ẢNH HƯỞNG CỦA CẢM NHẬN VỀ RỦI RO BẢO MẬT VÀ QUYỀN RIÊNG TƯ ĐẾN NIỀM TIN VÀ HÀNH VI KIỂM SOÁT QUYỀN RIÊNG TƯ CỦA NGƯỜI DÙNG TRÊN MẠNG XÃ HỘI

Phạm Thị Huyền
Trường Đại học Kinh tế Quốc dân
Email: huyenpt@neu.edu.vn
Phan Thùy Anh
Trường Đại học Kinh tế Quốc dân
Email: phnthuyanh@gmail.com
Trịnh Phương Anh
Trường Đại học Kinh tế Quốc dân
Email: tpa170102@gmail.com
Mai Xuân Bách
Trường Đại học Kinh tế Quốc dân
Email: maixbach.workneu@gmail.com
Lê Quỳnh Chi
Trường Đại học Kinh tế Quốc dân
Email: chilequynh2002@gmail.com

Mã bài: JED-1166
Ngày nhận: 22/03/2023
Ngày nhận bản sửa: 11/06/2023
Ngày duyệt đăng: 19/06/2023
DOI 10.33301/JED.VI.1166

Tóm tắt:
Bài viết đo lường ảnh hưởng của cảm nhận về rủi ro bảo mật và quyền riêng tư đến niềm tin và hành vi kiểm soát quyền riêng tư của người dùng trẻ trên mạng xã hội. Kết quả phân tích dữ liệu khảo sát với 429 người dùng trong độ tuổi 18 – 24 bằng phần mềm SPSS và AMOS, cho thấy "Hành vi kiểm soát quyền riêng tư" chịu ảnh hưởng thuận chiều của "Cảm nhận về rủi ro bảo mật thông tin" và "Mối lo ngại về quyền riêng tư" nhưng lại chịu ảnh hưởng nghịch chiều bởi "Niềm tin". Từ đó, nhóm tác giả đề xuất một số giải pháp cho nhà cung cấp dịch vụ nền tảng mạng xã hội giảm thiểu mối lo ngại về quyền riêng tư và rủi ro bảo mật thông tin của người dùng, cải thiện niềm tin của họ với nền tảng để thu hút được nhiều người dùng hơn, tạo được môi trường an toàn, lành mạnh trên không gian mạng.
Từ khóa: Cảm nhận về rủi ro bảo mật, quyền riêng tư, niềm tin vào nền tảng mạng xã hội, kiểm soát quyền riêng tư, mạng xã hội.
Mã JEL: D83, L86

Impact of perceived information security risk and privacy concerns on trust and privacy protection behavior in social networking

Abstract:
This paper was conducted to measure the influence of perceived information security risk and privacy on the trust and the privacy protection behavior of young users in social networking sites (SNSs). The results of data analysis from a survey of 429 users between 18 – 24 years old, using SPSS and AMOS software, showed that privacy protection behavior is positively impacted by users' information privacy concerns and perceived security risks but negatively impacted by the trust. Based on those findings, the authors propose some solutions for SNSs service provider to reduce users' information privacy concerns and perceived information security risks; improve their trust in the platform to attract more users, create a safe and healthy environment in cyberspace.
Keywords: *Perceived information security risk, users' information privacy concerns, trust in social networking platforms, privacy protection behavior, online social networking.*
JEL Codes: D83, L86

1. Giới thiệu

Internet đã trở thành một phần không thể thiếu trong cuộc sống, góp phần thay đổi đời sống tinh thần của hầu hết người trẻ trong xã hội. Theo Internet Crime Report của FBI (2021), mạng internet với dữ liệu lớn, Internet vạn vật, điện toán đám mây, trí tuệ nhân tạo… tác động mạnh mẽ và tức thời, tạo nên một "không gian mạng" mà người trẻ có xu hướng đắm mình trong đó. Nhưng không gian mạng cũng đang bị lợi dụng khai thác thông tin cá nhân, tiềm ẩn rủi ro bảo mật dữ liệu, quyền riêng tư và an ninh cuộc sống. Năm 2021, thiệt hại do vi phạm dữ liệu cá nhân tăng gần 40% so với năm 2020. Có thể thấy, vấn đề an toàn thông tin mạng cần được quan tâm hơn, đặc biệt là thông tin trên các trang mạng xã hội (MXH), nơi người dùng vô tình hay bị yêu cầu phải cung cấp thông tin khi muốn sử dụng các tính năng được thiết kế cho từng trang mạng.

Mối lo ngại về quyền riêng tư và hành vi bảo vệ thông tin cá nhân trên mạng xã hội đã được quan tâm nghiên cứu gần đây với hai lý thuyết được sử dụng phổ biến: Lý thuyết quản lý quyền riêng tư trong truyền thông (Communication Privacy Management Theory – CPM); và Lý thuyết động cơ bảo vệ (Protection Motivation Theory - PMT). Lý thuyết CPM của Petronio (1991) cho rằng một cá nhân/tổ chức có thể được trao quyền đồng sở hữu thông tin khi họ được phép biết thông tin cá nhân của người khác và họ có thể không chỉ có thể tiết lộ thông tin của mình mà còn có thể tiết lộ thông tin của người khác mà họ có. Điều đó làm dấy lên nhu cầu hiểu biết về quản lý quyền riêng tư. Quản lý quyền riêng tư là việc đưa ra các quy định về hành vi cung cấp hoặc nhận thông tin dựa trên nguyên tắc về quyền sở hữu, kiểm soát và làm nhiễu loạn thông tin cá nhân.

Lý thuyết PMT của Rogers (1983) là khung lý thuyết tìm hiểu phản ứng của người dùng đối với rủi ro tiềm ẩn thông qua các yếu tố kích hoạt (ví dụ như thông điệp về nỗi sợ hãi khuyến khích các cá nhân thực hiện biện pháp bảo vệ, tránh hành vi có thể gây hại cho bản thân hoặc người khác). Việc "Đánh giá rủi ro" (bao gồm đánh giá "Mức độ nghiêm trọng của rủi ro", "Khả năng xảy ra rủi ro", "Phần thưởng bên trong" và "Phần thưởng bên ngoài") và "Đánh giá giải quyết" (bao gồm việc xem xét "Hiệu quả của phản ứng", "Hiệu quả bản thân" và "Chi phí phản hồi") ảnh hưởng đến "Động cơ bảo vệ" của các cá nhân. PMT cho rằng người dùng sẽ tự bảo vệ mình trước các rủi ro khi họ nhận thức được sự nghiêm trọng của chúng. Lý thuyết PMT phù hợp với bối cảnh nghiên cứu về quyền riêng tư trong hành vi sử dụng mạng xã hội khi xem xét các yếu tố rủi ro thông tin thúc đẩy người dùng thực hiện hành vi bảo vệ thông tin cá nhân.

