

GIẢI PHÁP BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG CÁC GIAO DỊCH THƯƠNG MẠI ĐIỆN TỬ TẠI VIỆT NAM

● LƯƠNG THỊ KIM OANH

Khoa Kinh tế, Trường Đại học Hàng hải Việt Nam

DOI: <https://doi.org/10.62831/202508027>

TÓM TẮT:

Trong bối cảnh thương mại điện tử (TMĐT) phát triển mạnh mẽ tại Việt Nam, vấn đề bảo vệ dữ liệu cá nhân của người dùng trở thành một yêu cầu cấp thiết. Nghiên cứu này phân tích thực trạng bảo mật dữ liệu cá nhân trong các giao dịch TMĐT tại Việt Nam và đề xuất các giải pháp nâng cao hiệu quả bảo vệ dữ liệu nhằm đảm bảo quyền riêng tư và tăng cường niềm tin của người tiêu dùng.

Từ khóa: dữ liệu cá nhân, thương mại điện tử, bảo mật dữ liệu, quyền riêng tư, Việt Nam.

1. Đặt vấn đề

Sự phát triển của công nghệ số và TMĐT tại Việt Nam đã mở ra nhiều cơ hội cho cả doanh nghiệp và người tiêu dùng. Tuy nhiên, cùng với sự phát triển này là những rủi ro ngày càng gia tăng liên quan đến việc thu thập, lưu trữ và xử lý dữ liệu cá nhân. Nhiều vụ rò rỉ thông tin đã làm dấy lên lo ngại về tính an toàn và bảo mật thông tin cá nhân trong môi trường giao dịch trực tuyến. Việc rò rỉ thông tin cá nhân của người tham gia các hoạt động giao dịch điện tử gây phiền toái và rất nhiều người dùng đã trở thành nạn nhân của các vụ lừa đảo trên không gian mạng. Do đó, nghiên cứu này nhằm mục tiêu thống kê các hình thức lừa đảo phổ biến, phân tích nguyên nhân cốt lõi để từ đó tìm kiếm các giải pháp khả thi góp phần bảo vệ dữ liệu cá nhân và giúp nâng cao nhận thức, cảnh báo cho người tiêu dùng tham gia các hoạt động giao dịch TMĐT hiệu quả.

2. Cơ sở lý thuyết và giả thuyết nghiên cứu

2.1. Khái niệm dữ liệu cá nhân

Theo Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, dữ liệu cá nhân là thông tin dưới dạng kí 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 về một con người cụ thể. 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. Các Luật và Nghị định của Việt Nam hiện nay sử dụng khá nhiều thuật ngữ có nội hàm tương tự về khái niệm dữ liệu cá nhân như: thông tin cá nhân, bí mật cá nhân hay dữ liệu cá nhân. Nhìn chung, khái niệm dữ liệu cá nhân bao gồm thông tin định danh trực tiếp (họ tên, địa chỉ, số điện thoại,...) và thông tin định danh gián tiếp (lịch sử giao dịch, hành vi mua sắm...).

2.2. Cơ sở pháp lý

Các quy định pháp luật tại Việt Nam như: Luật An ninh mạng 2018, Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đã quy định rất rõ:

Luật An ninh mạng 2018: Đặt nền tảng pháp lý về việc bảo vệ thông tin trên không gian mạng, yêu cầu các tổ chức thu thập và xử lý dữ liệu phải có biện pháp bảo đảm an toàn thông tin, đồng thời đặt ra các điều kiện đối với việc lưu trữ dữ liệu người dùng trong nước.

Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân: Là văn bản pháp lý chuyên sâu đầu tiên tại Việt Nam về bảo vệ dữ liệu cá nhân quy định rõ về nguyên tắc thu thập, xử lý dữ liệu, quyền và nghĩa vụ của các tổ chức, cá nhân liên quan, cũng như các biện pháp bảo vệ dữ liệu như yêu cầu được sự đồng ý của người dùng, thông báo về mục đích xử lý dữ liệu và nghĩa vụ bảo mật.

Nghiên cứu hệ thống pháp luật của Việt Nam so với Quy định bảo vệ dữ liệu chung của Liên minh châu Âu (GDPR) cho thấy, quy định của Việt Nam có một số điểm tương đồng và khác biệt:

Điểm tương đồng: Cả hai đều yêu cầu sự đồng ý rõ ràng từ người dùng trước khi thu thập và xử lý dữ

chế, các quy định trong nghị định khá chặt chẽ và nghiêm khắc áp dụng cho tất cả các doanh nghiệp trong nước và có thể nói tạo áp lực khá lớn cho các doanh nghiệp khi thực hiện.

