

PHÁP LUẬT VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG HOẠT ĐỘNG GIAO DỊCH THƯƠNG MẠI ĐIỆN TỬ

PHẠM MỸ DUNG*

Bài viết phân tích hệ thống pháp luật về bảo vệ dữ liệu cá nhân trong lĩnh vực thương mại điện tử tại Việt Nam dưới góc độ pháp luật về kinh tế, tập trung vào việc giải quyết xung đột lợi ích giữa quyền tự do kinh doanh của doanh nghiệp và quyền riêng tư của chủ thể dữ liệu. Thông qua phương pháp phân tích quy phạm và so sánh pháp luật, đánh giá tính tương thích của Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ với các luật chuyên ngành và chuẩn mực quốc tế. Kết quả nghiên cứu chỉ ra những lỗ hổng trong cơ chế thực thi, trách nhiệm pháp lý của các bên trung gian và sự thiếu hụt các chế tài kinh tế đủ sức răn đe. Từ đó, đề xuất giải pháp hoàn thiện hành lang pháp lý nhằm thúc đẩy thị trường thương mại điện tử phát triển bền vững và minh bạch.

Từ khóa: Bảo vệ dữ liệu cá nhân; thương mại điện tử; pháp luật về kinh tế; kinh tế số; Nghị định số 13/2023/NĐ-CP.

The article analyzes the legal framework for personal data protection in e-commerce in Vietnam from an economic law perspective, focusing on resolving the conflict between enterprises' freedom of business and data subjects' privacy rights. Through normative analysis and comparative legal methods, the study assesses the compatibility of Government Decree No. 13/2023/ND-CP dated April 17, 2023, with sectoral laws and international standards. The findings indicate gaps in enforcement mechanisms, the legal responsibilities of intermediary parties, and the lack of sufficiently deterrent economic sanctions. On that basis, the article proposes solutions to improve the legal framework in order to promote the sustainable and transparent development of the e-commerce market.

Keywords: Personal data protection; e-commerce; economic law; digital economy; Decree No. 13/2023/ND-CP.

NGÀY NHẬN: 24/02/2026 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 24/3/2026 NGÀY DUYỆT: 17/4/2026

DOI: <https://doi.org/10.59394/qlnn.363.2026.1481>

1. Đặt vấn đề

Việt Nam đang chứng kiến sự bùng nổ mạnh mẽ của kinh tế số, trong đó thương mại điện tử đóng vai trò là đầu tàu tăng trưởng. Dữ liệu cá nhân không còn thuần túy là thông tin riêng tư của cá nhân mà đã

chuyển hóa thành một loại “nguyên liệu số” đầu vào, có giá trị thương mại đặc biệt đối với các doanh nghiệp. Việc thu thập, phân tích và xử lý dữ liệu cá nhân giúp các nền tảng

* ThS, Trường Đại học Lao động - Xã hội

thương mại điện tử tối ưu hóa quy trình vận hành, cá nhân hóa trải nghiệm khách hàng và tạo ra các giá trị thặng dư kinh tế mới. Tuy nhiên, sự phụ thuộc ngày càng tăng vào dữ liệu cũng làm nảy sinh những rủi ro pháp lý phức tạp, đe dọa trực tiếp đến quyền lợi hợp pháp của người tiêu dùng và sự ổn định của thị trường.

2. Tổng quan nghiên cứu và khung pháp lý tham chiếu

Quyền bảo vệ đời sống riêng tư, bí mật cá nhân đã được *Hiến pháp* năm 2013 (sửa đổi, bổ sung năm 2025) ghi nhận như một quyền cơ bản của công dân. Điều 21 *Hiến pháp* quy định “Mọi người có quyền bất khả xâm phạm về đời sống riêng tư, bí mật cá nhân và bí mật gia đình...”; khẳng định mọi hành vi thu thập, lưu giữ, sử dụng thông tin cá nhân phải dựa trên sự đồng ý của chủ thể. Đây là tiền đề tối thượng buộc các doanh nghiệp thương mại điện tử phải tuân thủ nguyên tắc “sự đồng ý tự nguyện” khi tiếp cận dữ liệu khách hàng.

Điều 38 *Bộ luật Dân sự* năm 2015 quy định “Quyền về đời sống riêng tư, bí mật cá nhân, bí mật gia đình”. Đây là cơ sở pháp lý nền tảng để xác định trách nhiệm dân sự và bồi thường thiệt hại khi các đơn vị cung cấp dịch vụ vi phạm cam kết bảo mật. Những quy định này đóng vai trò trở thành “khung pháp lý chung”, giúp giải quyết các mâu thuẫn lợi ích giữa bên thu thập và người có dữ liệu trên môi trường online.