Nghiên cứu về hành vi bảo vệ thông tin cá nhân trên mạng xã hội đã từng được nghiên cứu dựa trên 1 trong 2 mô hình lý thuyết nêu trên. Dựa trên lý thuyết CPM, các biến số "Cảm nhận về rủi ro bảo mật thông tin", "Mối lo ngại về quyền riêng tư và "Niềm tin vào nền tảng mạng xã hội" xuất hiện trong nghiên cứu của Dhami & cộng sự (2013), Paramarta & cộng sự (2018), Almadhoun & cộng sự (2011), Baruh & cộng sự (2017), Nemec & cộng sự (2019). Còn Boerman & cộng sự (2018), Wottrich & cộng sự (2018) đã nghiên cứu về mối quan hệ giữa "Cảm nhận rủi ro bảo mật thông tin", "Mối lo ngại về quyền riêng tư" và "Hành vi bảo vệ quyền riêng tư" của người dùng dựa trên lý thuyết PMT. Liệu các biến số đã được đề cập tới trong lý thuyết CPM ảnh hưởng như thế nào tới "Hành vi bảo vệ quyền riêng tư" trong bối cảnh mạng xã hội ngày càng trở nên phổ biến? Chính câu hỏi đó đã thúc đẩy nhóm tác giả tích hợp hai mô hình vào thực hiện nghiên cứu này với mục tiêu đánh giá ảnh hưởng của cảm nhận về rủi ro bảo mật và quyền riêng tư đến niềm tin vào nền tảng mạng xã hội, từ đó tác động tới hành vi kiểm soát quyền riêng tư của người dùng trên mạng xã hội.

2. Tổng quan nghiên cứu

2.1. Mạng xã hội và niềm tin vào nền tảng mạng xã hội

Mạng xã hội là nền tảng trực tuyến cho phép những người dùng kết nối với nhau một cách dễ dàng và kịp thời nhất (Pallis & cộng sự, 2011) với những tính năng phổ biến như: trò chuyện, đăng tải trạng thái, hình ảnh, tìm kiếm thông tin… mạng xã hội còn là "môi trường làm việc" lý tưởng, cho phép người kinh doanh truyền thông một cách dễ dàng. Theo thống kê vào năm 2022, ở Việt Nam có 76,95 triệu người dùng mạng xã hội, tương đương 78,1% dân số (DataReportal, 2022; Statista, 2022), tăng 6,9% so với năm 2021 với thời gian sử dụng trung bình hàng ngày là 2 giờ 28 phút. Những mạng xã hội được sử dụng nhiều nhất là Facebook, Zalo, Facebook Messenger, Tiktok, Instagram. Với lượng người dùng và thời gian sử dụng lớn như vậy, mạng xã hội là nơi sản sinh và lưu trữ nguồn dữ liệu lớn về hồ sơ người dùng, hình ảnh, video, lịch sử trò chuyện, thông tin tìm kiếm… Đây là nguồn tài nguyên vô cùng quý giá giúp nhà phát triển nền tảng

mạng xã hội cải thiện trải nghiệm dịch vụ song họ cũng cần bảo mật dữ liệu, củng cố niềm tin của người dùng với nền tảng.

Niềm tin là mức độ tin tưởng vào những tư tưởng, hành vi, năng lực và sự chính trực của đối phương (Kügler & cộng sự, 2013). Niềm tin với mạng xã hội được định nghĩa là sự tin tưởng của người dùng vào khả năng bảo mật thông tin cá nhân của nền tảng mạng xã hội (Dhami & cộng sự, 2013). Mối lo ngại về quyền riêng tư và rủi ro bảo mật được chứng minh có tác động trực tiếp tới niềm tin của người dùng vào nền tảng (Paramarta & cộng sự, 2018; Kroll & Stieglitz, 2019; Krasnova & cộng sự, 2010). "Bảo mật" tập trung vào việc bảo vệ thông tin khỏi các yếu tố tấn công bên ngoài; "quyền riêng tư" nhấn mạnh việc sử dụng và quản lý thông tin (Bansal, 2017). Liệu niềm tin vào nền tảng có phải là một yếu tố quan trọng quyết định hành vi sử dụng của người dùng với mạng xã hội đó, trong đó bao gồm hành vi kiểm soát quyền riêng tư?

2.2. Hành vi kiểm soát quyền riêng tư

Theo Lanier & Saini (2008) và Van De Garde-Perik & cộng sự (2008), hành vi kiểm soát quyền riêng tư được định nghĩa là quá trình kiểm soát phạm vi thông tin được truy cập, chia sẻ với những người khác. Để kiểm soát quyền riêng tư trên mạng xã hội, người dùng cần kiểm soát hành vi của chính mình khi tham gia mạng xã hội. Theo Petronio (1991), quản lý quyền riêng tư là việc cung cấp hoặc nhận thông tin riêng tư dựa trên quyền sở hữu, kiểm soát và làm nhiễu loạn thông tin cá nhân.

2.3. Cảm nhận về rủi ro, nhận thức về tính năng bảo vệ quyền riêng tư và mối lo ngại về quyền riêng tư

Nhận thức về tính năng bảo vệ quyền riêng tư của nền tảng mạng xã hội

Nhận thức về tính năng bảo vệ quyền riêng tư của nền tảng mạng xã hội là yếu tố thường xuất hiện trong các nghiên cứu có liên quan đến hành vi sử dụng mạng xã hội. Theo Adhikari & Panda (2018), nhận thức về tính năng bảo vệ quyền riêng tư, là sự nhận biết về tính năng có thể kiểm soát được thông tin được chia sẻ trên mạng xã hội thông qua tính năng bảo mật và là yếu tố ảnh hưởng thuận chiều đến mối quan tâm của người dùng về quyền riêng tư.

