Tiên phong trên hành trình chuyển đổi số, hướng đến đại học thông minh và đáp ứng những yêu cầu đào tạo trong xu thế mới, UEH đang không ngừng nỗ lực để mang

đến những sản phẩm chất lượng phục vụ cho công tác giáo dục và đào tạo tại Nhà trường. Song song đó là sự hỗ trợ hết mình và đồng hành cùng người học trong mọi hành trình để các bạn có thể tự tin tiếp thu kiến thức, tiếp cận xu hướng giáo dục hiện đại, trở thành những thế hệ công dân toàn cầu đủ năng lực cạnh tranh trên thị trường lao động tương lai.

UEH Global - Hệ thống học tập trực tuyến miễn phí của UEH dành cho các trường THPT, hướng đến phát triển bền vững

Dự án cộng đồng “Hỗ trợ chuyển đổi số miễn phí cho các trường THPT” - UEH Global Learning là dự án chia sẻ và chuyển giao kinh nghiệm chuyển đổi số trong hoạt động dạy và học cho các trường THPT, đặc biệt là các điểm trường bị hạn chế về địa lý, khó khăn trong việc triển khai dạy và học trực tuyến nhằm hỗ trợ các trường vượt qua thách thức giảng dạy và học tập trực tuyến trong mùa dịch Covid-19, đồng thời đặt nền tảng lâu dài cho việc ứng dụng công nghệ thông tin, hỗ trợ chuyển đổi số cho các trường THPT. Dự án Global Learning với 06 sản phẩm chính bao gồm: (1) Dạy và học trực tuyến; (2) Tổ chức thi tự luận và trắc nghiệm trực tuyến, (3) Trộn đề thi và đáp án trắc nghiệm trên giấy, (4) Khóa luyện thi tốt nghiệp THPT trực tuyến, (5) Chương trình trắc nghiệm tính cách, lựa chọn nghề nghiệp và (6) Chức năng tư vấn tuyển sinh. Nằm trong khuôn khổ dự án, hệ thống học tập trực tuyến UEH Global chuyển giao hoàn toàn miễn phí cho các trường THPT với 3 tính năng quan trọng sau:

- Nền tảng giảng dạy trực tuyến UEH Global hỗ trợ quản lý lớp học, tài liệu học tập, tổ chức làm bài kiểm tra, đánh giá quá trình học tập, thực hiện trao đổi giữa học viên và học sinh... thông qua dashboard: <https://global.ueh.edu.vn/>.
- Hệ thống tương tác trực tiếp giữa giáo viên và học sinh trong quá trình dạy và học trên nền tảng Google Meet do nhà trường cấp tài khoản.
- Tổ chức kiểm tra thường xuyên, định kỳ theo hình thức trực tuyến (xây dựng quy chế, tổ chức đề thi, coi thi, chấm thi... theo hình thức trực tuyến).

Hệ thống UEH Global được chia sẻ dựa trên nền tảng hệ thống giảng dạy trực tuyến đang sử dụng của UEH, được UEH xây dựng và vận hành trong hoạt động giảng dạy trong nhiều năm qua với số lượng 30.000 sinh viên mỗi năm. Đối với hệ thống này các tính năng cần thiết cho hoạt động giảng dạy trực tuyến gần như đầy đủ, vì vậy UEH mong muốn chia sẻ và chuyển giao miễn phí cho các trường để giải quyết các thách thức trong giảng dạy mùa dịch Covid-19, và sau đó là đặt nền tảng lâu dài cho việc sử dụng hiệu quả nguồn tài nguyên sẵn có trong ứng dụng công nghệ thông tin, hỗ trợ đẩy nhanh quá trình chuyển đổi số cho các trường THPT, hướng đến sự phát triển bền vững của cộng đồng.

Chuyển giao miễn phí UEH Global thông qua chương trình tập huấn cho các trường THPT

UEH triển khai chuyển giao cho các trường THPT tại 13 tỉnh khu vực Đồng bằng sông Cửu Long, sau đó sẽ tiến tới triển khai cho tất cả các trường THPT trong cả nước có quan tâm để cùng chia sẻ kinh nghiệm tổ chức giảng dạy trực tuyến. Việc tổ chức chuyển giao Hệ thống học tập trực tuyến UEH Global đến các trường được UEH triển khai bài bản, thông qua các chương trình tập huấn chuyên sâu, hướng dẫn sử dụng chi tiết cho giáo viên, đồng thời tổ chức đội ngũ hỗ trợ tư vấn thường xuyên các Thầy, Cô và các em học sinh trong quá trình sử dụng thực tế.

Chương trình tập huấn giai đoạn 2, đã chính thức diễn ra vào sáng ngày 30/08/2021, với sự tham gia của hơn 180 quý Thầy/Cô đến từ các trường: THPT Võ Văn Kiệt, THPT Phạm Hùng, THPT Hoàng Thái Hiếu, THPT Mang Thít, THPT Dân tộc nội trú, THPT Nguyễn Hiếu Tự, THCS và THPT Đông Thành, THPT Trần Đại Nghĩa, THCS và THPT Phú Quới,... tại tỉnh Vĩnh Long.

TS. Bùi Quang Hùng - Phó Hiệu trưởng UEH chia sẻ: *“Với vai trò là trường đại học công lập trọng điểm quốc gia, UEH đã và đang thực hiện sứ mạng của một đại học đa ngành, có uy tín, thực hiện nhiều chương trình gắn kết và hỗ trợ cộng đồng để cùng hướng đến phát triển bền vững, đơn cử như dự án cộng đồng “Hỗ trợ chuyển đổi số miễn phí cho các trường trung học phổ thông” – UEH Global Learning. Đây là một trong những dự án nằm trong chiến lược chuyển đổi số chung của UEH, và là dự án phi lợi nhuận nhằm hướng tới việc chia sẻ và chuyển giao kinh nghiệm chuyển đổi số trong hoạt động dạy và học cho các trường trung học phổ thông với mong muốn cùng các đối tác của nhà trường nâng cao năng lực chuyển đổi số trong lĩnh vực giáo dục, góp phần lan tỏa tri thức, hướng đến phát triển bền vững”.*

Hệ thống dạy học trực tuyến UEH Global nói riêng và dự án cộng đồng “Hỗ trợ chuyển đổi số miễn phí cho các trường trung học phổ thông” - Global Learning nói chung thể hiện trách nhiệm xã hội của Trường Đại học Kinh tế TP. Hồ Chí Minh trong việc hỗ trợ, kết nối và lan tỏa tri thức. Với mong muốn cùng nhau phát triển, hy vọng dự án sẽ giúp các trường THPT triển khai dạy và học trực tuyến hiệu quả trong điều kiện giãn cách hiện nay, đồng thời, tiến tới đẩy nhanh tiến trình chuyển đổi số, đóng góp cho sự phát triển bền vững của cộng đồng.

Hỗ trợ dạy học trực tuyến cho giáo viên THPT

Đối với sản phẩm dạy học trực tuyến dành cho các giáo viên THPT, hệ thống Global Learning hỗ trợ tạo các khóa học, giảng dạy trực tuyến qua công cụ BigBlueButtonBN có sẵn, đăng tải tài liệu học tập hoặc tài liệu tham khảo, tổ chức làm bài kiểm tra tự luận trực tuyến, trộn đề thi trắc nghiệm và đáp án tự động, tạo các cuộc khảo sát, diễn đàn trả lời, giải đáp thắc mắc và tư vấn cho học sinh.

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Bên cạnh đó, hệ thống dạy học trực tuyến Global Learning còn tích hợp Hệ thống chấm thi trắc nghiệm: <https://chamthitracngkiem.ueh.edu.vn/> được UEH xây dựng dựa trên công nghệ trí tuệ nhân tạo (AI). Sau khi học sinh làm bài kiểm tra bằng hình thức thi trắc nghiệm trên mẫu giấy trắc nghiệm sử dụng thi tốt nghiệp THPT, Quý Thầy Cô sử dụng máy quét thông thường để quét bài thi trắc nghiệm của học sinh và tải lên website, hệ thống sẽ gửi kết quả về email của Quý Thầy Cô. Quý Thầy cô xem hướng dẫn sử dụng hệ thống dạy học trực tuyến chi tiết tại [đây](#).

Khóa luyện thi tốt nghiệp trực tuyến dành cho học sinh THPT, đặc biệt học sinh lớp 12

UEH triển khai khóa luyện thi tốt nghiệp THPT trực tuyến dành cho học sinh THPT, sản phẩm này là kho dữ liệu tích hợp toàn bộ đề thi các môn học Toán, Lý, Hóa, Sinh, Sử, Địa, Giáo dục công dân từ năm 2015 đến nay, tích hợp với tính năng tự chấm điểm. Nhờ đó, học sinh lớp 11, 12 có thể tự ôn luyện và tự đánh giá trình độ kiến thức của bản thân, chuẩn bị tốt hơn cho kỳ thi cuối cấp. Đây cũng là cơ hội để các bạn học sinh làm quen dần với môi trường học tập và ôn luyện trực tuyến, rèn luyện tinh thần tự học, sẵn sàng cho các lớp học tích hợp blended-learning (lớp học gồm các giờ học truyền thống kết hợp với các giờ học trực tuyến) tại môi trường đại học.



