

NGHIÊN CỨU NHỮNG YẾU TỐ TÁC ĐỘNG ĐẾN HÀNH VI CHIA SẺ THÔNG TIN TRÊN MẠNG XÃ HỘI

Nguyễn Việt Dũng, Vũ Việt Tiến
Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: Nghiên cứu sử dụng thuyết hoạch tính cá nhân (Privacy Calculus) và Lý thuyết hành vi có kế hoạch (TPB) kết hợp với Hệ thống mô hình xử lý thông tin kép HSM (Heuristic-Systematic Model) để xây dựng mô hình nghiên cứu dựa trên những lý thuyết này. Mô hình nghiên cứu tập trung vào nhận thức của người sử dụng mạng xã hội về rủi ro bảo mật dữ liệu để khai thác hành vi chia sẻ thông tin trên mạng xã hội (MXH) ảnh hưởng bởi yếu tố này trong bối cảnh MXH đang dần trở thành một phương tiện không thể thiếu trong đời sống hàng ngày của người dân Việt Nam. Nghiên cứu đã xây dựng mô hình nghiên cứu với mười hai giả thuyết. Kết quả kiểm định cho thấy nhận thức rủi ro bảo mật dữ liệu tác động ngược chiều với ý định chia sẻ thông tin và nhận thức lợi ích bảo mật dữ liệu tác động thuận chiều với ý định chia sẻ thông tin, từ đó ý định chia sẻ thông tin tác động thuận chiều với hành vi chia sẻ thông tin của người dùng MXH. Bên cạnh đó mối quan hệ giữa các nhân tố xử lý thông tin có hệ thống, kiến thức nền về bảo mật dữ liệu, tìm kiếm thông tin, thiếu hụt thông tin cũng đã được kiểm định. Cuối cùng nghiên cứu đưa ra một vài khuyến nghị.

Từ khóa: Hành vi chia sẻ thông tin, mạng xã hội, nhận thức rủi ro, xử lý thông tin.

I. GIỚI THIỆU

Tác giả liên hệ: Nguyễn Việt Dũng, Vũ Việt Tiến
Email: dungnv@ptit.edu.vn, tienvv@ptit.edu.vn
Đến tòa soạn: 31/10/2022, chỉnh sửa: 08/12/2022, chấp nhận đăng: 15/12/2022

Sự phát triển mạnh mẽ của Internet, cuộc bùng nổ của công nghệ 4.0, con người ngày càng có nhiều cơ hội để dễ dàng tiếp cận, trao đổi, chia sẻ thông tin thông qua các nền tảng lớn, các mạng xã hội như Facebook, Instagram, Wechat,... Theo thống kê của Global Web Index Facebook hiện dẫn đầu thế giới với 2,23 tỉ người dùng, có đến 65 triệu doanh nghiệp lập trang thông tin trên mạng này. Kế đến là YouTube với 1,9 tỉ người dùng, WhatsApp là 1,5 tỉ, Messenger (thuộc Facebook) là 1,3 tỉ.

Cũng giống các quốc gia khác, tác động của cuộc Cách mạng Công nghiệp 4.0 đến các quyền con người là khá rõ ràng cả về mặt xây dựng pháp luật về quyền con người lẫn việc bảo đảm thực thi quyền trong thực tiễn. Sự phát triển của internet và các nền tảng mạng xã hội đặt ra nhiều thách thức về mặt pháp lý đối với việc ghi nhận và bảo đảm quyền con người ở Việt Nam. Liên quan đến quyền riêng tư, một số vấn đề mới đòi hỏi cần được pháp điển hóa bằng quy định pháp luật liên quan đến quyền được bảo vệ dữ liệu cá nhân, quyền được lãng quên trên internet,... Mặc dù đã được quy định trong Hiến pháp năm 2013, hiện nay Việt Nam vẫn chưa thông qua được một luật riêng về quyền riêng tư để điều chỉnh các vấn đề pháp lý mới này. Theo báo cáo thị trường ứng dụng điện thoại di động tại Việt Nam do Công ty Appota công bố năm 2021, 76% người tiêu dùng Việt Nam hiểu việc bảo vệ dữ liệu và bảo mật an toàn dữ liệu cá nhân là vô cùng quan trọng, thế nhưng lại có đến 82% số người được hỏi sẵn sàng chia sẻ

thông tin cá nhân để được nhận quà tặng khuyến mãi. Rõ ràng công nghệ đã tạo ra cơ hội cho nhiều chủ thể, bao gồm các chính phủ và các công ty, dễ dàng thu thập dữ liệu và theo dõi, giám sát các cuộc đàm thoại, trao đổi, các giao dịch thương mại, các hoạt động và thói quen của mọi cá nhân. Sự riêng tư của cá nhân, thậm chí là quyền tự do của con người, sẽ có thể không còn nữa khi các chủ thể khác có thể quan sát tất cả các hoạt động của họ, dự báo các hành động tương lai của họ và từ đó định hướng, kiểm soát cuộc sống của họ. Điều này có thể làm trầm trọng hơn sự mất cân bằng quyền lực giữa cá nhân và các thiết chế, cả thiết chế công và tư, trong xã hội hiện đại. Ý định và hành vi của người dùng mạng xã hội về việc chia sẻ thông tin đang là chủ đề được quan tâm và nghiên cứu. Việc người dùng có nhận thức được hay không về bảo mật dữ liệu, quyền riêng tư đã và đang trở thành vấn đề quan trọng, mang tính cấp bách, không chỉ gây ảnh hưởng đến cá nhân người dùng mà còn có những tác động nhất định đến các doanh nghiệp.

Nhóm tác giả nhận thấy tại Việt Nam ít có các công trình nghiên cứu về các hành vi bảo mật dữ liệu trong chia sẻ thông tin đặc biệt là trong bối cảnh bùng nổ công nghệ số, dẫn đến nhiều rủi ro trong thu thập, quản lý và lưu trữ dữ liệu. Từ đó nhóm tác giả đã tham khảo và cân nhắc các nghiên cứu có liên quan và hai lý thuyết: Thuyết hoạch tính cá nhân (Privacy Calculus) và Lý thuyết hành vi có kế hoạch (TPB) kết hợp với Hệ thống mô hình xử lý thông tin kép HSM (Heuristic-Systematic Model) để xây dựng mô hình nghiên cứu dựa trên những lý thuyết này. Mô hình nghiên cứu tập trung vào nhận thức của người sử dụng mạng xã hội về rủi ro bảo mật dữ liệu để khai thác hành vi chia sẻ thông tin trên mạng xã hội ảnh hưởng bởi yếu tố này. Mô hình nghiên cứu được kiểm định và đưa ra ý nghĩa của nhận thức rủi ro bảo mật dữ liệu tới Hành vi sử dụng mạng xã hội của người dùng.

II. TỔNG QUAN NGHIÊN CỨU VÀ MÔ HÌNH

A. Nghiên cứu tổng quan

Theo các tài liệu, nghiên cứu thực nghiệm trong quá khứ, kết hợp cùng các quan điểm, tiền đề lý thuyết, nhóm tác giả nhận thấy có nhiều nhân tố tham gia và có ảnh hưởng trong quá trình nhận thức rủi ro tác động đến hành vi con người. Nhóm đã kết hợp các mô hình trong lĩnh vực tâm lý học hành vi, tham khảo các giả thuyết đã được chứng minh từ các công trình nghiên cứu đi trước, từ đó đề xuất các giả thuyết và xây dựng mô hình cho đề tài.