Mối lo ngại về quyền riêng tư

Smith & cộng sự (1996) và Chung & cộng sự (2021) chung quan điểm khi cho rằng, mối lo ngại về quyền riêng tư thể hiện qua sự quan tâm của người dùng đối với hành vi thu thập và sử dụng thông tin cá nhân người dùng. Với mạng xã hội, mối lo ngại về quyền riêng tư được quan tâm hơn vì các nền tảng mạng xã hội thường có tính năng thu thập và lưu trữ thông tin của người dùng (Son & Kim, 2008; Young & Quan-Haase, 2013). Người dùng lo ngại rằng thông tin cá nhân của họ có thể bị sử dụng với mục đích xấu (Feng & Xie, 2014; Shin, 2010) hoặc cũng có thể, khả năng thông tin được thu thập và lưu trữ đó bị tiếp cận do mạng xã hội có cấu trúc thiết kế nền tảng thiếu tính chặt chẽ (Acquisti & Gross, 2006). Zhao & cộng sự (2012) đã xác nhận việc tuyên bố về quyền riêng tư, thu thập dữ liệu với sự đồng ý của người dùng, kiểm soát quyền riêng tư hoặc cung cấp thông tin dựa trên lợi ích của người dùng có thể giảm mối lo ngại về quyền riêng tư một cách hiệu quả.

Cảm nhận về rủi ro thông tin

Các nền tảng mạng xã hội phát triển kéo theo việc dữ liệu người dùng bị các nền tảng này thu thập và lưu trữ ngày một nhiều hơn, tạo nên các rủi ro bị đánh cắp danh tính, đe dọa an toàn thông tin cá nhân, vi phạm không gian riêng tư hoặc mất mát về tài chính (Millham, M. H., & Atkin, D., 2018). Rủi ro thông tin còn tạo nên xung đột lợi ích kinh tế giữa nền tảng mạng xã hội và người dùng. Hiện nay, với việc thu thập thông tin cá nhân, các nền tảng mạng xã hội có thể bán dữ liệu đó cho bên thứ ba và đây có thể là nguồn thu nhập chính của nền tảng đó (Kalev, 2018). Ngoài ra, nguy cơ dữ liệu thông tin về người dùng mà nền tảng thu thập có thể bị bên thứ ba truy cập nếu nền tảng không có khả năng kiểm soát dữ liệu. Theo Liu & cộng sự (2022), các đối tác của Facebook đã thu thập thông tin người dùng gồm tuổi, địa chỉ, nghề nghiệp và hình ảnh đăng tải trên nền tảng này và chia sẻ với các công ty quảng cáo mà hoàn toàn không có sự chấp thuận từ người dùng. Rủi ro này đặt ra một yêu cầu lớn về khả năng bảo mật thông tin và quyền riêng tư.

2.4. Ảnh hưởng của nhận thức về rủi ro và bảo vệ quyền riêng tư tới niềm tin và hành vi kiểm soát thông tin

Altman (1975) và nhiều nghiên cứu đã xác định rằng mối lo ngại về quyền riêng tư và bảo mật trực tuyến ảnh hưởng đáng kể đến niềm tin và cảm nhận về rủi ro (Kansal, 2014; Smith & cộng sự, 2011; Malhotra,

Kim, & Agarwal, 2004). Và nhận thức về rủi ro cũng tạo hành vi bảo vệ thông tin trên nền tảng trực tuyến (Son & Kim, 2008; Wang, Duong, & Chen, 2016). Malik & cộng sự (2016) đã chứng minh mối lo ngại về quyền riêng tư tác động tiêu cực đến hành vi của người dùng qua biến số "niềm tin vào nền tảng Facebook".

Trong lý thuyết quản lý quyền riêng tư trong truyền thông CPM, Petronio (2013) khẳng định rằng trước những mối lo ngại về sự nhiễu loạn quyền riêng tư, người dùng nhận thức được rằng họ có quyền kiểm soát thông tin cá nhân, thông qua việc sử dụng các chính sách bảo vệ quyền riêng tư. Các nghiên cứu của Schomakers & cộng sự (2019), Wang & cộng sự (2019), Dhami & cộng sự (2013) cũng xác nhận rằng mối lo ngại về quyền riêng tư là một trong những nhân tố ảnh hưởng trực tiếp tới niềm tin vào nền tảng và là nhân tố ảnh hưởng gián tiếp tới hành vi kiểm soát thông tin trên mạng xã hội. Adhikari & Panda (2018) xác định mối quan hệ thuận chiều giữa mối lo ngại về quyền riêng tư và hành vi kiểm soát thông tin. Gupta & Chennamaneni (2018) cũng chỉ ra những lo ngại của đối tượng trung niên khi tham gia các nền tảng trực tuyến có ảnh hưởng tích cực tới hành vi bảo vệ quyền riêng tư. Vì vậy, các giả thuyết H1 và H2 được xác lập:

H1: Mối lo ngại về quyền riêng tư có ảnh hưởng nghịch chiều tới Niềm tin vào nền tảng mạng xã hội.

H2: Mối lo ngại về quyền riêng tư có ảnh hưởng thuận chiều tới Hành vi kiểm soát quyền riêng tư.

Khi các nền tảng mạng xã hội liên tục phát triển tính năng bảo mật thông tin, giúp người dùng hạn chế lo ngại về rủi ro, nhận thức về tính năng bảo vệ quyền riêng tư được cho là tạo nên cảm giác an toàn khi chia sẻ thông tin trên mạng xã hội, do đó ảnh hưởng tích cực tới các hành vi sử dụng mạng xã hội (Kim và Kim, 2020). Theo Dhami & cộng sự (2013), nhận thức về tính năng bảo mật do Facebook cung cấp là một trong những yếu tố ảnh hưởng đến niềm tin vào nền tảng. Do đó, giả thuyết H3 được xác lập:

H3: Nhận thức về tính năng bảo vệ quyền riêng tư có ảnh hưởng thuận chiều tới Niềm tin vào nền tảng mạng xã hội.