Hình 3: Các em học sinh THPT có thể đăng ký và làm bài thi thử trực tuyến ngay tại <https://global.ueh.edu.vn/>

Hệ thống dạy và học trực tuyến Global Learning thể hiện trách nhiệm xã hội của nhà trường trong việc hỗ trợ, kết nối và lan tỏa tri thức. Đây cũng là một trong những dự án nằm trong chiến lược chuyển đổi số chung của Đại học UEH, với mong muốn cùng các đối tác của nhà trường nâng cao năng lực chuyển đổi số trong lĩnh vực giáo dục, góp phần lan tỏa tri thức trong cộng đồng.

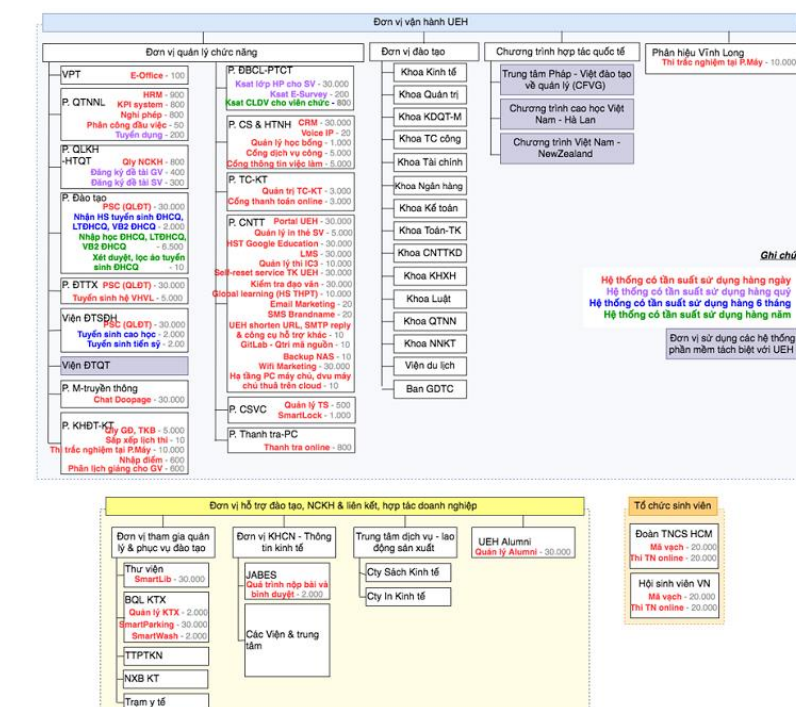
Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Số hóa hoạt động quản lý và giảng dạy

Trọng tâm của việc đẩy mạnh ứng dụng công nghệ vào giảng dạy, quản lý và số hóa các hoạt động chăm sóc sinh viên là nhằm đến định hình và xây dựng đại học thông minh.

Hiểu được tầm quan trọng của việc chuyển đổi số, trong 2 năm trở lại đây, UEH không chỉ quan tâm số hóa bài giảng, các hoạt động quản lý chung qua phần mềm, các ứng dụng tương tác giữa người học với nhà trường, dịch vụ phục vụ sinh viên mà còn triển khai sâu rộng chương trình đào tạo Blended Learning (phương pháp kết hợp giảng dạy truyền thống và E-learning).

TS. Đinh Tiên Minh - Khoa Kinh doanh Quốc tế - Marketing (UEH) cho biết: Từ năm 2016, UEH đã bắt đầu áp dụng mô hình Blended learning vào trong quá trình đào tạo tại các bậc/hệ với phương thức 30% thời lượng môn học cho các hoạt động giảng dạy trực tuyến (online) và 70% cho các hoạt động giảng dạy tại phòng học (offline), trong đó hệ thống LMS-UEH được xây dựng để quản lý và tạo môi trường trực tuyến cho các hoạt động đào tạo.



Hình 4: Bảng mô tả hệ thống phần mềm công nghệ mà UEH đang áp dụng
Xây dựng đại học thông minh

Với những nền tảng hạ tầng và cả tâm thế đã chuẩn bị suốt 3 năm qua, UEH đang đặt mục tiêu chuyển đổi thành đại học thông minh (ĐHTM) trong thời gian ngắn. Theo TS Bùi Quang Hùng - Phó Hiệu trưởng UEH, với ĐHTM, công nghệ trở thành công cụ quan trọng cho học tập, nghiên cứu, phục vụ học tập và các nhiệm vụ liên quan khác.

Trong đó, số hóa các hoạt động giảng dạy, nghiên cứu và các hoạt động khác bằng những phần mềm, thiết bị và công nghệ, tích hợp, chuyển đổi mô thức hoạt động...

sẽ thúc đẩy tinh gọn, hiệu quả, khả năng phân tích, đề ra giải pháp cải thiện môi trường giáo dục đại học cho các đối tượng liên quan.

“Tài nguyên số, nội dung giáo dục mở, môi trường giáo dục ảo, hạ tầng số là 4 yếu tố cơ bản của đại học thông minh V-SMARTH và dạy - học trực tuyến. Tính đến tháng 3/2021, UEH đang có 60 hệ thống, phần mềm được triển khai với tần suất sử dụng và số lượng người dùng khác nhau.

Đối sánh với các chỉ số, điều kiện để tiệm cận đến mô hình ĐHTM theo mô hình Nguyễn Hữu Đức và cộng sự (2020) thì UEH đang đáp ứng tốt 2 kết quả mức độ thông minh (Ci) và mức độ sẵn sàng (Ri). Đây là điều khiến chúng tôi tự tin sớm xây dựng UEH trở thành một ĐHTM”, TS Hùng nói.

Kết luận

Trong những năm gần đây, thành tựu khoa học công nghệ cùng với sự phát triển của Cách mạng công nghiệp 4.0 đã trở thành lực lượng sản xuất trực tiếp, góp phần tạo ra một hình thức phát triển mới mà điển hình là vấn đề số hóa và công nghệ thông tin kết nối vạn vật. Bên cạnh đó, đại dịch Covid-19 bùng phát trên phạm vi toàn cầu đã khiến mọi hoạt động kinh tế - xã hội bị đình trệ. Những yếu tố khách quan đó đặt ra vấn đề chuyển đổi số trong giáo dục đào tạo và đổi mới quản lý giáo dục. Kỹ thuật máy học có thể coi là giải pháp hiệu quả cho việc khai thác dữ liệu trong bối cảnh chuyển đổi số trong giáo dục đại học hiện nay.

Nghiên cứu các giải pháp tổ chức chuyển đổi số và khai thác dữ liệu trong quản lý đào tạo của trường đại học là một nhu cầu cấp thiết, đặc biệt là lượng hóa các tiêu chí hướng tới số hóa và đưa vào chuyển đổi số không chỉ đáp ứng nhu cầu cấp thiết trong quản lý đào tạo của nhà quản lý trường đại học trong bối cảnh hiện nay, góp phần mang lại lợi ích thiết thực cho việc nghiên cứu chuyên sâu và giải quyết các bài toán dự báo trong khoa học, quản lý, khoa học giáo dục mà còn là bước cơ bản không thể thiếu trong quá trình chuyển đổi số giáo dục và đào tạo. Đây là cách tiếp cận bước đầu cho sự ra đời và phát triển mạnh mẽ của một xu hướng nghiên cứu mới – ứng dụng trí tuệ nhân tạo (AI) trong giáo dục.

Xung đột lợi ích: Tác giả tuyên bố rằng không có bất kỳ xung đột lợi ích nào khi thực hiện nghiên cứu này.

TÀI LIỆU THAM KHẢO

Nguyễn Thị Ngọc Anh (2019), Quản lý đào tạo thực hiện quyền tự chủ và trách nhiệm xã hội của các trường đại học địa phương trong bối cảnh đổi mới giáo dục, Luận án tiến sĩ khoa học giáo dục, Viện Khoa học Giáo dục Việt Nam.

Sang, L.H., Điện, T.T., Nghe, N.T., & Hải, N.T. (2020), *Dự báo kết quả học tập bằng kỹ thuật học sâu với mạng nơ-ron đa tầng*, Can Tho University Journal of Science,

56(3)(June), tr.20-28, <https://doi.org/10.22144/ctu.jvn.2020.049>, ngày cập nhật 10/09/2023.

Nguyễn Hữu Đức (2019), Nghiên cứu mô hình trường đại học đáp ứng với cuộc cách mạng công nghiệp 4.0, Đề tài cấp quốc gia KHGD/16-20.ĐT.007, Trường Đại học Công nghệ - ĐHQGHN.

Trần Văn Tùng (2013), *Quản lý đào tạo trong các trường đại học Việt Nam theo tiếp cận quản lý theo kết quả (RBM)*, Luận án tiến sĩ Giáo dục học, Trường Đại học Giáo dục, Đại học Quốc gia Hà Nội.

Romeo, C and Ventura, S. 2010. Education Data Mining: A review of the State of the Art, IEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), Vol. 49, No. 6, pp 601-618, DOI: 10.1109/TSMCC.2010.2053532.

Vladimir L. Uskov, Eddited by Robert J. Howlett, Edited by Lakhmi C. Jain (2017), *SmartEducation and e-Learning*, Springer International Publishing AG, ISBN10 3319594508.

