Bảo vệ dữ liệu cá nhân trong thương mại điện tử theo quy định của pháp luật Việt Nam - Vướng mắc và định hướng hoàn thiện *

Nghiên cứu - Trao đổi

08:16 | 31/12/2025

ThS. LS. Trọng tài viên Nguyễn Đức Long

Công ty TNHH HCL Vietnam

Tóm tắt: Với sự phát triển mạnh mẽ của công nghệ thông tin, các rủi ro về xâm phạm dữ liệu cá nhân của các chủ thể, đặc biệt khi tham gia vào hoạt động thương mại điện tử, cũng ngày càng gia tăng. Do vậy, bảo vệ dữ liệu cá nhân đang trở thành vấn đề cấp thiết trong kỷ nguyên số. Bài viết phân tích quy định của pháp luật về bảo vệ dữ liệu cá nhân trong thương mại điện tử, trọng tâm là Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ quy định về bảo vệ dữ liệu cá nhân và Luật Bảo vệ dữ liệu cá nhân năm 2025, chỉ ra những tồn tại và đề xuất định hướng hoàn thiện pháp luật với mục tiêu bảo đảm sự hài hòa giữa phát triển thương mại điện tử và bảo vệ dữ liệu cá nhân của các chủ thể trong môi trường số.

Từ khóa: Luật Bảo vệ dữ liệu cá nhân; dữ liệu cá nhân; quyền riêng tư; thương mại điện tử; kỷ nguyên số; công nghệ thông tin.

Abstract: With the rapid development of information technology, the risks of personal data breaches, especially in e-commerce activities, are increasing. Therefore, protecting personal data is becoming an urgent issue in the digital age. This article analyzes legal regulations on personal data protection in e-commerce, focusing on Government Decree No. 13/2023/ND-CP dated April 17th, 2023, on personal data protection and the Law on Personal Data Protection of 2025. It identifies existing shortcomings and proposes directions for improving the law with the goal of ensuring harmony between e-commerce development and the protection of personal data of subjects in the digital environment.

Keywords: Law on Personal Data Protection; personal data; privacy rights; e-commerce; digital age; information technology.

Đặt vấn đề

Trong bối cảnh kinh tế số phát triển mạnh mẽ, dữ liệu cá nhân (DLCN) trở thành "tài nguyên" cốt lõi thúc đẩy thương mại điện tử (TMĐT) tại Việt Nam. Việc thu thập, phân tích và khai thác dữ liệu không chỉ giúp doanh nghiệp nâng cao năng lực cạnh tranh mà còn mở ra cơ hội tăng trưởng cho nền kinh tế. Tuy nhiên, đi cùng với lợi ích là nguy cơ

xâm phạm quyền riêng tư, rò rỉ hoặc lạm dụng DLCN ngày càng phức tạp. Sự ra đời của Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ quy định về bảo vệ dữ liệu cá nhân (Nghị định số 13/2023/NĐ-CP) và Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật có hiệu lực thi hành kể từ ngày 01/01/2026) đánh dấu sự hình thành khung pháp lý chuyên biệt để điều chỉnh hoạt động xử lý và bảo vệ DLCN, nhưng cũng đặt ra nhiều thách thức về thực thi và tuân thủ, đặc biệt, đối với các doanh nghiệp TMĐT. Bài viết phân tích những vướng mắc trong bảo vệ DLCN theo pháp luật Việt Nam, đánh giá khoảng trống giữa quy định và thực tiễn, từ đó, đề xuất một số giải pháp hoàn thiện pháp luật nhằm bảo đảm hài hòa giữa lợi ích kinh tế và quyền riêng tư của người tiêu dùng cá nhân.