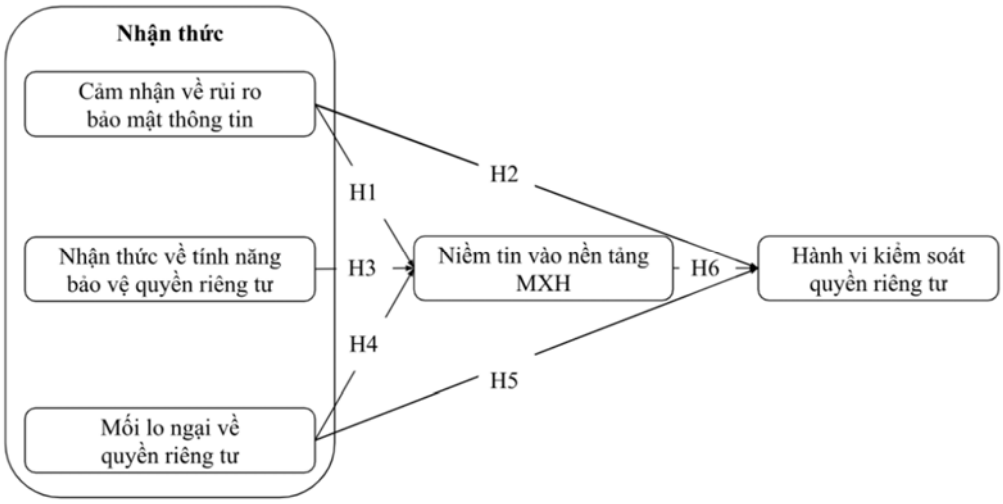
Theo lý thuyết động cơ bảo vệ PMT, người dùng sẽ tự bảo vệ mình trước các mối đe dọa khi họ nhận thức được sự nghiêm trọng của chúng. Khi cảm nhận được rủi ro bảo mật thông tin, người dùng sẽ thực hiện các hành vi kiểm soát quyền riêng tư nhằm mục đích bảo vệ thông tin cá nhân. Dinev & Hart (2006) và Mayer & cộng sự (1995) đã chứng minh rằng cảm nhận rủi ro bảo mật thông tin làm giảm niềm tin vào nền tảng mạng xã hội. Milne & cộng sự (2009) cũng lập luận rằng người dùng sử dụng mạng xã hội, khi cảm nhận được mối nguy hiểm về bảo mật, họ sẽ cố gắng bảo vệ thông tin của họ. Zhou & Liu (2023) cũng khẳng định lập luận tương tự khi nghiên cứu tại Trung Quốc, nhận thức rủi ro bảo mật của người dùng có ảnh hưởng tích cực tới các hành vi bảo vệ quyền riêng tư trực tuyến. Vì vậy, các giả thuyết H4 và H5 được xác lập:

H4: Cảm nhận về rủi ro bảo mật thông tin có ảnh hưởng nghịch chiều tới Niềm tin vào nền tảng mạng xã hội.

H5: Cảm nhận về rủi ro bảo mật thông tin có ảnh hưởng thuận chiều tới Hành vi kiểm soát quyền riêng tư.

Presthus & Vatne (2019) cho biết, niềm tin vào nền tảng có tác động nghịch chiều tới việc sử dụng các

Hình 1: Mô hình nghiên cứu đề xuất



cài đặt bảo vệ quyền riêng tư. Nghiên cứu của Sundaram & Shetty (2022) cũng khẳng định hành vi bảo vệ quyền riêng tư sẽ tăng lên nếu người dùng không đặt niềm tin vào các nền tảng trực tuyến. Theo CISCO (2020), 90% khách hàng nếu không tin tưởng vào nền tảng trực tuyến sẽ dừng các hành vi mua bán để bảo vệ dữ liệu cá nhân của họ. Giả thuyết H6 được xác lập:

H6: Niềm tin vào nền tảng mạng xã hội có ảnh hưởng nghịch chiều tới Hành vi kiểm soát quyền riêng tư

Tổng hợp các giả thuyết trên được thể hiện qua Hình 1.

3. Phương pháp nghiên cứu

Quy trình nghiên cứu được thực hiện lần lượt với nghiên cứu tại bàn, phỏng vấn sâu và khảo sát định lượng. Tổng quan nghiên cứu được thực hiện nhằm xác lập cơ sở lý thuyết và khoảng trống nghiên cứu, xây dựng giả thuyết và mô hình nghiên cứu. Cùng với đó là việc lựa chọn các thang đo làm cơ sở cho phỏng vấn sâu nhằm hoàn thiện cách thức diễn đạt các mệnh đề đo lường biến số. Mỗi biến số trong mô hình được đo lường qua 5 mệnh đề được thiết kế nhằm tìm hiểu mức độ đồng ý của người trả lời qua thang đo Likert, trong đó từ 1 (hoàn toàn không đồng ý) đến 5 (hoàn toàn đồng ý).

Khảo sát định lượng thông qua bảng hỏi được thực hiện với khách thể là giới trẻ trong độ tuổi sinh viên, từ 18 – 24 tuổi - đối tượng công dân dễ thích nghi nhất trong kỷ nguyên số, cởi mở, sẵn sàng đón nhận mọi sự thay đổi trong cuộc cách mạng công nghiệp 4.0. Nhóm nghiên cứu xác định lấy đối tượng nghiên cứu là giới trẻ trong độ tuổi 18 – 24 bởi theo Brent (2023) và Data Reportal (2023), nhóm người dùng nằm trong độ tuổi 18 – 24 tuổi chiếm tỷ lệ lớn nhất ở các nền tảng mạng xã hội phổ biến như Instgram (30,8%), Tiktok (21%) và chiếm tỷ lệ lớn ở các nền tảng như Facebook (22,6%), Youtube (15%)… Các kênh truyền thông mạng xã hội đã trở thành một "hiện tượng do giới trẻ điều khiển" (youth-driven phenomenon) (Spies Shapiro & Margolin, 2014). Nhóm khách thể trong độ tuổi 18-24 là ''đối tượng người dùng chủ yếu của các nền tảng mạng xã hội. Ở độ tuổi này, họ có đủ kiến thức và sự nhanh nhạy để nắm bắt các thông tin về quyền riêng tư và bảo mật thông tin" (NapoleonCat, 2021); "người trẻ chấp nhận các nền tảng truyền thông mạng xã hội nhanh hơn người trưởng thành, và là những người dùng tích cực nhất" (Yang & cộng sự, 2021).

Phiếu khảo sát được gửi đến nhóm đối tượng thông qua các nền tảng mạng xã hội, cụ thể là các trang, nhóm thông tin cộng đồng để đảm bảo được tính ngẫu nhiên, phù hợp với phương pháp lấy mẫu ngẫu nhiên đơn giản. Khảo sát đã nhận được 429 lượt trả lời có giá trị phân tích. Các phần mềm SPSS và AMOS được sử dụng nhằm khai thác dữ liệu.