Trong lĩnh vực công nghệ thông tin, *Luật An toàn thông tin mạng* năm 2015 đầu tiên đặt ra các nguyên tắc và yêu cầu cụ thể về bảo vệ thông tin cá nhân trên môi trường mạng, đưa ra chuẩn mực đầu tiên về nghĩa vụ của tổ chức xử lý dữ liệu, buộc doanh nghiệp phải công bố biện pháp bảo vệ. *Luật An ninh mạng* năm 2018 với quy định mang tính bước ngoặt về việc yêu cầu lưu trữ dữ liệu tại Việt Nam, trong đó, Điều 26 yêu cầu các thực thể cung cấp dịch vụ xuyên biên

giới phải lưu trữ dữ liệu người dùng tại lãnh thổ Việt Nam. Cụ thể, các doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, Internet và dịch vụ giá trị gia tăng trên không gian mạng (ví dụ: mạng xã hội, sàn thương mại điện tử, dịch vụ email...) phải lưu trữ trên lãnh thổ Việt Nam các dữ liệu quan trọng của người dùng, bao gồm: dữ liệu thông tin cá nhân người sử dụng, dữ liệu người dùng tạo ra, như: tên tài khoản, địa chỉ IP, nội dung trao đổi, thông tin thẻ tín dụng... Đồng thời, doanh nghiệp nước ngoài thuộc đối tượng trên có thể bị yêu cầu đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam khi cung cấp dịch vụ cho người dùng Việt Nam. Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ đã hướng dẫn chi tiết thi hành *Luật An ninh mạng* năm 2018, quy định thời gian lưu trữ tối thiểu (24 tháng) và quy trình thực hiện yêu cầu lưu trữ dữ liệu trong trường hợp có yêu cầu từ Bộ Công an.

Việc hợp nhất *Luật An ninh mạng* năm 2018 và *Luật An toàn thông tin mạng* năm 2015 thành *Luật An ninh mạng* năm 2025 đã phục tình trạng phân tán thẩm quyền và chồng chéo trong áp dụng. *Luật* mới thể hiện xu hướng chuyển từ quản lý “tách rời” sang khuôn khổ tích hợp dựa trên an ninh dữ liệu và an ninh hệ thống thông tin, qua đó đặt các yêu cầu về lưu trữ, bảo mật và cung cấp dữ liệu người dùng trong một chuẩn tuân thủ thống nhất.

Theo Điều 5 Chương I *Luật An ninh mạng* năm 2025, nêu rõ các biện pháp bảo vệ an ninh mạng, bao gồm: thẩm định, đánh giá, kiểm tra, giám sát an ninh mạng và biện pháp lưu trữ, sao lưu bảo vệ an ninh thông tin đối với hệ thống thông tin. Quy định này thiết lập nghĩa vụ bảo đảm an ninh hệ thống thông tin chứa dữ liệu, qua đó, chi phối cách doanh nghiệp xử lý và lưu trữ dữ liệu cá nhân trong thương mại điện tử và buộc họ triển khai các biện pháp kỹ thuật, quản trị nhằm hạn chế rủi ro rò rỉ, mất an toàn dữ liệu.

Trong lĩnh vực thương mại và bảo vệ người tiêu dùng, pháp luật Việt Nam cũng sớm đề cập việc bảo vệ thông tin cá nhân trong các giao dịch điện tử. Chẳng hạn: *Luật Giao dịch điện tử* năm 2023 đã pháp điển hóa việc cấm các hành vi thu thập, kinh doanh trái phép thông điệp dữ liệu, tạo ra hành lang an toàn cho các giao dịch không giấy tờ; *Luật Bảo vệ quyền lợi người tiêu dùng* năm 2023 buộc các doanh nghiệp phải thiết kế lại kiến trúc hệ thống, minh bạch hóa mục đích xử lý thông tin ngay từ thời điểm xác lập giao dịch.

Việc ban hành Nghị định số 13/2023/NĐ-CP và đặc biệt là *Luật Bảo vệ dữ liệu cá nhân* năm 2025 (có hiệu lực từ ngày 01/01/2026) đã thực sự trở thành lời giải then chốt cho tình trạng thiếu hụt văn bản pháp lý thống nhất trong thời gian qua. Theo đó, khung pháp lý mới này đã đi sâu vào cơ chế quản trị dựa trên mức độ rủi ro thông qua việc chia tách dữ liệu cá nhân thành hai nhóm: “cơ bản” và “nhạy cảm”. Quy định này cho phép các tổ chức tài chính cũng như các sàn thương mại điện tử áp dụng các quy trình bảo mật nghiêm ngặt và đặc thù hơn, đặc biệt đối với những thông tin có độ rủi ro cao, như: dữ liệu thanh toán và lịch sử tín dụng khách hàng.