1. Sự cần thiết phải bảo vệ dữ liệu cá nhân trong thương mại điện tử

Việc thiết lập cơ chế bảo vệ DLCN trong TMĐT là yêu cầu khách quan nhằm bảo đảm an ninh hệ thống, quyền lợi của người tiêu dùng và sự phát triển bền vững của thị trường, vì:

Thứ nhất, TMĐT vận hành trên hạ tầng kỹ thuật đa tầng và hệ sinh thái nhiều bên (website, ứng dụng di động, giao diện lập trình ứng dụng - API, cổng thanh toán, kho vận, cùng các nhà cung cấp dịch vụ bên thứ ba như giao nhận, định danh khách hàng - KYC, quảng cáo và phân tích). Cấu trúc phức hợp này mở rộng bề mặt tấn công, làm gia tăng nguy cơ khai thác lỗ hổng, xâm nhập trái phép, tấn công chuỗi cung ứng số và gây gián đoạn dịch vụ (ví dụ: DDoS). Với đặc thù hoạt động liên tục và lưu lượng giao dịch lớn, mọi sự cố đều tiềm ẩn gây ra hậu quả nghiêm trọng cho chủ thể dữ liệu và làm gián đoạn đáng kể cho doanh nghiệp.

Thứ hai, DLCN của người tiêu dùng trong TMĐT thường được chia sẻ cho nhiều đối tác (đơn vị giao nhận, trung gian thanh toán, nền tảng quảng cáo, đối tác phân tích). Nếu thiếu cơ chế kiểm soát, lượng dữ liệu được chia sẻ có thể bị sử dụng trong các quảng cáo không mong muốn, xây dựng hồ sơ hành vi phục vụ phân biệt giá hoặc bị lợi dụng cho hành vi gian lận, lừa đảo. Do đó, cần xác lập rõ quyền kiểm soát DLCN của người tiêu dùng và trách nhiệm, chuẩn mực chia sẻ dữ liệu của doanh nghiệp TMĐT.

Thứ ba, bảo đảm an toàn DLCN là điều kiện tiên quyết để TMĐT phát triển bền vững. Mặc dù tỷ trọng TMĐT trong năm 2024 đã chiếm 2/3 giá trị của nền kinh tế số Việt Nam1, nhưng lĩnh vực này còn nhiều cơ hội để phát triển nếu giải quyết được bài toán về lo ngại của người dùng đối với an toàn DLCN của họ. Những lo ngại này được phản ánh trong khảo sát: "Quyền riêng tư của người tiêu dùng năm 2024" của Cisco, khi có đến 75% người được khảo sát cho biết họ sẽ không mua hàng từ công ty mà họ không tin tưởng trong việc xử lý DLCN2. Do đó, bảo vệ DLCN cần được coi là ưu tiên của doanh nghiệp và cũng là mục tiêu điều chỉnh của pháp luật, nhằm củng cố niềm tin thị trường và nâng cao hiệu quả thực thi.

Như vậy, hoạt động TMĐT có mối liên hệ mật thiết với DLCN3, sự phát triển của TMĐT phụ thuộc vào cơ chế bảo vệ DLCN hữu hiệu. Vì vậy, việc hoàn thiện khuôn khổ pháp luật về bảo vệ DLCN nói chung và trong lĩnh vực TMĐT nói riêng là cần thiết. Bên cạnh các quy định trực tiếp về bảo vệ DLCN, pháp luật chuyên ngành về TMĐT cũng chứa đựng nhiều quy phạm liên quan đến hoạt động xử lý dữ liệu. Do đó, cần được rà soát, thống nhất và đồng bộ hóa, hình thành khung pháp lý hoàn chỉnh, nhất quán và khả thi để "trở thành công cụ bảo đảm sự an toàn về dữ liệu cá nhân cho người tiêu dùng"4.

2. Pháp luật Việt Nam về bảo vệ dữ liệu cá nhân trong thương mại điện tử

Trong lĩnh vực TMĐT và bảo vệ người tiêu dùng, pháp luật thường sử dụng các thuật ngữ "thông tin cá nhân của người tiêu dùng" hoặc "dữ liệu của người tiêu dùng", trong khi khái niệm "người tiêu dùng" gồm cả cá nhân và tổ chức. Theo pháp luật về bảo vệ DLCN, DLCN là dữ liệu gắn với một cá nhân xác định hoặc cho phép xác định một cá nhân. Vì vậy, trong bối cảnh bảo vệ người tiêu dùng, phạm vi DLCN chỉ điều chỉnh đối với người tiêu dùng là cá nhân, không bao gồm dữ liệu của tổ chức. Bên cạnh đó, theo quy định về bảo vệ DLCN, người tiêu dùng cá nhân, khách hàng cá nhân trong TMĐT được xác định là chủ thể dữ liệu cá nhân được DLCN phản ánh5.