THỰC TRẠNG VÀ GIẢI PHÁP PHÁT TRIỂN KỸ NĂNG THẨM ĐỊNH THÔNG TIN TRÊN MẠNG XÃ HỘI CHO SINH VIÊN

CURRENT STATUS AND SOLUTIONS TO DEVELOP INFORMATION APPRAISAL SKILLS ON SOCIAL NETWORKS FOR STUDENTS

ThS. Trần Minh Tú¹, ThS. Trương Thanh Văn²

¹Trường Đại học Kinh Tế - Tài Chính TP. Hồ Chí Minh

²Ngân hàng TMCP Ngoại Thương Việt Nam

*Tác giả liên hệ: ThS. Trần Minh Tú

(ĐTDD: 097.1989.784 ; Email: tutm@uef.edu.vn)

THÔNG TIN	TÓM TẮT
<i>Từ khóa:</i> An ninh mạng, sinh viên, thẩm định	Nền tảng mạng xã hội hiện nay được sử dụng rất phổ biến với mọi lứa tuổi từ khắp nông thôn lên thành thị. Bên cạnh những tiện ích của mạng xã hội về phát triển tri thức, tiếp cận thông tin, hay giải trí,... thì mạng xã hội cũng có tác động tiêu cực về vấn đề an ninh, như là tin giả, các tiềm ẩn rủi ro trong quá trình sử dụng cơ sở dữ liệu trong học tập. Sinh viên cần nhận thức rõ ràng về những mối đe dọa trên mạng xã hội, thẩm định rõ ràng thông tin, vấn đề trước khi sử dụng bằng cách hiểu rõ về luật an ninh, tham gia các khoá hướng dẫn về an ninh mạng và trao đổi thêm với các bên liên quan khác. Việc thẩm định thông tin là rất cần thiết, và hơn hết cần được quan tâm bởi nhà trường. Bằng cách này, sinh viên có thể cập nhật thêm các cách phòng tránh tin giả, cách thẩm định thông tin một cách chuẩn xác từ những người có nghiên cứu, có kinh nghiệm trong thẩm định thông tin.
<i>Keywords:</i> Cyber security, students, appraisal	ABSTRACT Social networks are commonly used by all ages from rural to urban areas. Besides the benefits of social networks in terms of developing knowledge, accessing information, or entertainment,... social networks also

have negative impacts on security issues, such as fake news, potential threats, etc. Hidden risks in the process of using databases in learning. Students need to be clearly aware of threats on social networks, clearly evaluate information and issues before using them by understanding security laws, and participate in instructional courses on social network security, meetings and discussions with other stakeholders to have a clearer view of cybersecurity issues. Information appraisal is very necessary, and above all needs to be paid attention to by the school. In this way, students can learn more ways to prevent fake news and how to accurately evaluate information from people who have research and experience in evaluating information.

1. Giới thiệu

Trong thời đại cách mạng 4.0 và chuyển đổi số hiện nay, các nền tảng mạng xã hội trực tuyến ngày càng được mở rộng và sử dụng rộng khắp với đủ mọi lứa tuổi, tác động đến mọi mặt của xã hội, làm thay đổi thói quen tiếp nhận tri thức, kiến thức và thông tin của mọi người, trong đó có sinh viên. Hơn nữa, sinh viên luôn phải đối mặt với rất nhiều vấn đề liên quan đến an ninh mạng. Trong môi trường giáo dục đại học, những nhu cầu về học liệu, sử dụng học liệu, thông tin trên mạng xã hội phục vụ cho việc học tập, nghiên cứu, giảng dạy là rất lớn. Do đó, việc tiếp cận được những thông tin cần thiết cho những nhu cầu này cần được chính xác hơn, nhanh chóng hơn. Tuy nhiên, trên mạng xã hội, các vấn đề tin giả mạo, thông tin sai lệch gây ảnh hưởng rất lớn đến những tin tức, kiến thức sinh viên tiếp nhận. Bước vào kỷ nguyên bùng nổ thông tin, khi mà tất cả mọi người thông qua trang cá nhân đều có thể trở thành một kênh tin tức với tốc độ chia sẻ và lan truyền nhanh làm cho việc thẩm định tính chính xác của các thông tin trên mạng xã hội càng trở nên khó khăn hơn. Bên cạnh những nỗ lực xử lý vấn đề tin giả đến từ công ty quản lý các nền tảng mạng xã hội và chính phủ thì người sử dụng mạng xã hội, đặc biệt là sinh viên cần trang bị những kỹ năng để thẩm định những thông tin tiếp cận được từ mạng xã hội. Do vậy, kỹ năng thẩm định thông tin trên mạng xã hội cho sinh viên hiện nay là vô cùng cần thiết.

2. Cơ sở lý thuyết

2.1. Khái quát về chia sẻ và tiếp cận thông tin trên mạng xã hội

Cùng với sự phát triển của công nghệ, xu hướng sử dụng mạng xã hội ngày càng tăng. Năm 2023, Internet Việt Nam phát triển mạnh mẽ với 77 triệu người dùng (tương

ứng 79,1% dân số). Trong đó, số lượng người sử dụng mạng xã hội là 70 triệu người, chỉ tính nền tảng Facebook là 66,2 triệu người. Sự phổ biến của các nền tảng mạng xã hội đã tác động đến nhiều mặt của cuộc sống, từ thói quen sinh hoạt, thói quen mua sắm cho đến cách thức tiếp cận, chia sẻ thông tin (Vnetwork, 2023). Thêm vào đó, mạng xã hội mang đến một không gian chia sẻ thông tin mới cho người dùng. Theo khoản 22, Điều 3 Nghị định số 72/2013/NĐ-CP, ngày 15.7.2013 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng: “Mạng xã hội (social network) là hệ thống thông tin cung cấp cho cộng đồng người sử dụng mạng các dịch vụ lưu trữ, cung cấp, sử dụng, tìm kiếm, chia sẻ và trao đổi thông tin với nhau, bao gồm dịch vụ tạo trang thông tin điện tử cá nhân, diễn đàn (forum), trò chuyện (chat) trực tuyến, chia sẻ âm thanh, hình ảnh và các hình thức dịch vụ tương tự khác” (Trang, 2022).

2.2. Tin giả mạo

Tin giả, trong từ điển tiếng Anh và truyền thông quốc tế gọi là fake news là những thông tin rác, sai lệch được lan truyền với mục đích lừa đảo. Theo Allcott và Gentzkow (2017) thì bất kỳ hình thức làm sai lệch nội dung nào dù cố ý, vô ý hay nhầm lẫn đều được xếp vào danh mục tin giả vì tác động khiến người đọc hiểu lầm. Tại Khoản 1 Điều 5 Nghị định 72/2013/NĐ-CP của Chính Phủ ngày 15/07/2023 cũng đề cập đến những hành vi các hình vi bị cấm đối với việc cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng. Đó là: “a) Chống lại Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; phá hoại khối đại đoàn kết dân tộc; tuyên truyền chiến tranh, khủng bố; gây hận thù, mâu thuẫn giữa các dân tộc, sắc tộc, tôn giáo; b) Tuyên truyền, kích động bạo lực, dâm ô, đồi trụy, tội ác, tệ nạn xã hội, mê tín dị đoan, phá hoại thuần phong, mỹ tục của dân tộc; c) Tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác do pháp Luật quy định; d) Đưa thông tin xuyên tạc, vu khống, xúc phạm uy tín của tổ chức, danh dự và nhân phẩm của cá nhân; đ) Quảng cáo, tuyên truyền, mua bán hàng hóa, dịch vụ bị cấm; truyền bá tác phẩm báo chí, văn học, nghệ thuật, xuất bản phẩm bị cấm; e) Giả mạo tổ chức, cá nhân và phát tán thông tin giả mạo, thông tin sai sự thật xâm hại đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.” (Thư viện pháp luật, 2013).

Tin giả có thể được bắt nguồn từ một cá nhân, nhóm người, tổ chức và thậm chí có thể đến từ các đặc vụ của những quốc gia. Về mục đích, tin giả có thể được lan truyền nhằm trêu chọc người khác, vì thù địch, chuộc lợi hay các lý do chính trị. Tình trạng tin giả mạo ảnh hưởng lớn đến những hiểu biết, kiến thức của người đọc. Rộng hơn thì tin giả có thể ảnh hưởng đến kinh tế, chính trị và cả hội thông qua việc lan truyền những thông tin dẫn dắt dư luận từ các đối tượng có động cơ xấu (Trang, 2022).

3. Phương pháp nghiên cứu

Phương pháp thu thập dữ liệu và xử lý thông tin được sử dụng trong bài nghiên cứu. Thu thập tài liệu từ những công trình nghiên cứu khoa học, bài báo và tài liệu nghiên cứu có liên quan đến công nghệ số trong ngành giáo dục đào tạo. Tìm ra khoảng trống nghiên cứu, đồng thời kế thừa lý luận khoa học, để xây dựng cơ sở lý thuyết về vấn đề nghiên cứu. Thêm vào đó, phương pháp phân tích và tổng hợp lý thuyết cũng được sử dụng. Nhóm tác giả phân chia các thông tin thu thập được thành các bộ phận riêng biệt từ những tài liệu có sẵn. Từ đó, phát hiện ra những đặc điểm chung của đối tượng nghiên cứu, lưu lại những thông tin quan trọng liên quan trực tiếp đến vấn đề nghiên cứu. Liên kết, sắp xếp tài liệu, thông tin lý thuyết đã thu được. Từ đó tạo tiền đề, hệ thống lý thuyết về chủ đề của nghiên cứu.