2.3. Các mô hình bảo vệ dữ liệu cá nhân

Hiện nay có một số mô hình bảo vệ dữ liệu cá nhân sau:

Nguyên tắc bảo mật theo thiết kế (Privacy by Design): Bảo mật được tích hợp ngay từ giai đoạn thiết kế hệ thống. Điều này bao gồm việc đảm bảo rằng chỉ những dữ liệu cần thiết mới được thu thập, dữ liệu được xử lý và lưu trữ an toàn ngay từ ban đầu.

Nguyên tắc bảo mật theo mặc định (Privacy by Default): Hệ thống phải được cấu hình sẵn để đảm bảo mức bảo vệ dữ liệu cao nhất cho người dùng. Mọi tính năng thu thập hoặc chia sẻ dữ liệu phải yêu cầu sự đồng ý rõ ràng của người dùng.

Mô hình quản lý dữ liệu tập trung: Tất cả dữ liệu được lưu trữ và quản lý từ một trung tâm duy nhất, giúp kiểm soát tốt hơn và tăng tính bảo mật.

Mô hình quản lý dữ liệu phân tán: Dữ liệu được lưu trữ trên nhiều hệ thống khác nhau nhằm giảm thiểu rủi ro khi một hệ thống bị xâm nhập.

Sơ đồ minh họa các nguyên tắc bảo vệ dữ liệu cá nhân:



liệu; quy định về quyền của người dùng như: quyền được biết, quyền truy cập, chỉnh sửa và xóa dữ liệu cá nhân.

Điểm khác biệt: GDPR có phạm vi điều chỉnh rộng hơn và áp dụng ngay cả với các tổ chức bên ngoài EU nếu xử lý dữ liệu của công dân EU. Tuy nhiên, cũng tạo điều kiện cho một số doanh nghiệp start up trong vòng 2 năm có thể chưa cần áp dụng luật này. Ngoài ra GDPR cũng quy định mức phạt cao hơn đối với các vi phạm. Pháp luật Việt Nam hiện tại chủ yếu tập trung vào việc bảo vệ dữ liệu trong lãnh thổ quốc gia và mức xử phạt còn hạn

Sơ đồ trên minh họa quy trình bảo vệ dữ liệu theo nguyên tắc bảo mật từ thiết kế và mặc định, đảm bảo thông tin cá nhân được bảo vệ toàn diện trong suốt vòng đời dữ liệu.

3. Phương pháp nghiên cứu

3.1. Nghiên cứu định tính (Bảng 1)

Bài viết sử dụng phương pháp phân tích định tính thông qua việc tổng hợp tài liệu thứ cấp, nghiên cứu luật pháp hiện hành và các mô hình bảo mật quốc tế. Ngoài ra, khảo sát trực tuyến với người tiêu dùng và doanh nghiệp TMDT cũng được thực hiện để đánh giá mức độ nhận thức và tình hình bảo mật thực tế.

Bảng 1. Các kỹ thuật bảo mật dữ liệu

Công nghệ	Mô tả	Ưu điểm	Hạn chế
Mã hóa dữ liệu	Chuyển đổi dữ liệu thành mã để ngăn chặn truy cập trái phép.	Bảo vệ tính bảo mật của dữ liệu; giảm nguy cơ bị rò rỉ.	Yêu cầu quản lý khóa mạnh; tốn tài nguyên xử lý.
Xác thực đa yếu tố (MFA)	Yêu cầu nhiều bước xác minh để truy cập hệ thống.	Tăng cường bảo mật tài khoản; giảm nguy cơ truy cập trái phép.	Có thể gây bất tiện cho người dùng; tăng thời gian đăng nhập.
Trí tuệ nhân tạo (AI)	Sử dụng học máy để phát hiện hành vi gian lận.	Xác định các mẫu phức tạp; phát hiện gian lận theo thời gian thực.	Cần lượng dữ liệu lớn để huấn luyện; có khả năng thiên lệch.

3.2. Thực trạng tình hình bảo mật dữ liệu cá nhân (Bảng 2)

Mặc dù Việt Nam đã ban hành nhiều quy định liên quan đến bảo vệ dữ liệu cá nhân, nhưng việc thực thi còn hạn chế, đặc biệt là ở các doanh nghiệp

nhỏ và vừa. Rất nhiều các vấn đề về rủi ro, lừa đảo, làm phiền tới người dùng khi tham gia thương mại điện tử và bị lộ dữ liệu cá nhân. Bảng sau tổng hợp các trường hợp bị lừa đảo khi dữ liệu cá nhân bị lộ và chỉ ra các nguyên nhân, đối tượng nạn nhân.