Ngoài ra, *Luật Bảo vệ dữ liệu cá nhân* năm 2025 còn khẳng định năng lực thực thi xuyên biên giới khi mở rộng đối tượng điều chỉnh đối với cả các tổ chức quốc tế có hoạt động xử lý dữ liệu của công dân Việt Nam. Sự thay đổi mang tính chiến lược này không chỉ bảo đảm sự công bằng trong hoạt động kinh doanh giữa doanh nghiệp nội và ngoại mà còn xác lập năng lực tài phán quốc gia trên không gian số toàn cầu, tạo nền tảng vững chắc cho sự phát triển an toàn của nền kinh tế số.

Việc hệ thống hóa các quy định nêu trên cho thấy, lộ trình lập pháp nhất quán, chuyển từ các chuẩn mực mang tính định hướng sang hệ thống chế tài mang tính bắt buộc và chuyên biệt hơn. Tuy nhiên, thực

tiễn thực vẫn tồn tại “điểm nghẽn” về năng lực giám sát kỹ thuật và thiếu cơ chế xử phạt dựa trên tỷ lệ doanh thu theo tiêu chuẩn quốc tế. Nhận diện các tầng nấc quy phạm này nhằm làm rõ “trục logic xuyên suốt” giữa nghĩa vụ của doanh nghiệp, quyền của cá nhân và vai trò điều tiết của Nhà nước. Đây là nền tảng để phân tích các thực trạng vi phạm và đề xuất giải pháp hài hòa hóa giữa mục tiêu tăng trưởng kinh tế số với yêu cầu bảo hộ quyền con người trong kỷ nguyên số.

3. Thực trạng bảo vệ dữ liệu cá nhân trong giao dịch thương mại điện tử tại Việt Nam hiện nay

Hoạt động bảo vệ dữ liệu cá nhân tại Việt Nam đang ở giai đoạn chuyển dịch từ cơ chế tự nguyện sang tuân thủ bắt buộc. Các sàn thương mại điện tử quy mô lớn đã bắt đầu nội hóa các tiêu chuẩn quốc tế thông qua việc cập nhật chính sách bảo mật và thiết lập bộ phận bảo vệ dữ liệu. Tuy nhiên, sự phân hóa năng lực tuân thủ giữa các nhóm doanh nghiệp vẫn diễn ra rõ nét. Dữ liệu thực chứng cho thấy, rủi ro lộ lọt thông tin đang trở thành vấn đề cấp bách khi chỉ riêng trong quý III/2026, thị trường ghi nhận khoảng 6,5 triệu tài khoản cá nhân bị xâm nhập, tương đương 8 - 10% tổng số tài khoản trực tuyến toàn quốc¹. Điều này phản ánh sự mất cân bằng giữa tốc độ khai thác dữ liệu để tối ưu hóa lợi nhuận và mức độ đầu tư cho hạ tầng an ninh dữ liệu. Đặc biệt, mô hình vận hành “mở quyền truy cập cho đối tác” nhưng thiếu cơ chế kiểm soát nhật ký và truy vết trách nhiệm đang tạo ra những lỗ hổng nghiêm trọng, khiến dữ liệu cá nhân bị chuyển giao trái phép vì lợi ích thương mại giữa các đơn vị tài chính, bảo hiểm và bất động sản. Cụ thể như:

(1) Sự thiếu đồng bộ trong hệ thống quy phạm pháp luật.

Hành lang pháp lý hiện nay vẫn tồn tại những xung đột về mặt kỹ thuật lập pháp. Việc sử dụng các thuật ngữ không nhất quán

giữa “bí mật đời tư”, “thông tin cá nhân” và “dữ liệu cá nhân” gây khó khăn cho các doanh nghiệp trong việc xác lập quy trình tuân thủ thống nhất. Trong giai đoạn chuyển tiếp, sự chồng chéo giữa các quy định thiên về an ninh quốc gia và các quy định bảo vệ quyền riêng tư cá nhân tạo ra những “vùng xám” pháp lý, khiến việc thực thi quyền của chủ thể dữ liệu đối với các giao dịch ngoại tuyến hoặc phi thương mại trở nên mơ hồ.