4. Kết quả nghiên cứu và thảo luận

4.1. Kết quả nghiên cứu

4.1.1. Tầm quan trọng và thực trạng của kỹ năng thẩm định thông tin trên mạng xã hội của sinh viên

Internet và mạng xã hội đang trở thành nguồn thông tin lớn nhất hiện nay. Mỗi khi truy cập vào các nền tảng mạng xã hội ta sẽ thấy rất nhiều bài viết, hình ảnh, video được chia sẻ. Những thông tin được chia sẻ này không hẳn là sự thật. Tin giả không chỉ được lan truyền qua hình thức truyền miệng mà còn đang được lan truyền nhanh chóng thông qua mạng xã hội. Với tính chất tự do, mở rộng, lan truyền nhanh và dễ ẩn danh thì mạng xã hội đang trở thành công cụ cho việc lan truyền những thông tin sai lệch, độc hại và thường là với mục đích xấu. Con người chúng ta thường bị ảnh hưởng về quan điểm, suy nghĩ và những quyết định quan trọng dựa trên những tin tức mà ta tiếp cận. Đó là lý do vì sao tiếp nhận những thông tin chính xác vô cùng quan trọng đặc biệt là đối với sinh viên. Sinh viên là những bạn trẻ đang trong giai đoạn học hỏi và hoàn thiện nhận thức. Với đặc tính tò mò và thường xuyên sử dụng mạng xã hội nên khả năng tiếp cận các thông tin giả mạo cao. Sinh viên có thể nhìn thấy nhiều bài đăng và hình ảnh lan truyền khác nhau tác động đến tâm lý của các bạn với mọi thứ trong cuộc sống. Một lý do khiến tin giả ảnh hưởng nhiều đến sinh viên là hiện nay rất nhiều sinh viên sử dụng mạng xã hội chưa có thể thẩm định được tính chính xác của những thông tin được tiếp cận. Sự thiếu hụt kỹ năng này cũng góp phần gia tăng sự lan truyền của tin tức giả mạo. Chính vì thế, kỹ năng thẩm định thông tin trên mạng xã hội của sinh viên là vô cùng cần thiết.

Tuy nhiên, theo các nghiên cứu, nhiều người trẻ không có khả năng phân biệt thông tin thật và giả tìm thấy trên mạng. Nghiên cứu đã khảo sát 7.804 học sinh từ độ tuổi trung học cơ sở đến tuổi đại học, đặt câu hỏi về thông tin trực tuyến. Kết quả cho thấy khả năng suy luận của các bạn trẻ về những thông tin tìm thấy trên mạng là rất yếu.

Trong một phần của nghiên cứu, 44 sinh viên từ ba trường đại học đã được cho xem qua một dòng tweet (dòng tin trên nền tảng mạng xã hội Twitter) về việc kiểm soát súng từ một trang thông tin thuộc cánh tả⁷⁹ và hỏi về độ tin cậy của thông tin này, kết quả cho thấy chưa đến một phần ba số lượng sinh viên nhận ra có yếu tố thiên vị, thành kiến trong tin tức này. Một khảo sát tương tự, các sinh viên được cho xem một tin tức về mức lương tối thiểu được đăng tải từ trang web được tài trợ bởi một công ty vận động cho cánh tả, sau đó được hỏi về độ ưu tín của tin tức. Theo kết quả nghiên cứu, 93% sinh viên đại học và 91% học sinh trung học được khảo sát chưa bao giờ kiểm tra các trang web khác để xem thông tin có uy tín hay không (Haut, & Writer, 2017). Thêm vào đó, năng lực đánh giá thông tin của sinh viên thông qua nghiên cứu năng lực đánh giá chính xác nội dung thông tin trong học liệu. “Về việc lựa chọn các tiêu chí, nghiên cứu cho thấy hầu hết sinh viên Việt Nam đã biết lựa chọn các tiêu chí quan trọng để đánh giá chất lượng học liệu. Tuy nhiên, chỉ có “27,5%” lựa chọn đầy đủ các tiêu chí đúng với đáp án. Về khai thác thông tin, kỹ năng đọc và khai thác thông tin trong học liệu của sinh viên vẫn còn hạn chế, khả năng bao quát, nhận dạng thông tin quan trọng chưa thành thạo. Chỉ có “50%” sinh viên được hỏi trả lời đáp án đúng về câu hỏi điều tra nghiên cứu kỹ năng đọc và khai thác.” (Quý, 2015).

4.1.2 Kinh nghiệm về kỹ năng thẩm định thông tin tại các nước tiên tiến

Ngày càng nhiều bang ở Mỹ yêu cầu các trường học dạy học sinh cách đánh giá thông tin trên internet và mạng xã hội. Điển hình tại Tiểu bang California, Thống đốc Jerry Brown đã ký một đạo luật nhằm giúp các nhà giáo dục dạy cho học sinh các kỹ năng “kiến thức truyền thông” (09/2018). Luật mới yêu cầu Bộ Giáo dục California cung cấp các tài liệu liên quan đến kiến thức truyền thông trên trang web của mình. Các tài liệu này được thiết kế để cung cấp thông tin cho giáo viên và cung cấp công cụ để họ giảng dạy môn học. Thượng nghị sĩ bang California Bill Dodd đề xuất dự luật và trở thành luật. Ông cho biết mục tiêu là cung cấp cho sinh viên một bộ công cụ hiệu quả để “trao quyền cho họ đưa ra quyết định sáng suốt”. Ông nói thêm rằng kiến thức tin tức rất quan trọng đối với sinh viên và xã hội để giúp “bảo vệ tương lai của nền dân chủ”. Dự luật được thông qua ở California tương tự như dự luật được thông qua năm 2017 ở Bang Washington. Nó tạo ra một hệ thống tài liệu dựa trên web dành cho giáo viên. Luật Washington cũng yêu cầu các quan chức giáo dục báo cáo về cách họ dự định bổ sung chương trình giáo dục kiến thức truyền thông cho các trường học địa phương (VOA, 2018).

Hơn nữa, một dự luật đã được xem xét ở New Mexico. Dự luật đưa ra yêu cầu mới về bộ môn “kỹ năng sống”. Dự luật sẽ yêu cầu sinh viên học kiến thức truyền thông

như một phần của lớp học về kỹ năng sống để tốt nghiệp. Một đề xuất trước cơ quan lập pháp Hawaii sẽ phát triển một kế hoạch toàn tiểu bang để dạy các kỹ năng hiểu biết về truyền thông ở tất cả các cấp trong các trường công lập. Theo Hutchinson, và Brumpton (2022), thư viện trường học và nhân viên thư viện có thể đóng vai trò quan trọng trong việc hỗ trợ sinh viên phát triển kỹ năng, kiến thức truyền thông và kỹ thuật số đặc biệt là về thông tin sai lệch và tin tức giả mạo. Hutchinson & Brumpton cho rằng kiến thức thông tin và truyền thông (MIL) nên được dạy ở trường một cách có phương pháp và cách các thủ thư tại trường học có thể đóng vai trò quan trọng trong chương trình giảng dạy MIL (Hutchinson & Brumpton, 2022). UNESCO tuyên bố rằng “MIL tạo thành một tập hợp tổng hợp các kiến thức, kỹ năng, thái độ, năng lực và thực hành cho phép sinh viên tiếp cận, phân tích, đánh giá phản biện, diễn giải, sử dụng, tạo ra và phổ biến các sản phẩm thông tin và truyền thông bằng cách sử dụng các phương tiện và công cụ hiện có một cách hiệu quả”. trên cơ sở sáng tạo, hợp pháp và đạo đức” (UNESCO, 2022).

4.1.3 Giải pháp phát triển kỹ năng thẩm định thông tin mạng xã hội cho sinh viên

Trước tình hình tin tức giả mạo ngày càng lan rộng và kỹ năng thẩm định thông tin trên mạng xã hội của sinh viên còn hạn chế dẫn đến nhiều tác hại. Để nâng cao được kỹ năng thẩm định thông tin, để việc sử dụng mạng xã hội của sinh viên thật sự mang lại những tác động tích cực.

4.1.3.1 Về phía sinh viên

Về phía bản thân sinh viên, cần xác định mục đích sử dụng mạng xã hội lành mạnh. Mạng xã hội nên được sinh viên sử dụng như một phương tiện phục vụ hoạt động học tập, nghiên cứu, giải trí và chia sẻ thông tin tích cực. Hơn nữa, sinh viên cần biết và hiểu về luật An ninh mạng do Quốc hội ban hành ngày 12/06/2018. Nắm bắt được những biện pháp bảo vệ an ninh mạng, những hành vi bị cấm để có những hành vi và nhận thức đúng về những thông tin tiếp cận trên mạng xã hội. Nâng cao hiểu biết về chính trị, xã hội tránh tác động của các thế lực thù địch. Trau dồi kiến thức và trải nghiệm bản thân, những hiểu biết của bản thân sẽ góp phần nhận định được chất lượng của tin tức. Chia sẻ và vận động bạn bè cảnh giác trước những thông tin giả mạo và sử dụng mạng xã hội một cách văn minh, tích cực. Ngăn chặn và chủ động tố cáo những hành vi phát tán, lan truyền tin tức giả mạo.