Nhiều lý thuyết đã được sử dụng để giải thích những lo ngại về quyền riêng tư và những rủi ro được nhận thức về quyền riêng tư. Tuy nhiên, lý thuyết hoạch tính cá nhân (Privacy Calculus - PC) đã trở thành mô hình chính để giải thích sự hình thành các ý định tiết lộ và chia sẻ thông tin [36]. Một khái niệm của nhận thức rủi ro là sự không chắc chắn mà người tiêu dùng phải đối mặt khi họ không thể thấy trước hậu quả của các quyết định mua hàng của họ [34]. Nói cách khác, nhận thức rủi ro là nhận thức, cảm nhận về sự không chắc chắn mà người tiêu dùng phải đối mặt khi họ không thể thấy trước hậu quả của các quyết định. Lý thuyết hoạch tính cá nhân giải thích việc tiết lộ thông tin là một sự cân bằng giữa lợi ích được nhận thức và rủi ro theo ngữ cảnh cụ thể [11]. Ngoài ra, việc hình thành các nhận thức rủi ro và ý định chia sẻ thông tin được xác định bởi các mối quan tâm chung về quyền riêng tư của một cá nhân đối với môi trường.

Mối quan hệ giữa nhận thức lợi ích và ý định chia sẻ thông tin có thể được giải thích bằng lý thuyết “Sức mạnh của những quan hệ yếu”. Lý thuyết cho rằng những dòng thông tin mới thường đến với một cá nhân từ những mối quan hệ yếu. Lý do chính là bởi những người thân xung quanh một cá nhân - những mối quan hệ mạnh (bạn bè, gia đình, đồng nghiệp,...) thường có cùng nền tảng và thường chia sẻ những

nguồn thông tin chung. Chính vì vậy, các cá nhân thường tìm đến và tham gia vào những cộng đồng trực tuyến để tìm những nguồn thông tin còn thiếu mà những mối quan hệ mạnh không cung cấp cho họ [13]. Năm 2014, báo cáo nghiên cứu của Jae Hong Park & cộng sự về “Điều tra về hành vi chia sẻ thông tin và tìm kiếm thông tin trong cộng đồng đầu tư trực tuyến” đã kết luận rằng nhận thức về sự hữu dụng có ảnh hưởng đáng kể tới ý định chia sẻ và ý định tìm kiếm thông tin.

Nghiên cứu của Kahlor (2010) đã viết rằng: “Sự thiếu hụt kiến thức nhận thức được đặt trong khái niệm là khoảng cách giữa kiến thức nhận thức và kiến thức cần thiết”, đã đưa ra giả thuyết và chứng minh được rằng: Kiến thức nền (perceived knowledge) có tác động đến sự thiếu hụt về thông tin (information insufficiency). [24]

H1: Kiến thức nền về bảo mật dữ liệu có tác động ngược chiều tới sự thiếu hụt thông tin về bảo mật dữ liệu trên mạng xã hội của người dùng.

Đánh giá các tài liệu về hành vi tìm kiếm thông tin cho thấy rằng việc tìm kiếm thông tin thường được chấp nhận là động và phi tuyến tính. Mọi người trải nghiệm quá trình tìm kiếm thông tin như một sự tác động lẫn nhau của những suy nghĩ, cảm xúc và hành động [27]. Tìm kiếm thông tin được phát hiện có liên quan đến nhiều hành vi giao tiếp giữa các cá nhân ngoài việc đặt câu hỏi và trả lời của ứng viên. Tìm kiếm là hoạt động của con người nhằm tìm kiếm và sử dụng thông tin. Hành vi tìm kiếm thông tin là một trường hợp giải quyết vấn đề đặc biệt, bao gồm nhận biết và diễn giải vấn đề thông tin, thiết lập kế hoạch tìm kiếm, thực hiện tìm kiếm, đánh giá kết quả và lặp lại quá trình nếu cần thiết.

H2: Kiến thức nền về bảo mật dữ liệu có tác động ngược chiều tới việc tìm kiếm thông tin về

bảo mật dữ liệu trên mạng xã hội của người dùng.

Thiếu hụt thông tin được khái niệm là khoảng cách giữa kiến thức được nắm giữ và kiến thức cần thiết. Phù hợp với công việc trước đây [17], nó được vận hành bằng cách đưa kiến thức rủi ro được nhận thức vào mô hình phương trình cấu trúc bên cạnh kiến thức rủi ro cần thiết. Không giống như tính toán điểm số chênh lệch, kỹ thuật này giải thích mối quan hệ giữa kiến thức được nắm giữ và cần thiết trong khi tính toán đóng góp của kiến thức cần thiết trong mô hình và tránh các vấn đề về độ tin cậy tiềm ẩn và các hiệu ứng trần.

H3: Sự thiếu hụt thông tin có tác động cùng chiều đến việc tìm kiếm thông tin về bảo mật dữ liệu của người dùng trên MXH.

Kiến thức nền, trong nghiên cứu này, đề cập đến sự ước tính của một cá nhân về lượng kiến thức hiện tại của họ về rủi ro. Griffin (2012) và Kahlor (2006) đề xuất rằng kiến thức hiện tại của các cá nhân về rủi ro cụ thể sẽ tăng khả năng thu thập kiến thức mới và bổ sung của họ. Nói cách khác, kiến thức hiện có hoặc hiện tại cung cấp cho các cá nhân “năng lực được đào tạo” để tiếp cận và xử lý thông tin bổ sung. Kiến thức nền là một yếu tố ảnh hưởng đến việc xử lý thông tin như giả thuyết trong mô hình xử lý thông tin kép. Các tài liệu trước đây đã chỉ ra rằng kiến thức nền ảnh hưởng tích cực đến xử lý thông tin có hệ thống [24] [37]. Trumbo và McComas đã chỉ rằng mọi người có động lực và có khả năng sử dụng các chiến lược có hệ thống để xử lý thông tin khi họ nắm giữ nhiều kiến thức hơn [37]. Bên cạnh đó xử lý thông tin có hệ thống được tác động tích cực bởi kiến thức sẵn có [42] cũng được ủng hộ sau khi kiểm định.

H4: Kiến thức nền về bảo mật dữ liệu có tác động cùng chiều đến việc xử lý thông tin có hệ thống về rủi ro bảo mật dữ liệu của người dùng trên MXH.

Mô hình xử lý thông tin kếp (Heuristic – Systematic Model of Information Processing - HSM) là một mô hình của Shelly Chaiken được công nhận rộng rãi, giải thích cách mọi người tiếp nhận và xử lý các thông điệp thuyết phục. Trong đó, các cá nhân có thể xử lý thông tin theo một trong hai cách: theo phương pháp heuristic hoặc có hệ thống. Heuristic (tạm dịch: suy nghiệm) là các kỹ thuật dựa trên kinh nghiệm để giải quyết vấn đề, học hỏi hay khám phá nhằm đưa ra một giải pháp mà không được đảm bảo là tối ưu. Quan điểm heuristic không nhấn mạnh đến việc đánh giá thông tin chi tiết và tập trung vào vai trò của các quy tắc đơn giản hoặc heuristics nhận thức trong việc trung gian thuyết. Các cá nhân có thể có nhiều khả năng sử dụng phương pháp xử lý theo kinh nghiệm khi một vấn đề ít quan trọng hơn đối với cá nhân họ (họ có “mức độ liên quan đến vấn đề” thấp) hoặc khi họ tin rằng phán đoán của họ sẽ không có tác động đáng kể đến bản thân họ (“mức độ phản hồi thấp”). Trong khi đó, xử lý có hệ thống bao gồm xử lý toàn diện và phân tích, nhận thức các thông tin liên quan đến phán đoán. Tuy nhiên, xử lý thông tin theo cảm tính có xu hướng thực hiện các phán đoán và hành vi tiếp theo kém ổn định hơn so với xử lý có hệ thống [37]. Chính vì vậy, nhóm tác giả đã sử dụng nhân tố xử lý thông tin có hệ thống để đưa vào mô hình và kiểm định giả thuyết. Nghiên cứu của Johnson (2005) chỉ ra rằng việc tìm kiếm thông tin đóng góp những ảnh hưởng tích cực đến quá trình xử lý có hệ thống và những ảnh hưởng tiêu cực đối với quá trình xử lý theo kinh nghiệm. Nghiên cứu cũng đã đưa ra kết luận: Sự tìm kiếm thông tin có tác động tích cực đến xử lý thông tin có hệ thống [42].