Bảng 2. Thống kê các hình thức lừa đảo trên không gian mạng (tác giả tổng hợp)

STT	Hình thức lừa đảo	Bản chất dữ liệu bị lộ	Tổ chức thực hiện	Đối tượng hướng tới	Độ tuổi
1	Giả mạo cơ quan chức năng (công an, Viện kiểm sát, tòa án,...) yêu cầu cung cấp thông tin cá nhân	Người nhẹ dạ cả tin, thiếu hiểu biết, có vấn đề cá nhân không muốn người khác biết	Nhóm tội phạm có tổ chức	Người dân	Mọi lứa tuổi
2	Giả mạo doanh nghiệp (ngân hàng, tổ chức tài chính, NCC dịch vụ, bệnh viện, bất động sản...) để lừa đảo	Người có vấn đề tài chính, bệnh tật	Tội phạm mạng chuyên nghiệp	Khách hàng ngân hàng, người vay vốn, người sử dụng dịch vụ	25-50 tuổi
3	Giả mạo tuyển dụng (cộng tác viên, mẫu nhí...) để thu phí hoặc lừa đảo thông tin	Người muốn kiếm thu nhập, thiếu hiểu biết	Tổ chức lừa đảo việc làm	Người tìm việc	22-35 tuổi
4	Giả mạo trang web thương mại điện tử để thu thập thông tin thẻ tín dụng	Người hiểu chưa rõ về công nghệ, kĩ thuật khi tham gia TMĐT	Tội phạm mạng chuyên nghiệp	Người mua sắm trực tuyến	25-45 tuổi
5	Giả mạo nhân viên hỗ trợ kỹ thuật để chiếm quyền truy cập máy tính	Người chưa có hiểu biết đầy đủ về CNTT	Tội phạm mạng có kỹ thuật cao	Người dùng máy tính	30-60 tuổi
6	Lừa đảo qua email giả mạo yêu cầu cập nhật thông tin tài khoản	Chưa có hiểu biết đầy đủ về TMĐT	Tội phạm mạng chuyên nghiệp	Người dùng email	25-50 tuổi
7	Giả mạo trang web từ thiện để kêu gọi quyên góp	Người có lòng tốt, thiếu hiểu biết, nhẹ dạ cả tin	Cá nhân hoặc nhóm nhỏ	Người hảo tâm	25-60 tuổi

STT	Hình thức lừa đảo	Bản chất dữ liệu bị lộ	Tổ chức thực hiện	Đối tượng hướng tới	Độ tuổi
8	Lừa đảo qua ứng dụng hẹn hò, tạo mối quan hệ để chiếm đoạt tài sản	Người thiếu tình cảm, nhận thức chưa đủ	Cá nhân hoặc nhóm nhỏ	Người độc thân	25-40 tuổi
9	Lừa đảo bán hàng đa cấp, tham gia sàn TMĐT hứa hẹn lợi nhuận cao	Người có vấn đề tài chính, muốn kiếm thêm thu nhập, thiếu hiểu biết	Tổ chức lừa đảo kinh doanh	Người tìm kiếm cơ hội kinh doanh	25-45 tuổi
10	Tung tin giả để tống tiền (vợ chồng ngoại tình,...)	Người có vấn đề về tình cảm, thiếu hiểu biết	Cá nhân hoặc nhóm nhỏ	Người dân	30-60 tuổi
11	Lừa đảo qua tin nhắn SMS chứa liên kết độc hại, rải link phishing, seeding quảng cáo	Người dùng chưa có đủ hiểu biết về CNTT, chưa biết cách phân biệt link độc hại, rảnh rỗi	Cá nhân hoặc nhóm nhỏ	Người dùng điện thoại di động	18-50 tuổi
12	Giả mạo người thân, bạn bè để vay mượn tiền qua mạng xã hội	Người hay sử dụng mạng xã hội	Cá nhân hoặc nhóm nhỏ	Người dùng mạng xã hội	18-35 tuổi
13	Lừa đảo trúng thưởng, quà tặng yêu cầu nộp phí để nhận, đăng nhập app để nhận quà, chuyển tiền nhầm vào TK	Người hay mua sắm trên sàn TMĐT	Cá nhân hoặc nhóm nhỏ	Người dùng điện thoại, email	25-50 tuổi
...					