Thêm vào đó là luôn có sự thẩm định, kiểm tra khi đọc những thông tin trên mạng xã hội. Một là, kiểm tra nguồn đăng tải tin tức. Một trong những cách hiệu quả nhất để xác định dữ liệu giả là xác minh nguồn của nó. Kiểm tra địa chỉ web nếu nội dung đó đến từ một nguồn chưa từng nghe đến trước đây thì rất có thể đó là nội dung giả mạo. Kiểm tra các tên miền lạ, rất nhiều trang web giả mạo sử dụng tên miền không phổ biến chẳng hạn như .asia, .vip, .tk, .xyz... Kiểm tra mọi lỗi chính tả của tên công ty trong địa chỉ URL, thiếu, thừa ký tự hoặc sử dụng một ký tự gần giống (shopee.vn, kenh14.vn,...).

Sử dụng phần mềm bảo mật và phòng chống tên miền độc hại như Norton, McAfee, Kaspersky và Avast. Nhiều khi kẻ gian còn giả mạo website hoặc các trang web của các công ty, tổ chức có uy tín để tung tin giả. Tìm kiếm website hay công ty, tổ chức đó trên các công cụ tìm kiếm và so sánh tên miền với trang đang đăng tải tin tức (Anon, 2019). Hai là, kiểm tra người đăng tải, chia sẻ thông tin. Truy cập trang cá nhân của người đăng tải kiểm tra tần suất đăng tải bài viết, thời gian lập tài khoản, số lượng bạn bè, người theo dõi, hình ảnh,... hay những dấu hiệu nghi ngờ đó là tài khoản giả. Những thông tin đăng tải, chia sẻ từ những tài khoản không chính chủ thông thường có độ tin cậy thấp. Ba là, kiểm tra lại tính chính xác của thông tin trên một trang tin khác. Sinh viên cần kiểm tra xem những tin tức đó có chính xác hay không bằng cách sử dụng các trang web khác để tìm những tin tức tương tự. Nếu tin tức này có được đăng tải trên những trang thông tin uy tín hàng đầu thì có thể nói tin tức này là tin thật, còn nếu không thể tìm kiếm được thông tin thì khả năng cao đây là tin giả mạo. Tìm hiểu và nắm bắt được những trang tin tức uy tín để kiểm chứng thông tin, có thể kể đến là Dân trí - tờ báo điện tử trực thuộc Trung ương Hội khuyến học Việt Nam, Vietnamnet - nhật báo online của Bộ thông tin và truyền thông Việt Nam, Báo Lao Động - cơ quan thông tin của Liên đoàn Lao động Việt Nam, Báo Thanh Niên - tờ báo cách mạng đầu tiên của Việt Nam do Bác Hồ sáng lập,... (Bộ Thông tin và Truyền thông, 2023).

4.1.3.2 Đối với nhà trường

Nhà trường cần xây dựng và lồng ghép vào chương trình giảng dạy những kỹ năng từ cơ bản đến nâng cao về thẩm định thông tin trên mạng xã hội. Việc cập nhật thông tin vào bài giảng là cần thiết để sinh viên có thể học hỏi và tiếp thu nhanh chóng. Phổ biến đến sinh viên về những vấn đề do tin giả gây ra và nâng cao ý thức về tin giả bằng cách áp dụng các bài tập tình huống thực tế, các câu chuyện đã xảy ra trong thực tế. Bằng cách này, sinh viên có thể hiểu rõ hơn và thấy được tầm quan trọng của việc thẩm định thông tin trên mạng xã hội một cách hiệu quả. Từ đó, tại một thói quen cảnh giác, kiểm chứng thông tin cho sinh viên, cũng như lọc thông tin một cách dễ dàng trong việc học tập và phát triển bản thân bên ngoài xã hội.

4.2. Thảo luận

Mạng xã hội ngày càng phổ biến và dần đang trở thành kênh chia sẻ, tiếp cận thông tin, cung cấp tin tức, kiến thức về mọi lĩnh vực cuộc sống. Mạng xã hội còn tạo điều kiện cho các bạn trẻ chia sẻ quan điểm, kiến thức của mình và thuận lợi cho việc học tập, tiếp thu kiến thức thông qua các hội nhóm, bài viết chia sẻ kiến thức. Đặc biệt, sau đại dịch COVID19 thì hoạt động học tập, chia sẻ thông tin qua mạng xã hội càng được xem trọng hơn. Bên cạnh những tác động tích cực thì thông tin chia sẻ trên mạng xã hội cũng có nhiều biến tướng, độc hại. Do đó, sinh viên cần nhận thức rõ ràng về những mối đe dọa trên mạng xã hội, thẩm định rõ ràng thông tin, vấn đề trước khi sử

dụng bằng cách hiểu rõ về luật an ninh, tham gia các khoá hướng dẫn về an ninh mạng và trao đổi thêm với các bên liên quan khác để nắm rõ hơn về cách phòng tránh những thông tin tiềm ẩn rủi ro. Việc thẩm định thông tin là rất cần thiết, và hơn hết cần được quan tâm bởi nhà trường. Nhà trường cần phối hợp với các ban ngành, hoặc Đại học An Ninh để tạo các buổi hội thảo, hướng dẫn sinh viên, cũng như nâng cao khả năng thẩm định thông tin trên mạng xã hội. Bằng cách này, sinh viên có thể cập nhật thêm các cách phòng tránh tin giả, cách thẩm định thông tin một cách chuẩn xác từ những người có nghiên cứu, có kinh nghiệm trong thẩm định thông tin.

5. Kết luận

Nền kinh tế tri thức cần gắn liền với kho kiến thức chất lượng để phục vụ cho nhu cầu học tập, nghiên cứu, và tìm kiếm thông tin. Do đó, việc thay đổi cách nhìn về thẩm định thông tin giả mạo trên mạng xã hội là cần thiết. Và hơn nữa, làm thế nào để hướng dẫn cho sinh viên hiểu rõ được tầm quan trọng của việc này cũng là cả một quá trình. Tiếp theo đó, sinh viên cũng phải ý thức tìm hiểu về cách phòng tránh, cách thẩm định thông tin giả mạo trên các nền tảng mạng xã hội. Từ đó có thể tự chủ trong việc phòng tránh sự sai lệch thông tin. Và hơn hết, từ ghế nhà trường, giảng viên cần chú trọng hơn trong quá trình giảng dạy, cập nhật thêm kiến thức cho sinh viên trong việc thẩm định những nội dung chất lượng, những nội dung giả mạo, xuyên tạc trên mạng xã hội một cách rõ ràng. Từ đó, sinh viên có thể trao đổi và phát triển bản thân, góp phần phát triển nền tri thức một cách nhanh chóng và dễ dàng hơn.

Tài liệu tham khảo

- Anon, (2019). [Online] Available at: <https://www.bbc.co.uk/news/education-44454844> 14/04/2019 [Accessed 24 Apr. 2019].
- Quý, T. T. . (2018). *Trường Đại học KHXH&NV, Đại học Quốc Gia Hà Nội* . Retrieved from Năng lực thông tin của sinh viên Việt Nam: https://repository.vnu.edu.vn/bitstream/VNU_123/11613/1/OERBook%285%29.pdf
- Haut, S., & Writer, S. (2017). *The Ithacan*. Retrieved from Students lack awareness of fake news: <https://theithacan.org/14403/news/students-lack-awareness-of-fake-news/>
- Hutchinson, E. (2022). *Headteacher* . Retrieved from Media, information literacy and fake news: Using the skills of your school librarian : <https://www.headteacher-update.com/content/best-practice/media-information-literacy-and-fake-news-using-the-skills-of-your-school-librarian/>
- Trang, N., T. (2022). *Tạp chí Lý Luận Chính Trị*. Retrieved from Mạng xã hội và những thách thức đối với công tác thông tin, tuyên truyền, bảo vệ an ninh tư tưởng và đấu tranh phản bác các luận điệu sai trái, thù địch ở nước ta hiện nay:

<https://lyluanchinhtrivatruyenthong.vn/mang-xa-hoi-va-nhung-thach-thuc-doi-voi-cong-tac-thong-tin-tuyen-truyen-bao-ve-an-ninh-tu-tuong-va-dau-tranh-phan-bac-cac-luan-dieu-sai-trai-thu-dich-o-nuoc-ta-hien-nay-p26061.html>

Thư viện Pháp luật. (2013). *Thư viện Pháp luật*. Retrieved from Nghị định quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng : <https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-72-2013-ND-CP-quan-ly-cung-cap-su-dung-dich-vu-Internet-va-thong-tin-tren-mang-201110.aspx>