2.1. Khung pháp lý điều chỉnh hoạt động bảo vệ dữ liệu cá nhân trong thương mại điện tử

Hệ thống pháp luật Việt Nam về bảo vệ DLCN trong TMĐT được hình thành trên ba tầng chính: (i) văn bản pháp luật về bảo vệ DLCN mang tính nền tảng; (ii) quy định chuyên ngành trong TMĐT và bảo vệ người tiêu dùng; (iii) các luật về an toàn, an ninh thông tin trong không gian số.

Thứ nhất, Nghị định số 13/2023/NĐ-CP đã chuẩn hóa các khái niệm, nguyên tắc và nghĩa vụ cơ bản liên quan đến xử lý DLCN. Đồng thời, tạo tiền đề cho việc xây dựng Luật Bảo vệ dữ liệu cá nhân năm 2025, là văn bản luật đầu tiên điều chỉnh toàn diện và thống nhất việc xử lý, bảo vệ DLCN.

Thứ hai, trong lĩnh vực TMĐT và bảo vệ người tiêu dùng, nhiều văn bản điều chỉnh các hoạt động thu thập, sử dụng và chia sẻ thông tin của khách hàng/người tiêu dùng, gồm: Luật Bảo vệ quyền lợi người tiêu dùng năm 2023, Nghị định số 52/2013/NĐ-CP ngày 16/5/2013 của Chính phủ về thương mại điện tử (Nghị định số 52/2013/NĐ-CP), Nghị định số 91/2020/NĐ-CP ngày 14/8/2020 của Chính phủ về chống tin nhắn rác, cuộc gọi rác (Nghị định số 91/2020/NĐ-CP). Các văn bản này đặt ra yêu cầu minh bạch, đồng ý, mục đích sử dụng và cơ chế khiếu nại đối với hành vi xử lý dữ liệu trong quan hệ tiêu dùng và TMĐT.

Thứ ba, khung pháp lý về an toàn thông tin và an ninh dữ liệu gồm các luật có phạm vi áp dụng rộng đối với hạ tầng số và hoạt động trên môi trường mạng, như: Luật An toàn thông

tin mạng năm 2015, Luật An ninh mạng năm 2018, Luật Giao dịch điện tử năm 2023, Luật Dữ liệu năm 2024. Các luật này thiết lập chuẩn mực về bảo đảm an toàn hệ thống thông tin, quản trị rủi ro, lưu trữ, chia sẻ và khai thác dữ liệu trong không gian số.

Hiện nay, hệ thống pháp luật về lĩnh vực này tiếp tục được hoàn thiện. Dự thảo Luật An ninh mạng dự kiến hợp nhất quy định của Luật An ninh mạng năm 2018 và Luật An toàn thông tin mạng năm 2015 (sửa đổi, bổ sung năm 2018)6 và dự thảo Luật Thương mại điện tử đang được trình Quốc hội xem xét thông qua tại Kỳ họp thứ 10 Quốc hội khóa XV để thay thế Nghị định số 52/2013/NĐ-CP vốn đang "tồn tại một số bất cập"7, hướng tới tăng cường bảo đảm an toàn thông tin, an ninh dữ liệu và bảo vệ DLCN trong môi trường điện tử theo hướng toàn diện, minh bạch và đồng bộ.

2.2. Các yêu cầu cơ bản về bảo vệ dữ liệu cá nhân trong thương mại điện tử

2.2.1. Trách nhiệm minh bạch thông tin

Trước khi xử lý DLCN, doanh nghiệp TMĐT phải thông báo về hoạt động xử lý dữ liệu, yêu cầu này tiếp tục được thể hiện trong dự thảo Luật Thương mại điện tử. Trong đó, cách tiếp cận của Nghị định số 13/2023/NĐ-CP đòi hỏi các thông tin cung cấp chi tiết hơn đáng kể so với yêu cầu trong TMĐT hay bảo vệ quyền lợi người tiêu dùng. Theo đó, bên cạnh những thông tin cơ bản, doanh nghiệp phải làm rõ cách thức xử lý, các bên được chia sẻ/ nhận dữ liệu, thời hạn lưu trữ, rủi ro có thể phát sinh8, vì vậy, nếu lựa chọn thông báo theo Nghị định số 13/2023/NĐ-CP sẽ cơ bản bao trùm các nội dung thông báo được yêu cầu trong quy định khác.