4. Phân tích và kết luận

4.1. Phân tích

Qua bảng thống kê trên cho thấy, tình trạng rò rỉ dữ liệu cá nhân đang diễn ra ngày càng phổ biến, gây ra nhiều hậu quả nghiêm trọng đối với cá nhân và tổ chức. Nguyên nhân dẫn đến tình trạng này có thể từ cả phía cá nhân lẫn các tổ chức quản lý dữ liệu. Về phía cá nhân, việc sử dụng mật khẩu yếu, bị lừa đảo qua email giả mạo (phishing), chia sẻ thông tin công khai trên mạng xã hội, kết nối vào wi-fi công cộng không bảo mật hoặc tải ứng dụng chứa mã độc là những nguyên nhân phổ biến khiến dữ liệu cá nhân bị đánh cắp. Trong khi đó, các tổ chức, doanh nghiệp cũng có thể làm lộ dữ liệu do lỗ hổng bảo mật hệ thống, rò rỉ nội bộ, bị hacker tấn công hoặc do chính sách bảo vệ dữ liệu chưa chặt chẽ.

Dữ liệu cá nhân sau khi bị lộ thường được sử dụng vào nhiều mục đích khác nhau, trong đó có các hành vi vi phạm pháp luật như: lừa đảo tài chính, đánh cắp danh tính, chiếm đoạt tài khoản mạng xã hội, tống tiền hoặc quấy rối. Ngoài ra, dữ liệu cá nhân còn bị khai thác cho mục đích thương mại thông qua việc bán thông tin khách hàng cho bên thứ ba để chạy quảng cáo hoặc nghiên cứu hành vi tiêu dùng mà không có sự đồng ý của người dùng.

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, dữ liệu cá nhân trở thành mục tiêu quan trọng của tội phạm mạng. Khi thông tin cá nhân bị rò rỉ, người dùng có nguy cơ trở thành nạn nhân của các hành vi lừa đảo, chủ yếu do tác động của 3 yếu tố tâm lý: lòng tham, nỗi sợ và sự thiếu hiểu biết.

Để hạn chế nguy cơ rò rỉ dữ liệu cá nhân, mỗi

cá nhân cần nâng cao nhận thức về bảo mật thông tin, sử dụng mật khẩu mạnh, cảnh giác với các hình thức lừa đảo trực tuyến, hạn chế chia sẻ thông tin nhạy cảm trên môi trường số và sử dụng các công cụ bảo mật như xác thực hai lớp. Với các tổ chức, doanh nghiệp, cần có chính sách bảo vệ dữ liệu chặt chẽ, mã hóa thông tin quan trọng, kiểm tra và cập nhật hệ thống bảo mật định kỳ nhằm đảm bảo an toàn thông tin cho người dùng. Trong đó, đặc biệt chú trọng tới một số yếu tố sau:

Thứ nhất, lòng tham khiến người dùng dễ bị dụ dỗ bởi những lợi ích bất ngờ. Tội phạm mạng thường khai thác tâm lý này thông qua các chiêu trò như giả mạo tin nhắn trúng thưởng, hứa hẹn đầu tư sinh lời cao hoặc cung cấp khoản vay với lãi suất ưu đãi. Khi nhận được thông tin có chứa tên, số điện thoại, địa chỉ chính xác của mình, nhiều người tin tưởng và làm theo hướng dẫn mà không xác minh tính xác thực.

Thứ hai, nỗi sợ là một yếu tố quan trọng khiến người dùng mất khả năng phán đoán, dẫn đến hành vi cung cấp thông tin cá nhân hoặc chuyển tiền theo yêu cầu của kẻ gian. Các hình thức lừa đảo phổ biến bao gồm giả danh cơ quan công an, tòa án để đe dọa nạn nhân có liên quan đến vụ án hình sự, cảnh báo tài khoản ngân hàng có giao dịch bất thường hoặc đe dọa công khai thông tin nhạy cảm để tống tiền. Trong trạng thái hoang mang, nhiều người vội vàng thực hiện theo hướng dẫn mà không kịp kiểm chứng.

Thứ ba, sự thiếu hiểu biết về an toàn thông tin khiến người dùng dễ dàng mắc bẫy. Nhiều người chưa có kiến thức đầy đủ về các phương thức bảo mật, không nhận diện được trang web giả mạo, vô tình cung cấp thông tin đăng nhập cho kẻ xấu hoặc không kích hoạt các biện pháp bảo vệ tài khoản như xác thực hai lớp (2FA). Bên cạnh đó, việc chia sẻ thông tin cá nhân công khai trên mạng xã hội

cũng tạo điều kiện để kẻ gian khai thác và thực hiện các hành vi lừa đảo tinh vi hơn.