4. Kết quả nghiên cứu

4.1. Kiểm định độ tin cậy của thang đo

Hệ số Cronbach's Alpha được sử dụng để đánh giá về độ tin cậy của thang đo lường. Toàn bộ các biến quan sát đều có hệ số tương quan biến lớn hơn 0,3 và hệ số Cronbach's Alpha lớn hơn 0.6 (Bảng 1). Theo Hair & cộng sự (1998), các thang đo đáng tin cậy và hệ tố tương quan cho thấy sự phù hợp của các thang đo cho các biến số.

Bảng 1: Kết quả kiểm định độ tin cậy thang đo lường

Nhân tố	Hệ số Cronbach Alpha	Hệ số tương quan biến tổng	Số thang đo bị loại
Mối lo ngại về quyền riêng tư (PRI)	0,931	0,825-0,877	0/3
Cảm nhận về rủi ro bảo mật thông tin (RISK)	0,906	0,739-0,819	0/4
Nhận thức về tính năng bảo vệ quyền riêng tư của nền tảng mạng xã hội (RE)	0,929	0,823-0,871	0/3
Niềm tin vào nền tảng mạng xã hội (TRUST)	0,837	0,652-0,761	0/3
Hành vi kiểm soát quyền riêng tư (PP)	0,947	0,886-0,894	0/3

Nguồn: Tổng hợp kết quả nghiên cứu từ SPSS (2023)

4.2. Phân tích nhân tố khám phá EFA

Phân tích EFA được thực hiện để xem xét các mối quan hệ giữa các biến trong cùng một nhóm với các chỉ số KMO > 0,5, kiểm định Bartlett có p-value < 0,05, các hệ số Factor Loading đều lớn hơn 0,5 – biểu

thị mối tương quan giữa biến quan sát và nhân tố (Factor Loading tại mức 0,5 có ý nghĩa thống kê tốt) và tổng phương sai trích lớn hơn 50% cho thấy mô hình EFA phù hợp (Hair & cộng sự, 2010). Các biến quan sát được sử dụng có tương quan với nhau trong cùng một nhân tố (Bảng 2).

Bảng 2: Kết quả đánh giá sơ bộ thang đo

Thang đo	Hệ số tải nhân tố	KMO	p-value	TVE (%)
RISK1	0,901	0,862	0,000	83,869
RISK2	0,897			
RISK3	0,872			
PRI1	0,853			
PRI2	0,842			
PRI3	0,870			
PRI4	0,829			
RE1	0,899			
RE2	0,892			
RE3	0,897			
TRUST1	0,791			
TRUST2	0,840			
TRUST3	0,854			
PP1	0,874			
PP2	0,915			
PP3	0,910			

Nguồn: Tổng hợp kết quả nghiên cứu từ SPSS (2023)

Để đánh giá tính hội tụ và tính phân biệt của thang đo, nhóm sử dụng độ tin cậy tổng hợp Composite Reliability (CR>0,7) và phương sai trung bình được trích Average Variance Extracted (AVE>0,5). Bảng 3 cho thấy các chỉ số đảm báo giá trị hội tụ và giá trị phân biệt.

Bảng 3: Kiểm định hiệu lực thang đo mô hình (Model Validity Measures)

	CR	AVE	MSV	MaxR (H)	RISK	PRI	PP	RE	TRUST
PRI	0,907	0,710	0,178	0,914	**0,843**				
RISK	0,932	0,820	0,190	0,938	0,417***	**0,906**			
PP	0,947	0,857	0,226	0,947	0,365***	0,360***	**0,925**		
RE	0,929	0,814	0,194	0,935	-0,341***	-0,441***	-0,355***	**0,902**	
TRUST	0,842	0,642	0,226	0,866	-0,422***	-0,261***	-0,475***	0,309***	**0,801**

Nguồn: Tổng hợp kết quả nghiên cứu từ SPSS-AMOS (2023)
Ghi chú: CR (Composite Reliability): Độ tin cậy tổng hợp; AVE (Average Variance Extracted): Phương sai trung bình được trích; MSV (Maximum Shared Variance): Phương sai chia sẻ lớn nhất.

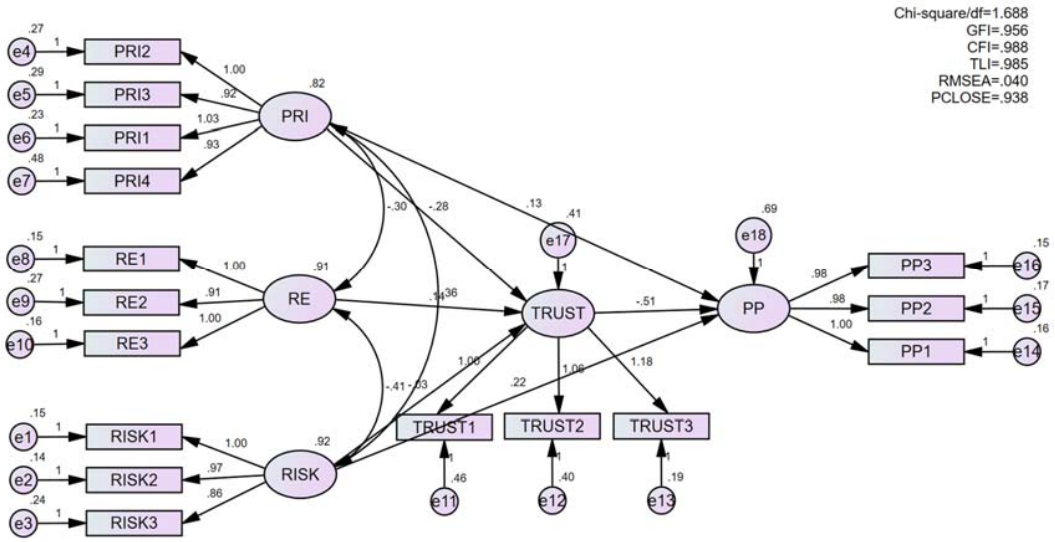
Điều đó chứng tỏ mô hình nghiên cứu đề xuất là phù hợp. Các thang đo đo lường cho các biến PRI, RISK, PP, RE, TRUST trong mô hình nghiên cứu có mối quan hệ mạnh với nhau và có khả năng giải thích tốt cho chính biến đại diện đó.