H5: Tìm kiếm thông tin có tác động cùng chiều đến việc xử lý thông tin có hệ thống về rủi ro bảo mật dữ liệu của người dùng trên MXH.

H6: Sự thiếu hụt thông tin về bảo mật dữ liệu có tác động cùng chiều đến việc xử lý thông tin

có hệ thống về rủi ro bảo mật dữ liệu của người dùng trên MXH.

Mô hình Tìm kiếm và Xử lý Thông tin Rủi ro (RISP), được phát triển bởi Griffin, Dunwoody và Neuwirth (1999) mô tả sự khác biệt này giữa các mức độ hiểu biết hiện tại và một trạng thái tiêu chí là "thông tin đầy đủ". sự thiếu hụt thông tin là một trong những động lực chính thúc đẩy việc tìm kiếm và xử lý thông tin rủi ro của một cá nhân. Nếu sự đầy đủ thông tin được định nghĩa là “mức độ tin cậy khác nhau nhưng thỏa mãn một cách chủ quan về thông tin mà một người nắm giữ về một chủ đề nhất định” [17] thì thiếu hụt thông tin đề cập đến cảm giác chủ quan của cá nhân về lượng thông tin bổ sung mà họ cần để đủ tin cậy.

Xử lý thông tin là một yếu tố quyết định khác của nhận thức rủi ro [37]. Các học giả trước đây đã mở rộng mô hình xử lý thông tin theo mô hình xử lý thông tin kếp (HSM) để khám phá ảnh hưởng của việc xử lý thông tin đối với rủi ro của cá nhân. Trumbo (2002) cho rằng xử lý thông tin là một tiền đề cho nhận thức của cá nhân về rủi ro. Một nghiên cứu đưa ra quá trình xử lý theo hệ thống ảnh hưởng tích cực đến nhận thức rủi ro, trong khi xử lý theo cảm tính ảnh hưởng tiêu cực đến nhận thức rủi ro [37]. Do đó, các nhà nghiên cứu đã tiến hành kiểm định giả thuyết: “Xử lý thông tin có hệ thống tác động tích cực đến nhận thức rủi ro” và kết quả đã được kiểm chứng.

H7: Xử lý thông tin có hệ thống có tác động cùng chiều đến nhận thức rủi ro về bảo mật dữ liệu của người dùng trên MXH.

H8: Xử lý thông tin có hệ thống có tác động cùng chiều đến nhận thức giá trị về bảo mật dữ liệu của người dùng trên MXH.

Lượng kiến thức nền mọi người có về một vấn đề nào đó là liên quan đến nhận thức của họ về những rủi ro có thể xảy ra xoay quanh vấn đề đấy. Ví dụ, Klerck và Sweeney (2007) xác nhận có tác động đáng kể của kiến thức nền trong

việc giảm đánh giá rủi ro của người tiêu dùng đối với thực phẩm biến đổi gen. Bên cạnh đó, kiến thức nền về rủi ro được các học giả nghiên cứu là yếu tố rất quan trọng quyết định tới nhận thức rủi ro: càng có nhiều kiến thức về rủi ro, nhận thức rủi ro của mỗi cá nhân sẽ càng cao. Theo Darker (2013) kiến thức nền về rủi ro ảnh hưởng đến nhận thức của mọi người về mức độ nghiêm trọng của rủi ro có thể xảy ra.

H9: Kiến thức nền về bảo mật dữ liệu có tác động cùng chiều đến nhận thức rủi ro về bảo mật dữ liệu của người dùng trên MXH

Lý thuyết về Hành vi có kế hoạch (TPB) đề xuất thông qua bài báo “Từ ý định đến hành động: Một Lý thuyết về Hành vi có kế hoạch” [1]. Lý thuyết này được phát triển từ Lý thuyết về hành động hợp lý (TRA), được Martin Fishbein cùng đề xuất với Icek Ajzen vào năm 1980. Lý thuyết về hành vi có kế hoạch cho rằng mọi người có ý định thực hiện một số hành vi nhất định thì họ sẽ thực hiện hành vi đó trong thực tế. Thuyết hành vi dự định (TPB) được phát triển từ lý thuyết hành vi hợp lý [1], lý thuyết này được tạo ra do sự hạn chế của lý thuyết trước về việc cho rằng hành vi của con người là hoàn toàn do kiểm soát lí trí. Nhân tố trung tâm trong lý thuyết hành vi có kế hoạch là ý định của cá nhân trong việc thực hiện một hành vi nhất định.

Ý định là hành vi thúc đẩy ý thức của con người thực hiện hành động [33]. Ajzen cho rằng ý định được coi là một chỉ số về mức độ mọi người sẵn sàng tiếp cận một hành vi nhất định và sự cố gắng thực hiện hành vi nhất định đó [1].

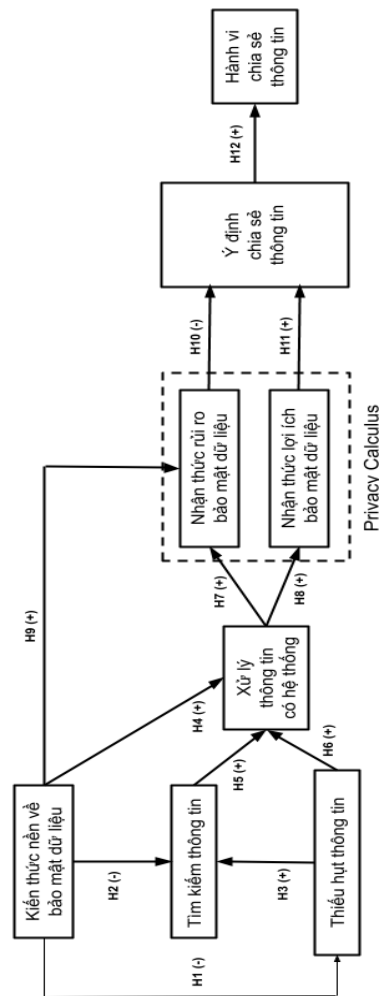
Ngoài ra, mô hình nghiên cứu của Jae Hong Park & cộng sự cũng đã khẳng định rằng ý định chia sẻ thông tin có ảnh hưởng tích cực tới hành vi chia sẻ thông tin trên các cộng đồng trực tuyến.

H10: Nhận thức rủi ro về bảo mật dữ liệu có tác động ngược chiều đến ý định chia sẻ thông tin của người dùng trên MXH.

H11: Nhận thức giá trị về bảo mật dữ liệu có tác động cùng chiều đến ý định chia sẻ thông tin của người dùng trên MXH.

H12: Ý định chia sẻ thông tin trên MXH có tác động cùng chiều đến hành vi chia sẻ thông tin của người dùng trên MXH.

B. Mô hình nghiên cứu



Hình 1: Mô hình nghiên cứu đề xuất

III. PHƯƠNG PHÁP NGHIÊN CỨU

Trong nghiên cứu này, nhóm tác giả chủ yếu dùng phương pháp nghiên cứu định lượng. Nghiên cứu định lượng nhằm kiểm định mô hình nghiên cứu đã đề xuất. Việc xây dựng các

thang đo dựa trên thang đo của các nghiên cứu trước, cụ thể nhóm nghiên cứu đã đưa ra 8 khái niệm được nghiên cứu, đó là:

(1) Kiến thức nền về bảo mật dữ liệu được kí hiệu là KNOW với các tiêu chí đo lường từ KNOW1 đến KNOW4 [41].