4.2. Kết luận

TMĐT phát triển kéo theo những rủi ro về lộ lọt dữ liệu cá nhân và lừa đảo trực tuyến. Để bảo vệ bản thân, người dùng cần trang bị kiến thức và áp dụng các biện pháp bảo mật sau:

Một là, xác minh độ tin cậy của nền tảng giao dịch: chỉ thực hiện giao dịch trên các trang web, sàn TMĐT uy tín, có chứng nhận bảo mật (HTTPS), tránh truy cập vào đường link lạ.

Hai là, không cung cấp thông tin cá nhân tùy tiện: hạn chế chia sẻ số CMND/CCCD, số tài khoản ngân hàng, mã OTP trên các nền tảng không chính thống.

Ba là, sử dụng phương thức thanh toán an toàn: ưu tiên các phương thức thanh toán có lớp bảo vệ bổ sung như ví điện tử, thẻ tín dụng có chức năng xác thực giao dịch.

Bốn là, bật xác thực hai lớp (2FA): kích hoạt 2FA trên các tài khoản mua sắm trực tuyến, tài khoản ngân hàng để tăng cường bảo mật.

Năm là, cảnh giác với các chiêu trò giảm giá, khuyến mãi bất thường: không mua hàng qua các đường link quảng cáo không rõ nguồn gốc, không tin vào các chương trình tặng quà giá trị cao bất thường.

Sáu là, thường xuyên cập nhật phần mềm và kiểm tra bảo mật thiết bị: sử dụng phần mềm diệt virus, cập nhật hệ điều hành và ứng dụng để tránh bị khai thác lỗ hổng bảo mật.

Như vậy, lòng tham, nỗi sợ và sự thiếu hiểu biết là những yếu tố quan trọng dẫn đến việc người dùng bị lừa đảo khi dữ liệu cá nhân bị rò rỉ. Để hạn chế rủi ro, mỗi cá nhân cần chủ động trang bị kiến thức về bảo mật thông tin, đặc biệt là trong các giao dịch TMĐT. Đồng thời, các cơ quan chức năng và doanh nghiệp cần đẩy mạnh công tác tuyên truyền, nâng cao nhận thức của người dân nhằm ngăn chặn những hành vi lừa đảo trên không gian mạng ■

Lời cảm ơn:

Nghiên cứu này được tài trợ bởi Trường Đại học Hàng hải Việt Nam trong đề tài mã số: DT24-25.108.

TÀI LIỆU THAM KHẢO:

Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam (2018), Luật An ninh mạng 2018.

Chính phủ nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023), Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân.

Phan Thảo Đan, Đoàn Đức Thắng. (2023). Bảo vệ dữ liệu cá nhân: “Quyền được lãng quên” theo quy định của Liên minh châu Âu và một số kiến nghị cho Việt Nam. Tạp chí Khoa học Kiểm sát, 6(68). Truy cập tại <https://khoaahockiemsat.hpu.vn/portal/article/view/278>

Cục An toàn thông tin (2023). Infographic: 24 hình thức lừa đảo phổ biến trên không gian mạng. Truy cập tại <https://antoanthongtin.gov.vn/giai-phap-khac/infographic-24-hinh-thuc-lua-dao-pho-bien-tren-khong-gian-mang-109512>

Binh ND (2021), Protecting personal data of social network users in the context of international integration. Sci.Tech.Dev. J.-Eco.Law Manag.; 5(3):1764-1771

European Union (2018), General Data Protection Regulation (GDPR).

Ngày nhận bài: 19/1/2024

Ngày phản biện đánh giá và sửa chữa: 3/2/2025

Ngày chấp nhận đăng bài: 20/2/2025

SOLUTIONS FOR PROTECTING PERSONAL DATA OF USERS IN E-COMMERCE TRANSACTIONS IN VIETNAM

● **LUONG THI KIM OANH**

Faculty of Economics,
Vietnam Maritime University

ABSTRACT:

Amid the rapid growth of e-commerce in Vietnam, protecting users' personal data has become an increasingly urgent priority. This study examines the current state of personal data security in Vietnamese e-commerce transactions, identifying key challenges and vulnerabilities in existing practices and legal frameworks. Based on the analysis, the study proposes targeted solutions to enhance the effectiveness of data protection, safeguard users' privacy rights, and strengthen consumer trust in digital commerce.

Keywords: personal data, e-commerce, data protection, privacy, Vietnam.