Tuyết, Đ. T., & Hạnh, V. T. (2023). *Hội đồng Lý Luận Trung ương*. Retrieved from Ảnh hưởng và hậu quả của tin giả (Fake News) trên không gian mạng đến chính trị, kinh tế, xã hội: <https://hdl.vn/vi/nghien-cuu---trao-doi/anh-huong-va-hau-qua-cua-tin-gia-fake-news-tren-khong-gian-mang-den-chinh-tri-kinh-te-xa-hoi.html>

VOA. (2018). *VOA Education*. Retrieved from More US Schools Teaching Skills to Recognize False News: <https://learningenglish.voanews.com/a/more-us-schools-teaching-skills-to-recognize-false-news/4586357.html>

Vnetwork. (2023). *Vnetwork*. Retrieved from Internet Việt Nam 2023: Số liệu mới nhất và xu hướng phát triển: <https://www.vnetwork.vn/news/internet-viet-nam-2023-so-lieu-moi-nhat-va-xu-huong-phat-trien>

NÂNG CAO NĂNG LỰC NHẬN DIỆN, CẢNH GIÁC TRƯỚC THÔNG TIN XẤU, ĐỘC TRÊN KHÔNG GIAN MẠNG CHO SINH VIÊN TRƯỜNG ĐẠI HỌC AN NINH NHÂN DÂN

Thiếu tá, ThS. Phạm Thị Thu,

Khoa Tâm lý – Trường Đại học An ninh nhân dân

Email: ptthuk53@gmail.com.vn

THÔNG TIN	TÓM TẮT
Từ khóa: Năng lực nhận diện, cảnh giác; Thông tin xấu, độc; Không gian mạng; Sinh viên; Trường Đại học An ninh nhân dân.	Bài viết trình bày lý luận về thông tin xấu, độc trên không gian mạng. Tác động tiêu cực của thông tin xấu, độc trên không gian mạng đến sinh viên đặc biệt là sinh viên Trường Đại học An ninh nhân dân. Trên cơ sở đó đưa ra một số biện pháp nhằm nâng cao năng lực nhận diện, cảnh giác trước thông tin xấu, độc trên không gian mạng cho sinh viên Trường Đại học An ninh nhân dân.

1. Hiện nay, với sự phát triển của công nghệ thông tin, xu hướng sử dụng không gian mạng ngày càng gia tăng, tác động lớn tới không gian sống thực của con người. Không chỉ đem đến nguồn thông tin vô tận, không gian mạng còn là nơi kết nối xã hội loài người, thúc đẩy sản xuất, kinh doanh và gia tăng giá trị cuộc sống. Tuy nhiên, không gian mạng với đặc tính “ảo”, dễ ẩn danh, lan truyền nhanh đã trở thành môi trường thuận lợi cho hoạt động phát tán thông tin xấu, độc.

Theo kết quả khảo sát năm 2022 từ Công ty Nghiên cứu thị trường DataReportal của Singapore, Việt Nam là một trong số 10 quốc gia có lượng người dùng mạng xã hội nhiều nhất thế giới. Các nền tảng mạng xã hội có lượng người sử dụng lớn như Facebook, Youtube, TikTok, Zalo... đang là môi trường phát tán thông tin xấu, độc phổ biến. Mặt khác, số liệu thống kê năm 2020 của Google cũng cho thấy Việt Nam đứng top 10 các nước có số lượng thông tin vi phạm chính sách bị yêu cầu xử lý. Trước “con bão” thông tin trên không gian mạng, việc nhận diện và cảnh giác với những thông tin xấu, độc là vô cùng cần thiết nhằm phát huy mặt tích cực, ngăn ngừa tác động tiêu cực, góp phần ổn định tình hình chính trị, xã hội của đất nước, xây dựng một môi trường sống an toàn, chất lượng.

Thông tin xấu, độc trên không gian mạng là những thông tin bịa đặt, bóp méo sự thật, xuyên tạc vấn đề, “đổi trắng, thay đen”, làm lẫn lộn đúng sai, thật giả hoặc có một phần sự thật nhưng được đưa tin với dụng ý xấu, phân tích và định hướng dư luận bằng luận điệu thù địch. Đó là các dạng thông tin có nội dung không phù hợp về chuẩn mực đạo đức, văn hóa, thuần phong mỹ tục như kích động bạo lực, bôi nhọ đời tư, vu khống...; thông tin sai trái, độc hại có tính chất tội phạm tin học như lừa đảo trên mạng, đánh cắp thông tin, mật khẩu ... Theo ghi nhận của Cục An toàn thông tin, Bộ

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

Thông tin và Truyền thông trong 6 tháng đầu năm 2023, tình hình lừa đảo trực tuyến tại Việt Nam tăng 64,78% so với cùng kỳ năm ngoái, tăng 37,82 % so với 6 tháng cuối năm 2022; Bên cạnh đó là những thông tin sai trái, độc hại có tính chất chính trị như chống phá nền tảng tư tưởng của Đảng và cách mạng Việt Nam hòng phủ định Chủ nghĩa Mác - Lênin, Tư tưởng Hồ Chí Minh; xuyên tạc, phủ nhận thành tựu, đường lối xây dựng và bảo vệ Tổ quốc, đường lối đối ngoại của Đảng, Nhà nước; xuyên tạc lịch sử dân tộc, nhất là lịch sử các cuộc kháng chiến, các cuộc chiến tranh bảo vệ Tổ quốc của Nhân dân ta; xuyên tạc thân thế, sự nghiệp, công lao to lớn của Chủ tịch Hồ Chí Minh đối với sự nghiệp cách mạng của Đảng, của dân tộc; vu cáo, bôi nhọ thanh danh các đồng chí lãnh đạo cấp cao của Đảng, Nhà nước; lợi dụng uy tín của một số tướng lĩnh trong lực lượng vũ trang để tuyên truyền, xuyên tạc. Nhiều đối tượng đưa thông tin kích động xu hướng ly khai, phá hoại sự thống nhất quốc gia, dân tộc, gây chia rẽ đoàn kết nội bộ, thúc đẩy “tự diễn biến”, “tự chuyển hóa” trong nội bộ; truyền bá lối sống ích kỷ vụ lợi, xa hoa, trụy lạc, bạo lực và thù hận đối với cá nhân và tổ chức, nhất là đối với chủ nghĩa cộng sản và Đảng Cộng sản; phá hoại bản sắc văn hóa dân tộc, tuyên truyền, áp đặt các giá trị văn hóa và lối sống phương Tây, nhất là về văn hóa và chính trị...

Thông tin xấu, độc thường có xu hướng lan truyền nhanh hơn tin chính thống từ các phương tiện truyền thông. Thông tin xấu, độc được các thế lực thù địch, phản động, cơ hội chính trị phát tán trên không gian mạng bằng nhiều phương thức, thủ đoạn mới, tinh vi, xảo quyệt. Chúng lợi dụng các trang mạng lớn như Google, Facebook, kênh Youtube làm công cụ, sử dụng và nhân rộng mạng lưới cộng tác viên rộng khắp để xuyên tạc, chống phá. Đồng thời, tận dụng tối đa những ý kiến, đánh giá, nhận xét của các cá nhân, tổ chức có uy tín, có tầm ảnh hưởng trong và ngoài nước, tạo dựng các trang web, các tài khoản cá nhân trên mạng nói chung, trên Facebook nói riêng để “chia sẻ”, phát tán thông tin xuyên tạc, bịa đặt chống phá. Những thủ đoạn phát tán thông tin xấu, độc bao gồm: Mỗi đối tượng sử dụng một điện thoại smartphone, máy tính bảng để quay phim, chụp ảnh, truyền tải video, hình ảnh livestream trực tiếp, có tác động nhanh chóng, tạo hiệu ứng lan truyền rộng rãi đối với những người sử dụng mạng xã hội; Giả mạo các hình ảnh, video hoặc sử dụng các thông tin cũ có hiệu ứng kích động cao đối với cộng đồng mạng để xuyên tạc, lôi kéo người dân. Giả mạo lực lượng chức năng (công an, quân đội) trà trộn vào lực lượng tham gia biểu tình hoặc có những hành vi phản cảm để quay phim, chụp ảnh phát tán trên mạng xã hội; Tạo hiệu ứng đám đông trên không gian mạng bằng cách huy động một số lượng lớn các tài khoản mạng xã hội (đa số tài khoản ảo) gán các biểu ngữ phản đối Đảng, Nhà nước để tạo ra hiệu ứng đám đông, từ đó người dùng mạng xã hội thường xuyên nhìn thấy các biểu ngữ phản đối hoặc những người không có lập trường tư tưởng vững vàng sẽ bị tác động thay đổi tư tưởng theo chiều hướng tiêu cực; Giả

mạo tài khoản, xây dựng hàng loạt mạng lưới tài khoản, trong đó có một số tài khoản chính thường xuyên đăng tải bài viết, thông tin xuyên tạc về một số nội dung, lĩnh vực nhất định và sử dụng hàng trăm tài khoản vệ tinh (thực chất là tài khoản ảo, có chung một chủ tài khoản) thực hiện nhiệm vụ chia sẻ trong các nhóm diễn đàn phản động hoặc các trang mạng xã hội có lượng thành viên lớn. Đặc biệt, có nhiều tài khoản được thể lực thù địch mạo danh các nhân vật nổi tiếng, có ảnh hưởng đến cộng đồng để phát huy tối đa khả năng lan truyền thông tin gây hoang mang dư luận trong quần chúng nhân dân, kích động người dân tụ tập biểu tình và có hành vi vi phạm pháp luật.