(2) Sự tìm kiếm thông tin được kí hiệu là SEEK với các tiêu chí đo lường từ SEEK1 đến SEEK4 [14].

(3) Sự thiếu hụt thông tin được kí hiệu là LACK với 2 tiêu chí đo lường là LACK1 VÀ LACK2 [42].

(4) Xử lý thông tin có hệ thống được kí hiệu là SP với các tiêu chí đo lường từ SP1 đến SP5 [29].

(5) Nhận thức lợi ích được kí hiệu là VALUE với các tiêu chí đo lường từ VALUE1 đến VALUE6 [21] [30] [38].

(6) Nhận thức rủi ro bảo mật dữ liệu được kí hiệu là RISK với các tiêu chí đo lường từ RISK1 đến RISK6 [28] [34].

(7) Ý định chia sẻ thông tin trên các trang mạng xã hội được kí hiệu là YDINH với các tiêu chí đo lường từ YDINH1 đến YDINH4 [10].

(8) Hành vi chia sẻ thông tin trên các trang mạng xã hội được kí hiệu là HV với các tiêu chí đo lường từ HV1 đến HV5 [4] [34].

Dữ liệu nghiên cứu được thu thập bằng phương pháp gửi bảng hỏi điều tra trên internet với thang đo Likert 5. Kích thước mẫu trong nghiên cứu $n = 419$ sau khi đã loại đi những bảng hỏi điều tra không hợp lệ. Các đối tượng được đều sinh sống tại một số tỉnh ở miền Bắc Việt Nam, với độ tuổi chủ yếu từ 18 đến 65 tuổi thường xuyên truy cập internet. Phiếu hỏi sau khi thu về được mã hóa và tiến hành phân tích trên phần mềm SPSS 22 và AMOS. Các kỹ thuật phân tích chính trong nghiên cứu gồm: Thống kê đặc điểm của mẫu nghiên cứu, đánh

giá độ tin cậy của thang đo, kiểm định giá trị của thang đo bằng phương pháp phân tích nhân tố khám phá – EFA, kiểm định thang đo bằng phương pháp phân tích nhân tố khẳng định – CFA, phân tích cấu trúc tuyến tính SEM để kiểm tra mức độ phù hợp của mô hình và các giả thuyết nghiên cứu.

IV. KẾT QUẢ NGHIÊN CỨU

A. Kết quả độ tin cậy của các thang đo

Kết quả kiểm định cho thấy các nhân tố này có hệ số Cronbach's Alpha đều lớn hơn 0,6. Các biến quan sát đều có hệ số tương quan biến tổng lớn hơn 0.3 và đều nhỏ hơn giá trị Cronbach's Alpha chung. Các nhân tố đều phù hợp với nghiên cứu. Cụ thể thang đo: Kiến thức nền về bảo mật dữ liệu = 0.826, tìm kiếm thông tin = 0.726, sự thiếu hụt thông tin = 0.8, xử lý thông tin có hệ thống = 0.783, nhận thức rủi ro bảo mật dữ liệu = 0.809, nhận thức giá trị bảo mật dữ liệu = 0.810, ý định chia sẻ thông tin trên MXH của người dùng = 0.901, hành vi chia sẻ thông tin trên MXH của người dùng = 0.831.

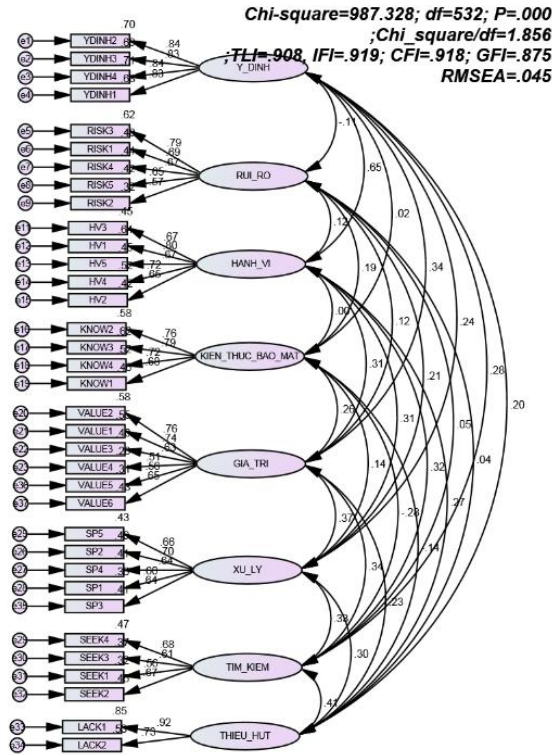
B. Phân tích nhân tố khám phá EFA

Sau khi phân tích kết quả EFA lần 1 thì loại biến quan sát RISK6 vì có hệ số tải $0.435 < 0.5$. Kết quả phân tích EFA lần 2, kiểm định Bartlett cho thấy giữa các biến trong tổng thể có mối tương quan với nhau (mức ý nghĩa $\text{sig} = 0.000 < 0.05$) với hệ số KMO = 0.840 ($0.5 < \text{KMO} < 1$), hệ số trích tại eigenvalue là 1.295 chứng tỏ phân tích EFA là thích hợp. Kết quả EFA cho thấy tổng phương sai trích là 62.302% tức là khả năng sử dụng yếu tố này để giải thích cho biến quan sát là 62.302% ($> 50\%$) ứng với tám nhân tố như bảng câu hỏi đề ra. Tuy nhiên hệ số tải của các biến quan sát đều lớn hơn 0.5 nên ta sẽ chuyển qua phân tích CFA.

C. Phân tích nhân tố khẳng định (CFA)

Kết quả CFA cho thấy mô hình này có độ phù hợp với dữ liệu thị trường: chi – square = 987.328, $\text{df} = 532$ với giá trị $p = .000$. Các chỉ

tiêu đo lường độ phù hợp khác nhau và chưa đạt tiêu chuẩn: TLI = 0.908, IFI = 0.919, CFI = 0.918, GFI = 0.875, CMIN/df = 1.856 và RMSEA = 0.045.

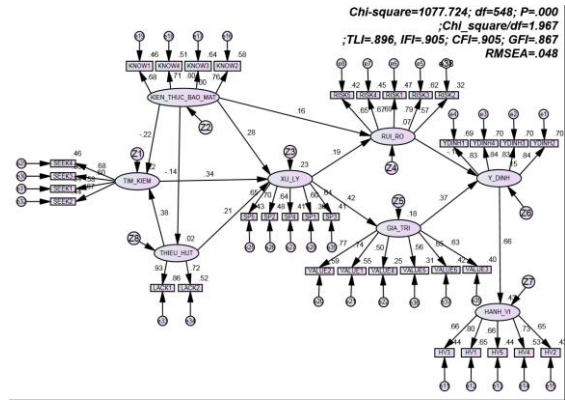


Hình 2: Kết quả CFA cho các thang đo

Dựa trên kết quả phân tích thì tất cả các nhóm nhân tố đều có trọng số chuẩn hóa lớn hơn 0.5 và các trọng số chưa chuẩn hóa đều có ý nghĩa thống kê do đó các khái niệm đều đạt giá trị hội tụ. Kết quả tính giá trị độ tin cậy tổng hợp và phương sai trích ta kết luận các khái niệm nghiên cứu đạt được giá trị phân biệt.

D. Kiểm định mô hình nghiên cứu SEM

Kết quả kiểm định SEM cho thấy mô hình này có Chi-square = 1077.724 và bậc tự do df = 548. Kiểm định Chi-square/df = 1.967 cho thấy mô hình này có độ phù hợp với dữ liệu thị trường. Các chỉ tiêu đo lường độ phù hợp khác cũng đạt rất cao (TLI = 0.896, IFI = 0.905, CFI = 0.905, GFI = 0.867, CMIN/df = 1.967 và RMSEA = 0.048).