Tuy nhiên, yêu cầu thông tin quá chi tiết có thể gây khó khăn tại thời điểm thu thập, như phải xác định sẵn bên nhận dữ liệu, hệ thống kỹ thuật, thời hạn lưu trữ, rủi ro. Khi hoạt động xử lý kéo dài, thay đổi công nghệ hoặc mô hình chia sẻ dữ liệu, thông báo ban đầu có thể nhanh chóng lỗi thời. Vì vậy, Luật Bảo vệ dữ liệu cá nhân năm 2025 đã tinh gọn nội dung phải thông báo, tập trung vào các yếu tố cốt lõi, ổn định cao.

2.2.2. Trách nhiệm xin sự đồng ý

Sự đồng ý của chủ thể dữ liệu là căn cứ pháp lý trung tâm trong hệ thống pháp luật Việt Nam về bảo vệ DLCN. Khác với cách tiếp cận của Quy định bảo vệ dữ liệu chung (GDPR) của Liên minh châu Âu (EU) (nơi đồng ý thường được sử dụng sau cùng, còn "lợi ích hợp pháp" hoặc "thực hiện hợp đồng" hay được viện dẫn)9, sự đồng ý thường chỉ áp dụng khi doanh nghiệp muốn gửi các thông tin quảng cáo, tiếp thị tới chủ thể dữ liệu. Pháp luật Việt Nam đặt ra tiêu chuẩn chặt chẽ đối với sự đồng ý: phải tự nguyện, rõ ràng, có thể kiểm chứng và gắn với từng mục đích cụ thể; im lặng hoặc không phản hồi không phải là đồng

ý hợp lệ. Do đó, thông lệ "tiếp tục sử dụng dịch vụ đồng nghĩa với đồng ý" hay "sự đồng ý cho tất cả các mục đích ở hiện tại và tương lai" tiềm ẩn rủi ro vi phạm.

Trường hợp không dựa trên sự đồng ý, doanh nghiệp chỉ được xử lý khi thuộc các trường hợp ngoại lệ như xử lý dữ liệu đã công khai, xử lý để tính giá/cước dịch vụ trên môi trường mạng10. Tuy nhiên, việc áp dụng ngoại lệ không được thực hiện tùy tiện, mà phải dựa trên phân tích cụ thể và bằng chứng kèm theo; lạm dụng hoặc xác định sai căn cứ có thể dẫn tới vi phạm mang tính hệ thống, nhất là trên môi trường điện tử.

2.2.3. Bảo đảm thực thi quyền của chủ thể dữ liệu

Bảo đảm quyền của chủ thể dữ liệu là tiêu điểm phân biệt giữa DLCN và dữ liệu phi cá nhân. Việc luật hóa đầy đủ, rõ ràng và thống nhất các quyền đã khắc phục tình trạng thiếu cơ chế thực thi trong giai đoạn trước, qua đó trao cho chủ thể dữ liệu công cụ pháp lý để chủ động bảo vệ lợi ích của mình, đúng với định hướng "lấy chủ thể dữ liệu làm trung tâm".

Kế thừa Nghị định số 13/2023/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân năm 2025 xác lập 11 quyền của chủ thể dữ liệu, gồm các nhóm sau: (i) nhóm trước khi xử lý: quyền được biết; quyền đồng ý; (ii) nhóm trong khi xử lý: quyền truy cập; quyền chỉnh sửa; quyền nhận/cung cấp dữ liệu; quyền rút lại sự đồng ý; quyền yêu cầu xóa; quyền phản đối; quyền hạn chế xử lý; (iii) nhóm theo luật định khác: quyền khiếu nại; quyền tố cáo; quyền yêu cầu được bảo vệ.

Trong giai đoạn xử lý dữ liệu, Nghị định số 13/2023/NĐ-CP đặt ra thời hạn ngắn, phần lớn là 72 giờ kể từ khi nhận được yêu cầu đối với việc đáp ứng các quyền. Đây là thách thức đáng kể đối với doanh nghiệp có hệ thống xử lý quy mô lớn, kiến trúc phân tán hoặc phụ thuộc nhiều bên thứ ba.