(2) *Hiệu quả thực thi và cơ chế phối hợp liên ngành.*

Bất cập lớn nhất nằm ở sự phân tán trong công tác quản lý nhà nước. Dù *Luật Bảo vệ dữ liệu cá nhân* năm 2025 đã định hướng Bộ Công an là cơ quan đầu mối nhưng quy trình phối hợp giữa các đơn vị chuyên ngành vẫn thiếu các hướng dẫn chi tiết về phân định trách nhiệm khi xảy ra sự cố lộ lọt dữ liệu liên tỉnh hoặc xuyên biên giới. Bên cạnh đó, các chế tài xử phạt hiện tại vẫn chưa thực sự tạo ra sức răn đe kinh tế tương xứng với lợi nhuận từ việc khai thác dữ liệu trái phép. Đối với khối doanh nghiệp vừa và nhỏ (SMEs), rào cản về chi phí công nghệ và nhân sự tuân thủ khiến việc thực hiện các nghĩa vụ như đánh giá tác động xử lý dữ liệu (DPIA) đôi khi chỉ mang tính hình thức.

(3) *Thách thức quản trị dữ liệu xuyên biên giới và tội phạm công nghệ cao.*

Sự phát triển của các nền tảng số nước ngoài không có hiện diện pháp lý hữu hình tại Việt Nam đang đặt ra thách thức về năng lực tài phán quốc gia. Việc kiểm soát dòng chảy dữ liệu ra nước ngoài hiện vẫn gặp “điểm nghẽn” về năng lực kiểm tra chuyên sâu và hợp tác quốc tế trong thu thập chứng cứ. Thực trạng này, kết hợp với sự gia tăng của tội phạm công nghệ cao, không chỉ gây thiệt hại trực tiếp về tài sản cho người tiêu dùng mà còn xói mòn niềm tin vào môi trường kinh doanh số, đe dọa đến mục tiêu phát triển bền vững của nền kinh tế trực tuyến tại Việt Nam.

(4) *Khó khăn trong việc xác định thiệt hại và cơ chế khởi kiện dân sự.*

Một trong những điểm nghẽn lớn nhất trong việc bảo vệ quyền lợi người tiêu dùng hiện nay là sự thiếu hụt các quy định hướng dẫn cụ thể về việc xác định và định giá thiệt hại do xâm phạm dữ liệu cá nhân gây ra. Dưới góc độ tố tụng dân sự, nghĩa vụ chứng minh thiệt hại thực tế thuộc về chủ thể dữ liệu (người tiêu dùng) - bên vốn dĩ yếu thế về năng lực kỹ thuật. Sự thiếu vắng các quy định về “bồi thường thiệt hại mặc định” khiến các vụ kiện dân sự về dữ liệu tại Việt Nam còn rất hạn chế, dẫn đến việc người tiêu dùng thường chấp nhận im lặng thay vì khởi kiện, làm giảm tính răn đe đối với các doanh nghiệp vi phạm.

(5) *Sự bất cập trong cơ chế quản trị dữ liệu tự động và định danh số.*

Thực tiễn thương mại điện tử hiện nay đang chứng kiến sự bùng nổ của các công cụ ra quyết định tự động dựa trên thuật toán và hồ sơ hóa dữ liệu. Tuy nhiên, khung pháp lý hiện hành chưa quy định chi tiết về quyền được giải thích đối với các quyết định tự động của sàn thương mại điện tử (như việc khóa tài khoản khách hàng, áp dụng giá cá nhân hóa hay xếp hạng tín nhiệm). Sự thiếu minh bạch trong thuật toán xử lý dữ liệu khiến người tiêu dùng dễ bị rơi vào tình trạng bị phân biệt đối xử mà không có công cụ pháp lý hữu hiệu để phản đối. Bên cạnh đó, các quy định về định danh và xác thực điện tử vẫn chưa thực sự đồng bộ với các tiêu chuẩn bảo vệ dữ liệu nhạy cảm, tạo ra kẽ hở cho các hành vi gian lận danh tính trên các nền tảng giao dịch trực tuyến.

4. Giải pháp hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân trong thương mại điện tử

Thứ nhất, chuẩn hóa và đồng bộ hóa hệ thống quy phạm pháp luật. Cần sớm ban hành các văn bản hướng dẫn thi hành *Luật Bảo vệ dữ liệu cá nhân* năm 2025 nhằm thiết

lập một “ngôn ngữ pháp lý” thống nhất; đồng thời, điều chỉnh các khái niệm tại *Bộ luật Dân sự*, *Luật Giao dịch điện tử* và *Luật Bảo vệ quyền lợi người tiêu dùng* theo hướng lấy định nghĩa tại *Luật Bảo vệ dữ liệu cá nhân* năm 2025 làm chuẩn mực gốc để loại bỏ các “vùng xám” như đã đề cập ở trên. Đồng thời, cần xác lập nguyên tắc *Luật Bảo vệ dữ liệu cá nhân* năm 2025 giữ vai trò là luật chung tạo chuẩn tối thiểu, trong khi các luật chuyên ngành chỉ bổ sung quy định đặc thù theo rủi ro lĩnh vực, tránh tình trạng một hành vi xử lý dữ liệu phải chịu sự điều chỉnh chông chéo của nhiều văn bản khác nhau.