4.3. Phân tích mô hình cấu trúc tuyến tính (SEM)

Kỹ thuật SEM được thực hiện để kiểm tra mối quan hệ giữa "Hành vi kiểm soát quyền riêng tư" (PP) và "Niềm tin vào nền tảng mạng xã hội" (TRUST) với "Mối lo ngại về quyền riêng tư" (PRI), "Cảm nhận về rủi ro bảo mật thông tin" (RISK), "Nhận thức về tính năng bảo vệ quyền riêng tư của nền tảng mạng xã hội" (RE) với mức ý nghĩa là 5%. Kết quả SEM được thể hiện trong Hình 2.

Kết quả cho thấy Chi-square / df = 1,688 (<3), CFI = 0,988 (>0.95), GFI = 0,956, TLI = 0,985 đều lớn hơn 0,9, RMSEA = 0,040 (<0,06) theo Hu & Bentler (1999). Do đó, mô hình đạt các chỉ số phù hợp với dữ liệu nghiên cứu.

Hình 2: Kết quả SEM chưa chuẩn hóa



Nguồn: Tổng hợp kết quả của nhóm nghiên cứu từ SPSS-AMOS (2023)

Với độ tin cậy 95%, kết quả cho thấy, 5 giả thuyết (H2-3-4-5-6) được chấp nhận với chỉ số Sig < 0,05. Riêng H1 bị bác bỏ bởi giá trị p-value = 0,540. Hệ số hồi quy chưa chuẩn hóa ***β*** cho thấy mức độ tác động của các biến độc lập lên biến phụ thuộc.

Bảng 4: Tóm tắt kết quả kiểm định SEM

Giả thuyết (Hs)		Unstandardized Weights (***β***)	p-value (Sig)	Kết quả
H1	TRUST ← RISK	-0,027	0,540	Bác bỏ
H2	PP ← RISK	0,224	0,000	Chấp nhận
H3	TRUST ← RE	0,139	0,001	Chấp nhận
H4	TRUST ← PRI	-0,276	0,000	Chấp nhận
H5	PP ← PRI	0,131	0,029	Chấp nhận
H6	PP ← TRUST	-0,510	0,000	Chấp nhận

Nguồn: Tổng hợp kết quả của nhóm nghiên cứu từ SPSS-AMOS (2023)

5. Kết luận và khuyến nghị

5.1. Thảo luận

Nghiên cứu đã bổ sung những bằng chứng cho thấy ảnh hưởng của cảm nhận về rủi ro thông tin, lo ngại về quyền riêng và nhận thức về tính năng bảo mật tới sự tin cậy vào nền tảng mạng xã hội và hành vi kiểm soát thông tin. Phân tích SEM cho thấy có 5 giả thuyết đề xuất được chấp nhận. Nghiên cứu đã phát hiện ra tác động của niềm tin vào nền tảng mạng xã hội, mối lo ngại về quyền riêng tư và cảm nhận về rủi ro bảo mật thông tin đến hành vi kiểm soát quyền riêng tư.

Mối quan hệ thuận chiều giữa "Cảm nhận về rủi ro bảo mật thông tin" và "Mối lo ngại về quyền riêng tư" với "Hành vi kiểm soát thông tin" tương tự kết luận của Gupta & Chennamaneni (2018), Adhikari & Panda (2018), Zhou & Liu (2023), Milne & cộng sự (2009). Những cá nhân không chấp nhận cung cấp thông tin là những người có nhiều lo lắng về khả năng lạm dụng thông tin, hay không an tâm với việc bảo mật dữ liệu của nền tảng mạng xã hội. Mối quan hệ thuận chiều của "Nhận thức về các tính năng bảo vệ quyền riêng tư" và "Niềm tin vào nền tảng mạng xã hội" cũng chỉ ra rằng, niềm tin của người dùng với mạng xã hội tăng lên khi họ nhận thức được tính năng bảo mật của nền tảng, giống với nghiên cứu của Boerman & cộng sự (2018).

Mối quan hệ nghịch chiều giữa "Cảm nhận về rủi ro bảo mật thông tin" và "Niềm tin vào nền tảng mạng xã hội" chưa được khẳng định, khác với kết quả nghiên cứu của Dinev & Hart (2006), Mayer & cộng sự

(1995). Sự khác biệt này có thể là do những người dùng để tâm nhiều hơn đến các mối đe dọa đến từ những người dùng khác nhiều hơn so với mối đe dọa đến từ nền tảng (Malik & cộng sự, 2016); hoặc dù họ nhận thức được những rủi ro tiềm ẩn, họ vẫn chấp nhận tin tưởng để sử dụng nền tảng cho nhu cầu giao tiếp.

Mối quan hệ nghịch chiều giữa "Mối lo ngại về quyền riêng tư" với "Niềm tin vào nền tảng mạng xã hội" và giữa "Niềm tin vào nền tảng" với "Hành vi kiểm soát thông tin" thống nhất với các công trình nghiên cứu của Zhou (2020), Rodríguez-Priego (2023) và Presthus & Vatne (2019). Người dùng càng đặt niềm tin vào nền tảng mạng xã hội, họ càng giảm bớt sự đề phòng và hạn chế các hành vi kiểm soát thông tin (Olivero & Lunt, 2004; Sundaram & Shetty, 2022).

Bên cạnh đó, nghiên cứu cho thấy cảm nhận về các mối đe dọa hay bảo mật chưa chắc đã làm giảm sự tin cậy của người dùng vào nền tảng mạng xã hội. Phát hiện này mâu thuẫn với kết quả nghiên cứu của Dinev & Hart (2006) hay Mayer & cộng sự (1995). Sự khác biệt này có thể là do dù quan tâm đến bảo mật, nhưng người dùng để tâm đến các mối đe dọa đến từ bạn bè trên mạng xã hội nhiều hơn so với mối đe dọa đến từ nền tảng (Malik & cộng sự, 2016). Mặt khác, có thể nhu cầu sử dụng mạng xã hội để chia sẻ thông tin của giới trẻ ngày càng cao, nhưng chưa tìm được phương thức nào thay thế. Vì vậy, người dùng trẻ chấp nhận sử dụng nền tảng cho nhu cầu giao tiếp.