Hình 3: Kiểm định mô hình SEM

Kết quả kiểm định cho thấy tất cả các giả thuyết đã được đề ra đều được chấp nhận và có ý nghĩa thống kê với giá trị P-value nhỏ hơn 5%. Có 3 sự tương quan ngược chiều có thể dễ dàng nhận ra đó là Kiến thức nền về bảo mật dữ liệu tới Tìm kiếm thông tin và Sự thiếu hụt thông tin (-0.144 và -0.225); Nhận thức rủi ro tới Ý định chia sẻ thông tin của người dùng trên MXH (-0.132). Với các mối quan hệ còn lại, Hành vi chia sẻ thông tin của người dùng trên MXH nhận sự tác động mạnh nhất từ Ý định chia sẻ thông tin (chỉ số hồi quy đạt 0.657). Và Nhận thức rủi ro về bảo mật dữ liệu nhận sự ảnh hưởng cùng chiều thấp nhất từ Kiến thức nền về vấn đề này

V. THẢO LUẬN KẾT QUẢ NGHIÊN CỨU VÀ KHUYẾN NGHỊ

Kiến thức nền về bảo mật dữ liệu có tác động ngược chiều tới sự thiếu hụt thông tin về bảo mật dữ liệu trên mạng xã hội của người dùng. Thông qua đánh giá thống kê mô tả, số người tham gia khảo sát ở các thế hệ khác nhau đánh giá về kiến thức nền của bản thân về bảo mật dữ liệu trên MXH là khá cao, dao động trong khoảng từ 3.9 - 4.1. Đặc biệt, phát biểu "Tôi biết và nhận thức được việc một số MXH theo dõi và ghi lại dữ liệu, lịch sử sử dụng của tôi." có giá trị trung bình lên tới 4.1002 là giá trị cao nhất ghi được trong bốn phát biểu được nghiên cứu đưa ra. Tức là, người dùng đang có nhận thức khá rõ trong các vấn đề xoay quanh kiến thức nền về bảo mật dữ liệu trên MXH. Cùng

với đó, 3.6205 là giá trị trung bình cao nhất thu được cho phát biểu "Tôi thấy nguy cơ bị đánh mất dữ liệu khi sử dụng mạng xã hội là rất cao." được cho là một con số trung bình cao. Trọng số hồi quy phản ánh mối quan hệ ngược chiều giữa hai yếu tố là -0.144 cho biết người dùng nếu có kiến thức nền càng nhiều, họ sẽ ít thiếu hụt thông tin về bảo mật dữ liệu hơn và ngược lại. Tuy nhiên, mức độ Kiến thức nền về bảo mật dữ liệu tác động tới Sự thiếu hụt thông tin có trọng số chỉ đạt 0.144 là khá thấp, cho thấy sự ảnh hưởng giữa hai yếu tố này không nhiều.

Kết quả nghiên cứu cũng đã chỉ ra rằng, Kiến thức nền về bảo mật dữ liệu có tác động ngược chiều tới sự tìm kiếm thông tin về bảo mật dữ liệu trên mạng xã hội của người dùng. Khi người dùng có càng nhiều kiến thức về một lĩnh vực, cụ thể trong nghiên cứu này là kiến thức nền về bảo mật dữ liệu, họ sẽ ít có xu hướng tìm kiếm thông tin về bảo mật dữ liệu hơn, và ngược lại. Trọng số -0.225 cho thấy yếu tố về kiến thức nền tuy có ảnh hưởng nhưng không quá nhiều tới ý định và hành vi tìm kiếm thông tin của người dùng MXH. Điều này được thể hiện thông qua giá trị trung bình của các giá trị SEEK1 SEEK2 SEEK3 SEEK4 đạt mức dao động từ 3.4678 - 3.9833 vẫn là khá cao so với giá trị trung bình của các biến KNOW1 tới KNOW4 là 3.95 - 4.1 như đã đề cập ở trên.

Kết luận khác được nghiên cứu chứng minh đó là Sự thiếu hụt thông tin có tác động cùng chiều đến sự tìm kiếm thông tin về bảo mật dữ liệu của người dùng trên MXH. Theo Eagly và Chaiken (1993), kiến thức nền là một yếu tố ảnh hưởng đến việc xử lý thông tin như giả thuyết trong hệ thống mô hình mẫu heuristic HSM. Càng thiếu hụt thông tin, người dùng càng có xu hướng tìm kiếm thông tin nhiều hơn để tra dồi và bù đắp phần còn chưa được hoàn thiện của mình. Trọng số 0.383 cho thấy các ảnh hưởng tích cực của sự tác động của hai yếu tố này, tức là, khi sự thiếu hụt đạt mức cao, các cá nhân sẽ bắt đầu tìm kiếm thông tin và sẽ có động lực lớn

hơn để tham gia vào quá trình xử lý thông tin có hệ thống hơn là xử lý theo kinh nghiệm - điều đã được chứng minh trong Mô hình Tìm kiếm và Xử lý thông tin rủi ro (RISP). Cuộc nghiên cứu với giả thuyết "Xử lý thông tin có hệ thống được tác động tích cực bởi kiến thức sẵn có" cũng nhận được sự ủng hộ sau khi kiểm định [42].

Tiếp theo, kết luận về Kiến thức nền về bảo mật dữ liệu có tác động cùng chiều đến việc xử lý thông tin có hệ thống về rủi ro bảo mật dữ liệu của người dùng trên MXH. Việc xử lý thông tin có hệ thống là có chủ ý và được tiến hành bằng cách phân tích, so sánh và phán đoán thông tin, trong khi xử lý thông tin theo cảm tính được dựa trên các quy tắc quyết định đơn giản để đưa ra phán quyết [23]. Những thông tin này thuộc về kiến thức nền về bảo mật dữ liệu, khi đã có khối lượng kiến thức nhất định, người dùng sẽ xử lý thông tin một cách có quy trình và hệ thống, bắt đầu từ việc đánh giá các thông tin và dữ liệu mình đã có sẵn. Trọng số 0.284 cho thấy kết quả của cuộc nghiên cứu đã chỉ ra rằng sự tác động không quá mạnh trong quá trình từ Kiến thức nền đi tới Việc xử lý thông tin có hệ thống của người dùng.

Nghiên cứu đã kết luận Tìm kiếm thông tin về bảo mật dữ liệu có tác động cùng chiều tới Xử lý thông tin có hệ thống. Dựa trên kết quả đánh giá thống kê mô tả về tìm kiếm thông tin mà nhóm thu thập được, giá trị trung bình đánh giá dao động từ 3.46 đến 3.98 với độ lệch chuẩn tương đối thấp. Điều này cho thấy rằng phần lớn người dùng MXH tham gia khảo sát đã có nhu cầu tìm kiếm thông tin về bảo mật dữ liệu. Đặc biệt với phát biểu "Tìm hiểu về bảo mật dữ liệu rất quan trọng đối với tôi", người tham gia khảo sát đánh giá với kết quả trung bình là 3.9, có nghĩa là phần lớn thái độ của họ đối với việc tìm hiểu về bảo mật dữ liệu ở mức trung lập tới mức rất quan trọng, cho thấy hành vi tìm kiếm thông tin về vấn đề này là khá quan trọng đối với người dùng MXH tham gia cuộc khảo sát. Ngoài ra, việc tìm kiếm thông tin đóng góp

những ảnh hưởng tích cực đến quá trình xử lý có hệ thống [23]. Một nghiên cứu khác sự tìm kiếm thông tin có tác động tích cực đến xử lý thông tin có hệ thống [42]. Từ kết luận của những nghiên cứu trước và từ kết quả của cuộc nghiên cứu này, nhóm đã đồng nhất sự tác động của tìm kiếm thông tin về bảo mật dữ liệu tới xử lý thông tin có hệ thống.