2.2.4. Triển khai biện pháp bảo vệ dữ liệu cá nhân

Nghị định số 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định doanh nghiệp có trách nhiệm áp dụng các biện pháp phù hợp nhằm bảo đảm tính bí mật, toàn vẹn và khả dụng của DLCN trong quá trình xử lý. Hai văn bản này không quy định một danh mục biện pháp cứng nhắc, mà trao cho doanh nghiệp quyền chủ động lựa chọn và triển khai phù hợp với quy mô, đặc thù lĩnh vực hoạt động và mức độ rủi ro trong xử lý dữ liệu. Về cơ bản, các biện pháp bảo vệ DLCN được chia thành hai nhóm chính: (i) biện pháp tổ chức: ban hành chính sách/quy tắc bảo vệ dữ liệu; phân công/bổ nhiệm nhân sự phụ trách (DPO/bộ phận chuyên trách); đào tạo và nâng cao nhận thức; kiểm tra, đánh giá định kỳ; quản trị rủi ro nhà cung cấp; thiết lập cơ chế phát hiện xử lý vi phạm; quản lý vòng đời dữ liệu; (ii) biện pháp kỹ thuật: mã hóa; khử nhận dạng/ẩn danh; kiểm soát truy cập và phân

quyền; sao lưu khôi phục; giám sát nhật ký; quản lý lỗ hổng và vá lỗi; tường lửa và chống mã độc; kiểm thử an ninh định kỳ.

2.2.5. Đánh giá tác động xử lý dữ liệu, chuyển dữ liệu xuyên biên giới

Nghị định số 13/2023/NĐ-CP lần đầu ghi nhận nghĩa vụ đánh giá tác động, được Luật Bảo vệ dữ liệu cá nhân năm 2025 tiếp tục khẳng định với hai bộ hồ sơ chủ đạo: đánh giá tác động xử lý DLCN (khi có hoạt động xử lý) và đánh giá tác động chuyển DLCN xuyên biên giới (khi có chuyển ra nước ngoài). Mục tiêu là minh bạch hóa quy trình, nhận diện và lượng hóa rủi ro, từ đó đề xuất biện pháp giảm thiểu phù hợp đối với chủ thể dữ liệu và các bên liên quan. Ngoài ra, việc lập các hồ sơ này sẽ hỗ trợ tốt hơn quá trình kiểm tra, giám sát của cơ quan chức năng.

Đối với doanh nghiệp TMĐT, dữ liệu xử lý chủ yếu ở dạng điện tử, vận hành trên hạ tầng đám mây, phần mềm dịch vụ và thường xuyên chia sẻ với đối tác quốc tế; vì vậy, nghĩa vụ đánh giá tác động có thể đòi hỏi đầu tư nguồn lực đáng kể về con người, quy trình và hệ thống kỹ thuật.

2.2.6. Báo cáo sự cố

Nghị định số 13/2023/NĐ-CP yêu cầu báo cáo mọi vi phạm về DLCN trong vòng 72 giờ cho cơ quan chuyên trách thuộc Bộ Công an (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - A05) sau khi xảy ra vi phạm. Nội dung này đã được sửa đổi trong Luật Bảo vệ dữ liệu cá nhân năm 2025 khi doanh nghiệp chỉ phải báo cáo trong một số trường hợp nhất định, thời hạn thông báo vẫn là 72 giờ, nhưng tính từ thời điểm phát hiện được hành vi vi phạm. Quy định mới cho thấy, các vi phạm nhỏ sẽ được miễn trách nhiệm thông báo và thời gian để tính mốc 72 giờ cũng phù hợp hơn bởi thời điểm xảy ra vi phạm và phát hiện được vi phạm có thể cách rất xa nhau.

Nghị định số 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định, khi có sự cố tấn công hệ thống gây nguy cơ mất thông tin thì phải báo cáo cơ quan chức năng trong vòng 24 giờ. Như vậy, đối với sự cố liên quan đến DLCN, doanh nghiệp TMĐT có thể phải thực hiện hai báo cáo độc lập với khoảng thời gian khác nhau và cho các cơ quan khác nhau.