Thông tin tại buổi họp báo thường kỳ của Bộ Thông tin – Truyền thông ngày 6/4/2023, ông Lê Quang Tự Do, Cục trưởng Cục Phát thanh, truyền hình - thông tin điện tử (Bộ Thông tin – Truyền thông), cho biết cơ quan quản lý tổng hợp và chỉ rõ 6 sai phạm của mạng xã hội TikTok tại Việt Nam bao gồm: Không có các biện pháp kiểm soát hiệu quả những nội dung vi phạm liên quan đến chính trị, chống phá Đảng, Nhà nước, tin giả, nội dung nhảm nhí, độc hại, thậm chí gây nguy hiểm với trẻ em; việc sử dụng thuật toán phân phối nội dung tự động để tạo xu hướng (trend) nhằm phát tán những nội dung giật tít, câu view, gây ảnh hưởng xấu đến cộng đồng và giới trẻ; không có biện pháp kiểm soát hiệu quả để ngăn chặn hoạt động kinh doanh, buôn bán, quảng cáo hàng giả, hàng nhái, thực phẩm chức năng không rõ nguồn gốc; không quản lý hoạt động của các idol TikTok, để nhiều idol có xu hướng sản xuất những nội dung nhảm nhí, thiếu văn hóa; không có biện pháp kiểm soát hiệu quả các nội dung vi phạm bản quyền; không có biện pháp quản lý để người dùng tự ý sử dụng hình ảnh riêng tư, cá nhân của người khác để tung tin giả, thông tin xấu, độc, hoặc bôi nhọ, xúc phạm người khác.

Thực tế cho thấy, thông tin xấu, độc trên không gian mạng đã và đang có tác động tiêu cực đến một bộ phận người dùng mạng xã hội trong đó có thanh niên, sinh viên. Với lực lượng đông đảo chiếm hơn 1/3 dân số thanh niên, sinh viên là đối tượng trọng điểm mà các thế lực thù địch, phản động trong và ngoài nước lợi dụng thực hiện âm mưu “diễn biến hòa bình”. Chúng tác động, hướng lái tư tưởng hòng tạo ra một thế hệ trẻ sống theo chủ nghĩa thực dụng, vụ lợi, vị kỷ, sẵn sàng xét đoán quá khứ và vai trò lãnh đạo của Đảng, Nhà nước ta bằng “hệ thống” thông tin xấu, độc, xuyên tạc, thù địch.

2. Trường Đại học An ninh nhân dân là một đơn vị vũ trang trọng yếu, hàng năm cung cấp một số lượng sỹ quan An ninh đáng kể cho các tỉnh, thành phía Nam (từ Quảng Trị trở vào). Vì vậy, Nhà trường rất chú trọng đến công tác đào tạo ngũ sỹ quan an ninh tương lai. Sinh viên Đại học An ninh nhân dân không chỉ “có bản lĩnh chính trị vững vàng, tuyệt đối trung thành với Tổ quốc, với Đảng Cộng Sản Việt Nam, với Nhà nước Cộng hòa xã hội Chủ nghĩa Việt Nam” mà còn phải biết vận dụng học thuyết chủ nghĩa Mác – Lênin, tư tưởng Hồ Chí Minh, đường lối, chủ trương của Đảng, chính sách, pháp luật của Nhà nước vào thực tiễn công tác công an. Nhận thức rõ mạng xã hội là một trong

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

những kênh kết nối, chia sẻ, tiếp nhận thông tin phổ biến và là một phần không thể thiếu trong cuộc sống hàng ngày của sinh viên. Mạng xã hội đem lại nhiều thông tin hữu ích nhưng với sự xuất hiện của “làn sóng” thông tin xấu, độc, mạng xã hội cũng có những tác động tiêu cực ảnh hưởng đến tư tưởng, đạo đức, lối sống của sinh viên. Vì vậy, Nhà trường rất chú trọng đến vấn đề trang bị cho sinh viên kiến thức, kỹ năng để nhận diện, cảnh giác trước thông tin xấu, độc trên không gian mạng.

Khảo sát được thực hiện bằng Google forms đối với sinh viên Trường Đại học An ninh nhân dân cho thấy, bước đầu sinh viên đã có hiểu biết về thông tin xấu, độc trên không gian mạng. Tuy nhiên, phần lớn sinh viên cho rằng thông tin xấu, độc đơn thuần là những thông tin mang tính chất lừa đảo, bôi nhọ, xuyên tạc... mà chưa có sự hiểu biết đầy đủ, chính xác về thông tin xấu, độc trên không gian mạng. Việc nhận diện, cảnh giác trước thông tin xấu độc trên không gian mạng của sinh viên Đại học An ninh nhân dân chủ yếu dừng lại ở việc không phát tán, chia sẻ thông tin của đài, báo, trang mạng, bài viết, blog, video của những phần tử chống đối, phản động. Để nâng cao năng lực nhận diện và sự cảnh giác cần thiết trước thông tin xấu, độc trên không gian mạng cho sinh viên thiết nghĩ cần có những giải pháp đồng bộ từ phía Nhà trường; Các khoa, phòng, trung tâm, tổ chức quần chúng, đội ngũ giảng viên và từ chính bản thân sinh viên.

Thứ nhất về phía Nhà trường, cần chú trọng công tác giáo dục chính trị, tư tưởng cho sinh viên. Nghị quyết Đại hội XIII của Đảng xác định: “Tư tưởng chỉ đạo xuyên suốt của toàn Đảng, toàn dân và toàn quân ta là phải kiên định và vận dụng, phát triển sáng tạo chủ nghĩa Mác – Lênin, tư tưởng Hồ Chí Minh, kiên định mục tiêu độc lập dân tộc và chủ nghĩa xã hội; kiên định đường lối đổi mới của Đảng; kiên định các nguyên tắc xây dựng Đảng. Đây là vấn đề mang tính nguyên tắc, có ý nghĩa sống còn đối với chế độ ta, là nền tảng vững chắc của Đảng ta, không cho phép ai được ngả nghiêng, dao động”. Làm tốt công tác giáo dục chính trị, tư tưởng giúp sinh viên góp phần hình thành, bồi dưỡng thế giới quan, nhân sinh quan, phương pháp luận khoa học; trang bị những kiến thức cơ bản về tư tưởng Hồ Chí Minh, đường lối cách mạng của Đảng Cộng sản Việt Nam góp phần hình thành niềm tin vào Đảng, vào con đường đi lên chủ nghĩa xã hội. Những kẻ reo rắc thông tin xấu, độc trên không gian mạng có thể tạo ra những tin giả hoặc những tin mang tính chất nguy hiểm ở trình độ cao khiến người dùng mạng xã hội rất dễ bị mắc lừa. Nhưng nếu sinh viên được giáo dục chính trị, tư tưởng tốt sẽ có bản lĩnh, lý luận vững vàng, am hiểu thực tiễn chính trị, xã hội và sự tự tin để nhận diện, cảnh giác và cao hơn là phản biện, chống lại các thông tin xấu, độc, bảo vệ đất nước, bảo vệ chế độ.

Nhà trường cũng cần đẩy mạnh việc quán triệt và thực hiện nghiêm túc trong toàn trường những văn bản liên quan như: Nghị Quyết 35-NQ/TW, ngày 28/10/2018 của Bộ Chính trị về “Tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản

Kỷ yếu Hội thảo Khoa học: “An ninh Sinh viên trong thời kỳ Chuyển đổi số”

bác các quan điểm sai trái, thù địch trong tình hình mới”, Đề án số 08/ĐA-BCA-A03 ngày 29/9/2021 của Bộ Công an về “Công tác tăng cường bảo vệ nền tảng tư tưởng của Đảng, đấu tranh phản bác các quan điểm sai trái, thù địch trong tình hình mới”; Luật An ninh mạng được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ 5 thông qua ngày 12/6/2018 và có hiệu lực thi hành từ 01/01/2019; “Quy trình công tác công an phát hiện, đấu tranh, xử lý tin giả, tin sai sự thật trên internet, mạng xã hội” do Bộ Công an ban hành ngày 18/5/2022; Hướng ứng chiến dịch “Tháng hành động tuyên truyền về nhận diện và phòng chống lừa đảo trực tuyến” triển khai từ ngày 23/6 đến ngày 23/7/2023 dưới sự chủ trì Cục An toàn thông tin (Bộ Thông tin và Truyền thông), phối hợp cùng thành viên Liên minh tuyên truyền nâng cao nhận thức và kỹ năng đảm bảo an toàn thông tin, nhận diện, cảnh giác trước thông tin xấu, độc trên không gian mạng.