Kết luận tiếp theo là Sự thiếu hụt thông tin về bảo mật dữ liệu có ảnh hưởng tích cực tới Xử lý thông tin có hệ thống. Mô hình RISP đề xuất rằng sự thiếu hụt thông tin là một trong những động lực chính thúc đẩy việc tìm kiếm và xử lý thông tin rủi ro của một cá nhân. Các tiêu chuẩn chủ quan về thông tin không chỉ ảnh hưởng gián tiếp đến việc tìm kiếm và xử lý thông tin do thiếu hụt thông tin [17]. Dựa vào số liệu thống kê mô tả, nhóm nghiên cứu nhận thấy thang đo “Thiếu hụt thông tin” có giá trị trung bình điểm đánh giá từ 3.6 đến 3.7, điều này cho thấy phần lớn người dùng MXH tham gia vào cuộc khảo sát đã nhận thức được mức độ thông tin mình mong muốn nhận được và mức độ thông tin bản thân họ chưa nắm giữ về bảo mật dữ liệu, từ đó có thể xử lý thông tin một cách có hệ thống. Tuy nhiên, kết quả phân tích SEM cho ra trọng số tác động là 0.212 - ở mức không quá cao, cho thấy việc thiếu hụt thông tin về bảo mật dữ liệu có tác động tích cực tới xử lý thông tin có hệ thống, nhưng sự tác động này không quá mạnh mẽ. Song, cùng với những kết luận từ các cuộc nghiên cứu gần gũi với đề tài mà nhóm đã kể trên, chứng minh cho sự tác động này, nhóm đã đưa ra kết luận như trên.

Tiếp theo, nhóm nghiên cứu kết luận Xử lý thông tin có hệ thống tác động tích cực tới nhận thức rủi ro và nhận thức lợi ích về bảo mật dữ liệu. Với lý thuyết hoạch tính cá nhân đã được giải thích ở chương 2, nhóm tác giả sẽ đề cập lại mối liên hệ giữa nhận thức rủi ro và nhận thức lợi ích. Lý thuyết hoạch tính cá nhân giải thích việc tiết lộ thông tin là một sự cân bằng giữa lợi ích được nhận thức và rủi ro theo ngữ cảnh cụ

thể. Ngoài ra, việc hình thành các nhận thức rủi ro và ý định chia sẻ thông tin được xác định bởi các mối quan tâm chung về quyền riêng tư của một cá nhân đối với môi trường. Chính vì vậy, quá trình xử lý thông tin một cách hệ thống hoá đi kèm với cả việc xử lý thông tin về nhận thức rủi ro và nhận thức lợi ích. Trong kết quả khảo sát từ cuộc nghiên cứu của nhóm, trọng số tác động từ kết quả phân tích SEM đã chỉ ra sự tác động của xử lý thông tin có hệ thống tới nhận thức lợi ích là lớn hơn tới nhận thức rủi ro, với lần lượt các trọng số 0.423 và 0.189. Như vậy, người dùng MXH tham gia cuộc khảo sát khi cân nhắc đến lợi ích và rủi ro của việc chia sẻ thông tin, hay nói cách khác, sau khi tìm hiểu về bảo mật dữ liệu, họ nhận thấy lợi ích từ việc chia sẻ thông tin là nhiều hơn rủi ro họ sẽ gặp phải. Mặt khác, hai trọng số này không quá lớn để cho rằng sự tác động này ảnh hưởng đáng kể tới quá trình này, và cũng cần cân nhắc đến lý thuyết hoạch tính cá nhân mở rộng đã được giải thích: người dùng có thể ước tính lợi ích và rủi ro của việc chia sẻ thông tin với một số mức độ chính xác và sau đó đưa ra quyết định dựa trên mối quan hệ tuyến tính, hoặc sự cân bằng giữa 2 yếu tố đó.

Nghiên cứu đã chỉ ra được Kiến thức nền về bảo mật dữ liệu có tác động cùng chiều tới Nhận thức rủi ro bảo mật dữ liệu. Tuy nhiên kết quả kiểm định chỉ ra mức độ tác động khá thấp với trọng số chỉ 0.163. Điều này chỉ ra lượng kiến thức 1 tiếp thu được có tác động nhưng tác động không nhiều tới những rủi ro mà họ tự nhận thấy. Dựa trên kết quả đánh giá thống kê mô tả nhóm thu thập được, giá trị trung bình đánh giá Kiến thức nền về bảo mật dữ liệu khá cao, dao động từ 3.95 đến 4.10 với độ lệch chuẩn thấp, điều đó giúp nhóm đưa ra kết luận 419 người tại khu vực đô thị miền Bắc Việt Nam tham gia nghiên cứu có kiến thức tương đối vững về vấn đề bảo mật dữ liệu khi sử dụng MXH. Đây là thực trạng đáng mừng khi các cuộc cách mạng 4.0 đang diễn ra mạnh mẽ, vụ việc đánh cắp dữ

liệu người dùng thông qua các nền tảng MXH ngày càng gia tăng. Tuy nhiên cuộc nghiên cứu này của nhóm chỉ thực hiện tại khu vực đô thị miền Bắc Việt Nam, tức là tại những khu vực người dùng dễ dàng tiếp cận đến thông tin mới nhất, cập nhật nhất và hệ thống Internet hoàn thiện, tốc độ truy cập cao. Đặc biệt với phát biểu: “Tôi biết và nhận thức được việc một số MXH theo dõi và ghi lại dữ liệu, lịch sử sử dụng của tôi”, người tham gia đánh giá với kết quả trung bình là 4.1, có nghĩa là họ biết khá rõ về cách thức thu thập dữ liệu cá nhân của các nền tảng MXH. Chính những kiến thức này có tác động phần nào tới rủi ro nhận thấy về bảo mật dữ liệu trên MXH. Kiến thức nền về rủi ro là yếu tố rất quan trọng quyết định tới nhận thức rủi ro: càng có nhiều kiến thức về rủi ro, nhận thức rủi ro của mỗi cá nhân sẽ càng cao.

Tiếp đến Nhận thức giá trị và Nhận thức rủi ro bảo mật dữ liệu đều có tác động tới Ý định chia sẻ thông tin trên MXH. Trong khi Nhận thức giá trị có tác động cùng chiều tới Ý định thì Nhận thức rủi ro lại ảnh hưởng tiêu cực tới Ý định.

Nhận thức giá trị lại có ảnh hưởng tích cực tới Ý định chia sẻ thông tin trên MXH. Khi giá trị nhận được càng lớn, mọi người càng có động cơ thúc đẩy thay đổi ý định. Từ kết quả kiểm định giả thuyết, nhóm rút ra được kết luận mối quan hệ giữa 2 nhân tố này là mối quan hệ cùng chiều và mức độ tác động đạt mức tương đối 0.374. Thang đo “Nhận thức giá trị” thu được kết quả thống kê mô tả dao động ở mức 3 và 4, có nghĩa rằng các lợi ích của việc chia sẻ thông tin trên MXH được người dùng nhận thấy rõ. Đặc biệt với thang đo VALUE6, giá trị trung bình nhóm tác giả thống kê được là 3.90 - mức đánh giá cao, qua đó cho chúng ta thấy việc sử dụng MXH như 1 công cụ giải trí đã giúp cải thiện tinh thần của mọi người dù ở bất kì thế hệ nào và giúp họ thư giãn sau những giờ phút làm việc, học tập mệt mỏi.