5.2. Đóng góp của kết quả nghiên cứu

Về mặt lý thuyết, (i) Nghiên cứu kết hợp hai lý thuyết: CPM và PMT để đo lường ảnh hưởng của các yếu tố: cảm nhận về rủi ro bảo mật thông tin, nhận thức về tính năng bảo vệ quyền riêng tư của nền tảng và mối lo ngại về quyền riêng tư tới hành vi kiểm soát quyền riêng tư trên mạng xã hội; (ii) Nghiên cứu đưa thêm yếu tố "Niềm tin vào nền tảng" vào mô hình và khẳng định vai trò trung gian của nó trong mối quan hệ giữa các biến độc lập với biến phụ thuộc là hành vi kiểm soát quyền riêng tư trên mạng xã hội. Từ đó, bổ sung và hoàn thiện hơn khung lý thuyết về mối quan hệ giữa cảm nhận về rủi ro bảo mật và mối lo ngại về quyền riêng tư, niềm tin vào nền tảng mạng xã hội, và hành vi kiểm soát quyền riêng tư.

Về mặt thực tiễn, có thể khẳng định, kết quả nghiên cứu giúp các nhà cung cấp nền tảng mạng xã hội hiểu rõ hơn tầm quan trọng của việc giảm thiểu mối lo ngại về quyền riêng tư và rủi ro bảo mật thông tin của người dùng, tạo được môi trường an toàn, lành mạnh trên không gian mạng, tăng niềm tin người dùng. Ngoài việc chia sẻ cách thức xử lý và thu thập dữ liệu người dùng, các nền tảng cần: (i) Cung cấp cho người dùng mục đích nền tảng sử dụng dữ liệu của họ nhằm đảm bảo sự rõ ràng và minh bạch của nền tảng, đồng thời giúp người dùng chủ động hơn trong việc sử dụng các cài đặt quyền riêng tư; (ii) Nâng cấp, phát triển các chế độ cài đặt quyền riêng tư và hệ thống quản lý dữ liệu người dùng; phát triển các tính năng bảo mật thông tin và xử lý các rủi ro của nền tảng trở nên thuận lợi hơn.

Việc đảm bảo minh bạch thông tin, cung cấp cho người dùng các khuyến nghị bảo mật thông tin và có chính sách rõ ràng về quyền riêng tư, đề cập quyền lợi của người dùng một cách rõ ràng không chỉ thể hiện sự chuyên nghiệp của nền tảng, giúp người dùng hiểu rõ được quyền và nghĩa vụ của họ sẽ giúp các nhà cung cấp phát triển nền tảng dễ dàng hơn, tránh được những rủi ro không mong muốn.

Tài liệu tham khảo

Acquisti, A., & Gross, R. (2006), 'Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook', *Lecture Notes in Computer Science*, 36–58, doi:10.1007/11957454_3

Adhikari, K., & Panda, R. K. (2018), 'Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks', *Journal of Global Marketing*, 31(2), 96–110, doi:10.1080/08911762.2017.1412552

Almadhoun, N. M., Dhanapal Durai Dominic, P., & Lai Fong Woon. (2011). 'Perceived security, privacy, and trust concerns within Social Networking Sites: The role of Information sharing and relationships development in the Malaysian Higher Education Institutions' marketing', *2011 IEEE International Conference on Control System, Computing and Engineering,* 426-431, doi:10.1109/iccsce.2011.6190564

Altman, I. (1975), *The environment and social behavior: privacy, personal space, territory, and crowding*, Monterey, California: Brooks/Cole.

Bansal, G. (2017), 'Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation', *Journal of Computer Information Systems*, 57, 330 - 343.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017), 'Online privacy concerns and privacy management: A meta-analytical review', *Journal of Communication*, 67, 26-53, doi:10.1111/jcom.12276

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018), 'Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data', *Communication Research*, 48(7), 953–977.

Brent, B. (2023), *Social media demographics to inform your brand's strategy in 2023. Sprout Social*, https://sproutsocial.com/insights/new-social-media-demographics.

Chung, K.C., Chen, C., Tsai, H., & Chuang, Y. (2021). 'Social media privacy management strategies: A SEM analysis of user privacy behaviors'. *Computer Communications*, 174, 122-130.

CISCO (2020), *Protecting Data Privacy to Maintain Digital Trust*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf

DataReportal (2022), *Digital 2022: Vietnam*, https://datareportal.com/reports/digital-2022-vietnam

DataReportal (2023), *Facebook users, stats, data & trends*, https://datareportal.com/essential-facebook-stats

Dhami, A., Agarwal, N., Chakraborty, T., Singh, B.P., & Minj, J. (2013), 'Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook', *2013 3rd IEEE International Advance Computing Conference (IACC)*, 465-469.

Dinev, T., Hart, P., (2006),. 'An Extended Privacy Calculus Model for E-Commerce Transactions', *Information Systems Research*, 17, 61–80.

Feng, Y., & Xie, W. (2014), 'Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors', *Computers in Human Behavior*, 33, 153–162.

Gupta, B., & Chennamaneni, A. (2018), 'Understanding Online Privacy Protection Behavior of the Older Adults: An Empirical Investigation', *J. Inf. Technol. Manag*, 29(3), 1-13.

Hair J.F., Tatham R.L., Anderson R.E. and Black W. (1998), *Multivariate Data Analysis*, 5th Edition, New Jersey: Prentice-Hall, Inc.

Hair, J.F., Black, W.C., Babin, B.J. & Anderson, R.E. (2010), *Multivariate Data Analysis,* 7th Edition, Pearson, New York.

Hu, L. T., & Bentler, P. M. (1999), 'Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives', *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1-55.

Kalev L. (2018), *What Does It Mean For Social Media Platforms To "Sell" Our Data? AI & Big Data*, https://www.forbes.com/sites/kalevleetaru/2018/12/15/what-does-it-mean-for-social-media-platforms-to-sell-our-data/?sh=2966cbfd2d6c

Kansal, P. (2014), 'Online privacy concerns and consumer reactions: Insights for future strategies', *Journal of Indian Business Research*, 6(3), 190-212.

Kim, B., & Kim, D. (2020), 'Understanding the key antecedents of users' disclosing behaviors on social networking sites: The privacy paradox', *Sustainability*, 12(12), 5163.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010), 'Online social networks: why we disclose', *Journal of Information Technology*, 25, 109-125.

Kroll, T., & Stieglitz, S. (2019), 'Digital nudging and privacy: improving decisions about self-disclosure in social networks', *Behaviour & Information Technology*, 40(1), 1-19.

Kügler, M., Smolnik, S., & Raeth, P. (2013), 'Determining the Factors Influencing Enterprise Social Software Usage: Development of a Measurement Instrument for Empirical Assessment', *2013 46th Hawaii International Conference on System Sciences*, 3635-3644.