Nhà trường cần tích cực trong công tác tuyên truyền, giáo dục sinh viên nâng cao cảnh giác, phòng chống âm mưu, hoạt động “diễn biến hòa bình” nhằm phát huy sức mạnh tổng hợp của các khoa, phòng, trung tâm, tổ chức quần chúng (Đoàn thanh niên, Hội phụ nữ, Công Đoàn) trường trong công tác giúp sinh viên nhận diện, phòng ngừa, đấu tranh với thông tin xấu, độc trên không gian mạng. Khi xuất hiện thông tin xấu, độc, cần kịp thời “giải độc” thông tin nhanh chóng bằng nguồn tin xác thực, tin cậy giúp sinh viên nắm rõ bản chất vấn đề. Bên cạnh đó cần duy trì, khiêu khai các biện pháp đấu tranh, ngăn chặn, bóc gỡ, xác minh, xử lý nghiêm các trường hợp tung tin sai sự thật, tin xấu, độc trong sinh viên.

Thứ hai về phía các khoa, phòng, trung tâm, tổ chức quần chúng và đội ngũ giảng viên. Các đơn vị trong Nhà trường cần tích cực thực hiện công tác tuyên truyền nâng cao năng lực nhận diện, cảnh giác trước thông tin xấu, độc trên không gian mạng cho sinh viên. Xây dựng, triển khai chương trình ngoại khóa tập huấn kỹ năng nhận diện, cảnh giác trước thông tin xấu, độc trên không gian mạng. Khoa An ninh chính trị nội bộ xây dựng nội dung, chương trình tập huấn, báo cáo thực tế về đấu tranh phản bác quan điểm sai trái, thù địch, trong đó có nhận diện, cảnh giác với thông tin xấu, độc trên không gian mạng. Khoa Ngoại ngữ - Tin học tổ chức các buổi tập huấn về kỹ năng an toàn thông tin, kỹ năng sử dụng mạng xã hội an toàn cho sinh viên. Khoa Tâm lý tổ chức tập huấn về kỹ năng giao tiếp, văn hóa ứng xử trên mạng xã hội cho sinh viên...

Duy trì việc quản trị các diễn đàn, trang fanpage của Đoàn thanh niên như fanpage Lá Trung Quân, Câu lạc bộ văn nghệ xung kích, Câu lạc bộ kỹ năng... Thực hiện tốt công tác truyền thông, đăng tải bài viết tuyên truyền chủ trương, chính sách của Đảng, pháp luật của Nhà nước, phản ánh những vấn đề mang tính thời sự, vạch trần âm mưu, thủ đoạn của các thế lực thù địch giúp sinh viên có nhận thức đúng đắn, cập nhật thông tin đầy đủ, kịp thời. Đồng thời, cần phát huy vai trò của tổ chức quần chúng: Đoàn thanh

niên, Hội phụ nữ, Công Đoàn trường trong công tác tuyên truyền, giáo dục nâng cao kỹ năng nhận diện, cảnh giác trước thông tin xấu, độc trên mạng xã hội.

Đối với cán bộ, giảng viên cần chú trọng đến vấn đề nêu gương. Mỗi cán bộ, giảng viên là tấm gương sáng về đạo đức, lối sống, lý tưởng cách mạng. Bên cạnh đó, bản thân mỗi cán bộ, giảng viên phải là những người sử dụng mạng xã hội thông minh. Thường xuyên cập nhật, chia sẻ các thông tin từ nguồn thông tin chính thống, những thông tin mang tính tích cực. Mặt khác, cán bộ giảng viên bằng kiến thức, kỹ năng của bản thân có thể viết bài chia sẻ về cách sử dụng mạng xã hội an toàn, kỹ năng nhận diện, cảnh giác trước thông tin xấu, độc trên không gian mạng.

Thứ ba về phía sinh viên, bản thân mỗi sinh viên cần trang bị kỹ năng tự học, tự nghiên cứu để không ngừng cập nhật kiến thức, nâng cao “sức đề kháng” trước những thông tin xấu, độc trên không gian mạng. Luôn chủ động nâng cao kiến thức xã hội về mọi mặt, nhằm xây dựng cho bản thân nhận thức chính trị đúng đắn để xem xét, tiếp cận thông tin một cách khách quan, đầy đủ, chính xác; hình thành kỹ năng chọn lọc thông tin, tiếp cận nguồn thông tin chính thống, tránh tiếp cận thông tin phiến diện, một chiều. Nâng cao tinh thần cảnh giác, sẵn sàng tham gia đấu tranh với những nhận thức không đúng, ngộ nhận, mơ hồ trước các nguồn thông tin sai trái, thù địch, trái với quan điểm, đường lối của Đảng, chính sách và pháp luật của Nhà nước.

Sinh viên cần rèn luyện ý thức tự giác, phát huy tính kỷ luật của người đoàn viên, đảng viên công an nhân dân trong quá trình tiếp xúc thông tin. Chấp hành tốt các quy định về quyền thông tin, phạm vi thông tin theo quy định của Hiến pháp năm 2013, Luật tiếp cận thông tin năm 2016 và Luật an ninh mạng năm 2018. Đồng thời, tích cực tham gia vạch trần, cảnh báo đến người dùng mạng xã hội những biểu hiện xáo trộn thông tin, lưu truyền thông tin xấu, độc, thông tin thiếu chính xác.

Sinh viên cần rèn luyện cho bản thân năng lực tư duy biện chứng, tư duy phản biện khi tiếp xúc với các thông tin trên mạng xã hội. Một tư duy biện chứng với cách xem xét sự vật, hiện tượng một cách khách quan, đa chiều, lịch sử, cụ thể, phát triển, thống nhất giữa lý luận và thực tiễn,... sẽ giúp sinh viên nhìn thấu được bản chất ẩn giấu sau những hiện tượng bề ngoài, thấy được mục đích sâu xa ẩn đằng sau những câu chữ, hình ảnh, từ đó dễ dàng phát hiện ra những thông tin xấu, độc để có biện pháp nhận diện, cảnh giác.

Khi sử dụng mạng xã hội, sinh viên cần tỉnh táo không thực hiện việc phát tán, chia sẻ thông tin của đài, báo, trang mạng, bài viết, blog, video của những phần tử chống đối, phản động. Chẳng hạn như thông tin kích động biểu tình, xúi giục người dân thực hiện hành vi vi phạm pháp luật, đi ngược thuần phong mỹ tục của dân tộc Việt Nam... Bên cạnh đó, sinh viên cũng cần có kỹ năng công nghệ thông tin ở mức cơ bản để có thể chặn, lọc, xóa, “report” (báo xấu) các thông tin xấu, độc để không cho các thông tin đó lan tràn dễ dàng trên mạng xã hội. Khi nhận lời mời kết bạn với bất

kỳ tài khoản mạng xã hội nào cần xác định được danh tính của người dùng hoặc xác định đó là những trang, nhóm tin cậy trước khi chấp nhận tham gia. Cần phân nhóm bạn để xác định những nội dung người khác có thể xem được trên trang cá nhân của mình hoặc những nội dung thông tin người khác có thể chia sẻ với bản thân. Khi thấy những đường dẫn (link) hoặc thông tin chưa được kiểm chứng cần bình tĩnh xem xét, không nên like hoặc share hoặc “click” vào các đường link, có thể gây mất an toàn thông tin hoặc dẫn dụ đến những trang mạng chứa thông tin xấu, độc.

Mặt khác, sinh viên cũng cần thực hiện tốt trách nhiệm của một người công dân trong phát hiện, tố giác và sẵn sàng tham gia đấu tranh, ngăn chặn kẻ xấu kích động việc thực hiện hành vi vi phạm pháp luật, kịp thời thông báo cho cơ quan chức năng để xử lý. Tích cực chia sẻ thông tin chính thống để cùng tuyên truyền, vận động bạn bè, người thân, cộng đồng hiểu và nghiêm chỉnh chấp hành pháp luật, tin tưởng vào sự lãnh đạo của Đảng, Nhà nước, cấp ủy, chính quyền các cấp; không tham gia các hoạt động vi phạm pháp luật; thực hiện tốt Cương lĩnh, Điều lệ Đảng.

P.T.T

TÀI LIỆU THAM KHẢO

1. *Chương trình đào tạo trình độ đại học* ban hành kèm Quyết định số 1042/QĐ-T04-P3 ngày 31/7/2023 của Hiệu Trưởng Trường Đại học An ninh nhân dân.
2. *Văn kiện Đại hội đại biểu toàn quốc lần thứ XIII*, NXB Chính trị Quốc gia – Sự thật, 2021.
3. Phạm Anh Tuấn, (2022), “*Sự phát triển của mạng xã hội và khả năng ứng dụng các lợi thế, tiện ích của mạng xã hội trong công tác thông tin, tuyên truyền ở Việt Nam*”, Tạp chí cộng sản, https://www.tapchicongsan.org.vn/web/guest/dau-tranh-phan-bac-cac-luan-dieu-sai-trai-thu-dich/chi-tiet/-/asset_publisher/YqSB2JpnYto9/content/su-phat-trien-cua-mang-xa-hoi-va-kha-nang-ung-dung-cac-loi-the-tien-ich-cua-mang-xa-hoi-trong-cong-tac-thong-tin-tuyen-truyen-o-viet-nam.
4. <https://bocongan.gov.vn/tin-tuc-su-kien/nhan-dien-va-phong-chong-lua-dao-truc-tuyen/nhan-dien-va-phong-chong-lua-dao-truc-tuyen-s24-t35662.html>.
5. <https://thanhnien.vn/6-sai-pham-cua-tiktok-tai-vn-1852304070148137.htm>.