Ngược lại, khi càng nhận thức được nhiều rủi ro mà MXH có thể gây ra, người dùng có xu hướng e ngại trong việc chia sẻ thông tin, dữ liệu cá nhân của mình trên đây. Dựa vào kết quả thống kê mô tả, nhóm nghiên cứu nhận thấy thang đo “Nhận thức rủi ro” có giá trị trung bình dao động từ 3.33 đến 3.39. Đặc biệt với thang đo RISK2, tương đương với phát biểu: “Tôi không chắc việc chia sẻ thông tin trên MXH có thật sự an toàn và tiện lợi” có giá trị trung bình điểm đánh giá là 3.66. Kết quả này cho thấy, đa phần người tham gia khảo sát có nhận thức về rủi ro bảo mật dữ liệu khi chia sẻ thông tin trên MXH. Mức độ ảnh hưởng của nhóm nhân tố này đã được thảo luận dưới đây:

Kết quả phân tích SEM cho thấy, với P-value = 0.015, trọng số hồi quy đạt -0.132, Nhận thức rủi ro tác động ngược chiều tới Ý định chia sẻ thông tin, dù mức tác động còn nhỏ nhưng kết quả giúp nhóm có thể rút ra kết luận cuối cùng về mối quan hệ giữa Nhận thức rủi ro và Ý định.

Trong cuộc nghiên cứu này, nhóm tác giả đưa ra phát biểu sau và yêu cầu người tham gia đánh giá: “Chia sẻ thông tin trên MXH mang lại nhiều rủi ro hơn là lợi ích nhận được”. Dữ liệu thu thập được có giá trị trung bình là 3.38, tương đương với mức trung lập trên thang đo Likert. Giữa giá trị lợi ích nhận được và những rủi ro gặp phải, người dùng MXH tại khu vực đô thị miền Bắc Việt Nam chưa thể đánh giá rõ cái nào hơn, cái nào kém. Lợi ích thì luôn đi kèm với rủi ro, và như thuyết Privacy Calculus đã chỉ ra, khi một người nhận thức được càng nhiều lợi ích của việc tiết lộ thông tin thì người đó cũng tự nhận thấy được càng nhiều rủi ro có thể gây ra từ việc này.

Cuối cùng, Ý định có tác động tới Hành vi chia sẻ thông tin trên MXH của người dùng. Kết quả phân tích SEM cho thấy Ý định là nhân tố có tác động cùng chiều và mạnh nhất tới Hành vi, đạt trọng số 0.657. Thực tế cho thấy ý định thường là một tiền đề trước hành vi. Mỗi cá

nhân thường có xu hướng hành động theo ý định của mình, do vậy đây được coi là nhân tố thiết yếu, ảnh hưởng mạnh đến hành vi chia sẻ thông tin trên MXH của người dùng. Để thay đổi thói quen chia sẻ thông tin, bảo vệ dữ liệu cá nhân 1 cách an toàn hơn trên MXH cần có những giải pháp nhằm thay đổi ý định của người dùng. Người tham gia khảo sát cho rằng họ cần cân nhắc thêm về việc chấp nhận rủi ro và tiếp tục chia sẻ thông tin (giá trị trung bình thu được đạt mức 3.1), điều này cho thấy không phải ai cũng dễ dàng chấp nhận rủi ro và họ có sự cân nhắc kỹ lưỡng để bảo vệ các dữ liệu cá nhân khỏi các trang MXH.

Từ kết quả và thảo luận nghiên cứu chúng tôi xin đưa ra một vài khuyến nghị.

Khuyến nghị với cơ quan quản lý nhà nước: Nâng cao năng lực quản lý nhà nước đảm bảo an ninh mạng, an toàn thông tin, bảo vệ quyền riêng tư của công dân, tổ chức, đảm bảo chủ quyền trên không gian mạng, xây dựng cơ chế để các doanh nghiệp có thể kiểm soát việc sử dụng thông tin theo đúng thỏa thuận cam kết. Cần xây dựng và đưa ra các chế tài xử phạt với các trường hợp mạng xã hội liên kết với một bên thứ ba để sử dụng trái phép thông tin người dùng; ngăn chặn truy nhập bất hợp pháp, các hình thức tấn công trên môi trường mạng. Tiếp tục cải thiện khung khổ pháp lý, đưa ra những chính sách, cải cách tạo điều kiện thuận lợi, ổn định cho doanh nghiệp tại Việt Nam. Các cơ quan quản lý, chính quyền cần có các giải pháp nhằm nâng cao nhận thức của người dùng về tầm quan trọng của bảo mật thông tin trên mạng xã hội, nâng cao năng lực hiểu biết và sử dụng các dịch vụ mạng xã hội, đảm bảo an toàn khi chia sẻ thông tin trên mạng xã hội.

Khuyến nghị với doanh nghiệp: Doanh nghiệp cần có trách nhiệm hơn với người dùng trong việc tăng cường bảo mật dữ liệu thông tin người dùng, minh bạch cam kết chính sách sử dụng thông tin và bảo mật thông tin người dùng.

Doanh nghiệp cần thực hiện tuyên truyền, giáo dục cho người dùng nâng cao nhận thức về bảo mật thông tin cá nhân, cách chia sẻ thông tin hữu hiệu trên các nền tảng MXH, tạo niềm tin với người dùng khi sử dụng.

Khuyến nghị với người dùng: Cần tích cực tìm kiếm, tìm hiểu về các vấn đề liên quan tới chia sẻ và bảo mật dữ liệu trên MXH, thông thái, cẩn thận lựa chọn nguồn thông tin trong thời đại Hậu sự thật (Post-truth era) với sự bùng nổ và nhiễu loạn thông tin. Cẩn thận rà soát cài đặt quyền riêng tư, chia sẻ, các ứng dụng kết nối cùng tài khoản, chia sẻ vị trí (location sharing). Hạn chế lượng thông tin và dữ liệu cá nhân được chia sẻ mỗi ngày trên MXH và điều chỉnh hành vi của bản thân theo đó, rà soát đối tượng được xem các nội dung, thông tin trên mạng xã hội của mình và các bên thứ ba được cấp quyền thu thập dữ liệu. Cuối cùng người sử dụng cũng cần tập giới hạn thời gian sử dụng MXH.

LỜI CẢM ƠN

Nhóm tác giả xin cảm ơn Học viện đã tạo điều kiện để thực hiện nghiên cứu khoa học và công bố kết quả. Cảm ơn đồng nghiệp tham gia hội thảo đóng góp ý kiến để hoàn thiện hơn nghiên cứu. Cảm ơn tạp chí Học viện đã hỗ trợ để bài viết được đăng công bố. Xin cảm ơn những người đã tham gia khảo sát.

TÀI LIỆU THAM KHẢO

- [1] Ajzen, I. (1991), The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, Vol. 50, Issue 2, pp. 179-211.
- [2] Alaszewski, A. (2005), Risk communication: Identifying the importance of social context, *Health Risk & Society* 7(2).
- [3] Atkin, C. K. (1973). Instrumental utilities and information seeking. In P. Clarke (Ed.), *New models for mass communication research* (pp. 205–242). Beverly Hills, CA: Sage Publications.