Lanier, C. D., & Saini, A. (2008), 'Understanding consumer privacy: A review and future directions', *Academy of Marketing Science Review*, 12(2), 1–49.

Liu, Y., Tse, W.K., Kwok, P.Y., Chiu, Y.H (2022), 'Impact of Social Media Behaviour on Privacy Information Security Based on Analytic Hierarchy Process', *Information*, 13, 280.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004), 'Internet users' information privacy concerns (IUIPC): The construct,

the scale, and a causal model', *Information Systems Research*, 15(4), 336–355.

Malik, A., Hiekkanen, K., Dhir, A., & Nieminen, M. (2016), 'Impact of privacy, trust and user activity on intentions to share Facebook photos', *Journal of Information, Communication and Ethics in Society*, 14(4), 364–382.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995), 'An Integrative Model of Organizational Trust', *The Academy of Management Review*, 20(3), 709.

Millham, M. H., & Atkin, D. (2018), 'Managing the virtual boundaries: Online social networks, disclosure, and privacy behaviors', *New Media & Society*, 20(1), 50–67.

Milne G. R., Labrecque L. I., Cromer C. (2009), 'Toward an understanding of the online consumer's risky behavior and protection practices', *Journal of Consumer Affairs*, 43, 449-473.

Napoleon Cat (2021), *Facebook users in Viet Nam,* https://napoleoncat.com/stats/facebook-users-in-viet_nam/2021/03/

Nemec Zlatolas, Welzer, Hölbl, Heričko, & Kamišalić (2019), 'A Model of Perception of Privacy, Trust, and Self-Disclosure on Online Social Networks', *Entropy*, 21(8), 772, doi:10.3390/e21080772

Olivero, N., & Lunt, P. (2004), 'Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control', *Journal of Economic Psychology*, 25(2), 243–262.

Pallis, G., Zeinalipour-Yazti, D., & Dikaiakos, M. D. (2011), 'Online social networks: status and trends', *New directions in web data management,* 1, 213-234.

Paramarta, V., Jihad, M., Dharma, A., Hapsari, I.C., Sandhyaduhita, P.I., & Hidayanto, A.N. (2018), 'Impact of User Awareness, Trust, and Privacy Concerns on Sharing Personal Information on Social Media: Facebook, Twitter, and Instagram', *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, 271-276.

Petronio, S. (1991), 'Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples', *Communication Theory*, 1(4), 311–335.

Petronio, S. (2013), 'Brief status report on Communication Privacy Management theory', *Journal of Family Communication*, 13(1), 6–14.

Presthus, W., & Vatne, D. M. (2019), 'A Survey on Facebook users and information privacy', *Procedia Computer Science*, 164, 39-47.

Rodríguez-Priego, N., Porcu, L., Peña, M. B. P., & Almendros, E. C. (2023), 'Perceived customer care and privacy protection behavior: The mediating role of trust in self-disclosure', *Journal of Retailing and Consumer Services*, 72, 103284.

Rogers, R. W. (1983), 'Cognitive and Physiological processes in fear appeals and attitude change: A revised theory of Protection Motivation', *Social Psychophysiology*, 19(5), 153-176.

Schomakers, E. M., Lidynia, C., & Ziefle, M. (2019), 'A typology of online privacy personalities: Exploring and segmenting users' diverse privacy attitudes and behaviors', *Journal of Grid Computing*, 17, 727-747.

Shin, D. H. (2010), 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', *Interacting with Computers*, 22(5), 428–438.

Smith, H. J., Dinev, T., & Xu, H. (2011), 'Information privacy research: An interdisciplinary review', *MIS Quarterly*, 35(4), 989–1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996), 'Information privacy: Measuring individuals' concerns about organizational practices', *MIS Quarterly*, 20(2), 167–196.

Son, J. Y., & Kim, S. S. (2008), 'Internet users' information privacy-protective responses: A taxonomy and a nomological model', *MIS Quarterly*, 32(2), 503–529.

Spies Shapiro, L., & Margolin, G. (2014), 'Growing up wired: Social networking sites and adolescent psychosocial development', *Clinical Child and Family Psychology Review*, 17, 1–18, https:// doi. org/ 10. 1007/ s10567- 013-0135-1.

Statista (2022), *Average daily time spent on social media worldwide 2012-2022*, https://www.statista.com/statistics/433871/daily-social-media-usage-worldwide/

Sundaram, R., & Shetty, S. (2022), 'Privacy Concerns and Protection Behavior during the Covid-19 Pandemic', *Problems and Perspectives in Management*, 20, 57-70.

Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & Ijsselsteijn, W. (2008), 'Investigating privacy attitudes and behavior in relation to personalization', *Social Science Computer Review*, 26(1), 20–43.

Wang, L., Hu, H.-H., Yan, J., & Mei, M. Q. (2019), 'Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media', *Journal of Enterprise Information Management*, 33(2), 353–380.

Wang, T., Duong, T. D., & Chen, C. C. (2016), 'Intention to disclose personal information via mobile applications: A privacy calculus perspective', *International Journal of Information Management*, 36(4), 531–542.

Wottrich, V.M., Reijmersdal, E.A., & Smit, E.G. (2018), 'App Users Unwittingly in the Spotlight: A Model of Privacy Protection in Mobile Apps', *Journal of Consumer Affairs*, 53(3), 1056-1083.

Yang, C. C., Holden, S. M., & Ariati, J. (2021), 'Social media and psychological well-being among youth: the multidimensional model of social media use', *Clinical Child and Family Psychology Review*, 24(3), 631-650.

Young, A. L., & Quan-Haase, A. (2013), 'Privacy protection strategies on Facebook: The Internet privacy paradox revisited', *Information, Communication & Society*, 16(4), 479– 500.

Zhao, L., Lu, Y., & Gupta, S. (2012), 'Disclosure Intention of Location-Related Information in Location-Based Social Network Services', *International Journal of Electronic Commerce*, 16(4), 53–90.

Zhou, S.; Liu, Y. (2023), 'Effects of Perceived Privacy Risk and Disclosure Benefits on the Online Privacy Protection Behaviors among Chinese Teens', *Sustainability*, 15, 1657.

Zhou, T. (2020), 'The effect of information privacy concern on users' social shopping intention', *Online Information Review*, 44(5), 1119-1133.