Thứ hai, kiện toàn bộ máy thực thi và cơ chế phối hợp liên ngành. Trọng tâm của giải pháp này là xây dựng quy trình xử lý sự cố liên thông, xác định rõ trách nhiệm của Bộ Công an trong điều tra kỹ thuật, Bộ Công thương trong quản trị sàn thương mại điện tử và các cơ quan bảo vệ người tiêu dùng. Song song đó, cần ban hành các “gói tuân thủ tối thiểu” với hệ thống mẫu biểu và checklist chuẩn hóa sẽ giúp các doanh nghiệp vừa và nhỏ giảm bớt chi phí tuân thủ, từ đó chuyển dịch từ tư thế đối phó sang chủ động quản trị rủi ro.

Thứ ba, cần tăng cường năng lực quản trị dữ liệu xuyên biên giới gắn với phòng, chống tội phạm công nghệ cao. Trước các thách thức từ các nền tảng ngoại quốc không có hiện diện pháp lý hữu hình, cần kiên quyết thực thi quy định về việc chỉ định đại diện bảo vệ dữ liệu và đặt văn phòng tại Việt Nam. Nhằm xác lập đầu mối chịu trách nhiệm. Việc tham gia các mạng lưới thực thi quốc tế sẽ tạo tiền đề để truy vết, thu thập chứng cứ và xử lý các hành vi rao bán dữ liệu trái phép từ các máy chủ ngoài lãnh thổ, qua đó bảo đảm tính nghiêm minh của pháp luật nội địa trong môi trường không biên giới.

Thứ tư, cần sớm áp dụng mức phạt tiền dựa trên tỷ lệ phần trăm doanh thu đối với các

vi phạm quy mô lớn, buộc doanh nghiệp phải nội hóa chi phí rủi ro dữ liệu vào hạch toán kinh tế. Đặc biệt, cần quy định rõ cơ chế “bồi thường thiệt hại theo hướng mặc định”, cho phép ấn định mức bồi thường tối thiểu mà không buộc chủ thể dữ liệu phải chứng minh thiệt hại vật chất cụ thể.

Thứ năm, cần bổ sung quy định về “quyền được giải thích”. Các sàn thương mại điện tử phải có nghĩa vụ công khai logic cơ bản của các thuật toán gây ảnh hưởng trực tiếp đến quyền lợi kinh tế của khách hàng. Đồng thời, việc hoàn thiện tiêu chuẩn về định danh điện tử gắn liền với bảo vệ dữ liệu nhạy cảm sẽ tạo ra một lớp màng bảo vệ kép, ngăn chặn hiệu quả các hành vi gian lận danh tính và phân biệt đối xử trong các giao dịch trực tuyến, góp phần tạo dựng niềm tin bền vững cho môi trường thương mại điện tử tại Việt Nam □

Chú thích:

1. *Lộ khoảng trống giữa nhận thức và thực thi, tuân thủ bảo vệ dữ liệu cá nhân*. <https://vneconomy.vn>, ngày 20/3/2026.

Tài liệu tham khảo:

1. Chính phủ (2022). *Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 quy định chi tiết một số điều của Luật An ninh mạng năm 2022*.

2. Chính phủ (2023). *Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 về bảo vệ dữ liệu cá nhân*.

3. Quốc hội (2013, 2025). *Hiến pháp* năm 2013 (sửa đổi, bổ sung năm 2025).

4. Quốc hội (2015, 2025). *Bộ luật Dân sự* năm 2015 (sửa đổi, bổ sung năm 2025).

5. Quốc hội (2015). *Luật An toàn thông tin mạng* năm 2015.

6. Quốc hội (2025). *Luật An ninh mạng* năm 2025.

7. Quốc hội (2023). *Luật Giao dịch điện tử* năm 2023.

8. Quốc hội (2023). *Luật Bảo vệ quyền lợi người tiêu dùng* năm 2023.

9. Quốc hội (2025). *Luật Bảo vệ Dữ liệu cá nhân* năm 2025