- [4] Bauer, R.A. (1960) Consumer Behavior as Risk Taking. In: Hancock, R.S., Ed., *Dynamic Marketing for a Changing World*, Proceedings of the 43rd.
- [5] Belkin, N.J. (1980). Anomalous states of knowledge as a basis for information retrieval. *Canadian Journal of Information Science*, 5(1), 133–143.
- [6] Bhatnagar, A. & Ghose, S. (2004) Segmenting Consumers Based on the Benefits and Risks of Internet Shopping. *Journal of Business Research*, 57.
- [7] Case, D. O. (2012). *Looking for information: a survey of research on information seeking, needs, and behaviour*. Bingley, UK: Emerald Group Publishing Limited.
- [8] Chaiken, S., Liberman, A., & Eagly, A. (1989). "Heuristic and systematic processing within and beyond the persuasion context". In J. S. Vealeman & J. A. Bargh (Eds.), *Unintended Thought*. New York: Guilford: 212–252.
- [9] Cole, C. (2012). *Information need: a theory connecting information search to knowledge formation*. Medford, NJ: Information Today.
- [10] Diallo, M. F. (2012), Effects of store image and store brand price-image on store brand purchase intention: Application to an emerging market, *Journal of Retailing and Consumer Services*, Vol. 19, Issue 3, pp. 360-367.
- [11] Dinev, T., & Hart, P. (2006), "An Extended Privacy Calculus Model for E-Commerce Transactions", *Information Systems Research*, 17(1), pp. 61-80.
- [12] Dowling, G.R. & Staelin, R. (1994) "A model of perceived risk and intended risk handling activity," *Journal of Consumer Research*, vol. 21, no.1, pp. 119-134.
- [13] Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168
- [14] Elizabeth W.Morrison và Jeffrey B.Vancouver (2000), *Journal of Management*2000, Vol. 26, No. 1, 119 –137
- [15] Feng, S., Shao, S., & Yuan, Y. T., et al. (2014). Investigation on personal health information services markets demand. *Information and Communications*, (05), 265-266.
- [16] Gemuenden, H.G. (1985), *Coping with inter-organizational conflicts : Efficient interaction strategies for buyer and seller organization*.
- [17] Griffin, R. J., Dunwoody, S., & Yang, Z. J. (2012). Linking risk messages to information seeking and processing. In C. T. Salmon (Ed.), *Communication Yearbook 36* (pp. 323-362). New York, NY: Taylor & Francis.
- [18] Hair, Jr. J. F, Anderson, R. E. Tatham, R. L. & Black, W. C. (1998), *Multivariate Data Analysis*, 5th ed, Upper Saddle River Prentice-Hall.
- [19] Hoskisson, R. E., et al (2016), *Managerial Risk Taking: A Multitheoretical Review and Future Research Agenda*, *Journal of Management*, [Vol 43, Issue 1](#).
- [20] Hovick, S.R., Kahlor, L.A., Liang, M.C. (2014), *Personal Cancer Knowledge and Information Seeking Through PRISM: The Planned Risk Information Seeking Model*, *Journal of Health Communication* 19(4).
- [21] Igarria, M., Schiffman, S. J., Wieckowski, T. J. (1994), The respective roles of perceived usefulness and perceived fun in the acceptance of microcomputer technology, *Behavior & Information Technology*, Vol. 13, Issue 6, pp. 349-361.
- [22] Ivan Ross (1975) ,"Perceived Risk and Consumer Behavior: a Critical Review", in *NA - Advances in Consumer Research Volume 02*.
- [23] Johnson, B. B. (2005). Testing and expanding a model of cognitive processing of risk information. *Risk Analysis*, 25, 631-650.
- [24] Kahlor, L. A. (2010), *PRISM: A planned risk information seeking model*, *Health Communication*, PubMed, 25(4), pp. 345-356.

- [25] Keith, M. J., Babb, J. S., & Lowry, P. B. (2014). A Longitudinal Study of Information Privacy on Mobile Devices. 2014 47th Hawaii International Conference on System Sciences.
- [26] Kim, J., Paek, H.J. (2009), Information processing of genetically modified food messages under different motives: An adaptation of the multiple-motive heuristic-systematic model. *Risk Anal.* 29, 1973-1806
- [27] Kuhlthau, C. C. (2005), Kuhlthau's information search process.
- [28] Lee, M. C. (2009), Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit, *Electronic Commerce Research and Applications*, Vol. 8, Issue 3, pp. 130-141.
- [29] LeeAnn Kahlor, Sharon Dunwoody, Robert J. Griffin và Kurt Neuwirth (2006), Seeking and Processing Information about Impersonal Risk, *Science Communication* Volume 28 Number 2 163-194
- [30] Moon, J. W., Kim, Y. G. (2001), Extending the TAM for a World-Wide-Web context, *Information & Management*, 38(4):217-230.
- [31] Moore, N. (2002), A model of social information need, *Journal of Information Science*, Vol. 28, Issue 4, pp. 297-303.
- [32] Park, Jae Hong, et al. "An investigation of information sharing and seeking behaviors in online investment communities." *Computers in Human Behavior* 31 (2014): 1-12.
- [33] Rezvani, et al (2012), A Conceptual Study on the Country of Origin Effect on Consumer Purchase Intention, *Asian Social Science* 8(12).
- [34] Schiffman, L., O'Cass, A., Paladino, A., D'Alessandro, S., Bednall, D. (2010), *Consumer behavior*, Pearson Education, 5th edition.
- [35] Sweeney và cộng sự, (1999) The role of perceived risk in the quality-value relationship: A study in a retail environment. *Journal of Retailing*, 75.
- [36] Thompson, S., Keith, M.J. & Posey, C. (2012), "Putting Privacy in Its Place: A Taxonomy of the Costs and Benefits of Location Data Disclosure through Mobile Devices", Dewald Roode Workshop on Information Privacy (IFIP WG8.11/11.13).
- [37] Trumbo, C. W., McComas, K.A. (2003), The function of credibility in information processing for risk perception. *Risk Anal.* 23, 343-353.
- [38] Vallerand, R. J. (1997), Toward A Hierarchical Model of Intrinsic and Extrinsic Motivation, *Advances in Experimental Social Psychology*, Vol. 29, pp. 271-360.
- [39] Wilson, T. D. (1999), Models of information behavior research, *Journal of Documentation*, Vol. 55, Issue 3.
- [40] Xu, H., Teo, H.H., Tan, B.C.Y., & Agarwal, R. (2010), "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services", *Journal of Management Information Systems*, 26(3), pp. 135-174.
- [41] Yang, Z. J., Rickard, L. N., Harrison, T. M., & Seo, M. (2014). Applying the risk information seeking and processing model to examine support for climate change mitigation policy. *Science Communication*, 36, 296-324.
- [42] Zhu, W., Wei, J., & Zhao, D. (2016). Anti-nuclear behavioral intentions: The role of perceived knowledge, information processing, and risk perception. Bradberry T (2007). *The Personality Code*. Putnam Adult Publisher.

RESEARCH FACTORS IMPACT ON BEHAVIOR OF INFORMATION SHARED ON SOCIAL NETWORKS

Abstract: The study uses the theory of Privacy Calculus and the theory of planned behavior (TPB) in combination with the Heuristic-Systematic Model (HSM) to build a research model. based on these theories. The research model focuses on the perception of social network users about data security risks to exploit the information sharing behavior on social networks (MXH) affected by this factor

in the context that social networks are evolving. gradually become an indispensable means in the daily life of Vietnamese people.. The study has built a research model with twelve hypotheses. Model testing is analyzed from data with 419 valid questionnaires, surveys on social network users of some northern provinces of Vietnam between the ages of 18 and 65. The test results show risk perception. Data security risks are negatively related to the intention to share information, and the perception of data security benefits is positively related to the intention to share information, from which the intention to share information is positively related to the intention to share information. information sharing behavior of MXH users. Besides, the relationship between the factors of systematic information processing, background knowledge of data security, information search, information shortage has also been tested as hypothesized. Finally, the study makes a few recommendations for users, social network enterprises and state management agencies on user data security.

Keywords: Information sharing behavior, social networks, risk perception, information processing.



Nguyễn Việt Dũng: NCS Trường đại học Kinh tế Quốc dân. Thạc sĩ từ năm 2014. Hiện công tác tại Học viện Công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu: Truyền thông Marketing, bán hàng doanh nghiệp, hành vi tiêu dùng.



Vũ Việt Tiến: Tốt nghiệp thạc sĩ từ năm 2018, tại đại học Picardie Jules Verne, Pháp. Hiện công tác tại Học viện công nghệ Bưu chính viễn thông. Lĩnh vực nghiên cứu: Marketing số, bán hàng online, hành vi khách hàng.