2.2.7. Xử phạt vi phạm

Luật Bảo vệ dữ liệu cá nhân năm 2025 quy định cụ thể về mức phạt tối đa dành cho tổ chức đối với vi phạm liên quan đến DLCN, gồm: (i) 10 lần khoản thu có được từ hành vi vi phạm hoặc 03 tỷ đồng đối với hành vi mua bán DLCN; (ii) 05% doanh thu của năm trước liền kề của tổ chức hoặc 03 tỷ đồng đối với hành vi vi phạm quy định chuyển DLCN xuyên

biên giới; (iii) 03 tỷ đồng đối với các hành vi vi phạm khác. Chi tiết mức phạt cho các hành vi vi phạm được quy định cụ thể trong nghị định quy định xử phạt vi phạm hành chính. Có thể thấy, mức phạt tối đa theo Luật Bảo vệ dữ liệu cá nhân năm 2025 cao hơn nhiều so với các quy định xử phạt hiện hành, thể hiện chủ trương tăng cường răn đe và bảo vệ quyền, lợi ích của chủ thể dữ liệu11.

2.3. Một số vướng mắc về pháp luật bảo vệ dữ liệu cá nhân trong thương mại điện tử

2.3.1. Pháp luật chưa theo kịp với sự phát triển của hoạt động thương mại điện tử, chồng chéo và thiếu hướng dẫn chi tiết

Những năm gần đây, TMĐT tăng trưởng mạnh, phạm vi xử lý DLCN mở rộng, công nghệ mới (trí tuệ nhân tạo (AI), công nghệ chuỗi khối (blockchain), điện toán đám mây) và dòng chảy dữ liệu xuyên biên giới trở nên phổ biến. Tuy nhiên, trục điều chỉnh vẫn dựa nhiều vào Nghị định số 52/2013/NĐ-CP (được sửa đổi, bổ sung một số điều bởi Nghị định số 85/2021/NĐ-CP ngày 25/9/2021 của Chính phủ), không còn thực sự phù hợp với thực tiễn. Nghĩa vụ bảo vệ DLCN quy định rải rác trong nhiều văn bản (Nghị định số 52/2013/NĐ-CP, Luật Bảo vệ quyền lợi người tiêu dùng năm 2023, Nghị định số 13/2023/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân năm 2025), làm cho doanh nghiệp TMĐT phải đồng thời đáp ứng nhiều lớp yêu cầu, khó nhận diện đầy đủ nghĩa vụ và dễ phát sinh chồng chéo. Vì thế, nhiều nhà nghiên cứu nhận định, quy định về bảo vệ thông tin của người tiêu dùng tại Việt Nam đang được quy định phân mảnh và thiếu nhất quán12.

2.3.2. Thời gian chuyển tiếp ngắn, thiếu văn bản hướng dẫn thi hành

Luật Bảo vệ dữ liệu cá nhân năm 2025 được ban hành tháng 6/2025, có hiệu lực từ ngày 01/01/2026. Như vậy, thời gian chuyển tiếp thực hiện từ các văn bản hiện hành sang Luật Bảo vệ dữ liệu cá nhân năm 2025 là tương đối ngắn so với mức độ phức tạp của yêu cầu tuân thủ. Kinh nghiệm quốc tế cho thấy, một số nước dành thời gian chuẩn bị dài hơn (ví dụ, EU dành 02 năm trước khi GDPR có hiệu lực13; Thái Lan sau nhiều lần gia hạn, cho doanh nghiệp thêm tới 03 năm14). Luật Bảo vệ dữ liệu cá nhân năm 2025 dự kiến cần văn bản hướng dẫn chi tiết cho các nhóm nội dung trọng yếu (đánh giá tác động, chuyển dữ liệu xuyên biên giới, thực thi quyền của chủ thể dữ liệu, xử lý vi phạm…), nhưng đến nay dự thảo các văn bản hướng dẫn thi hành chưa được ban hành. Việc thiếu hướng dẫn chi tiết cản trở doanh nghiệp, đặc biệt, trong TMĐT, lập kế hoạch, phân bổ nguồn lực và xây dựng lộ trình tuân thủ, làm tăng rủi ro không kịp đáp ứng nghĩa vụ khi mốc hiệu lực thi hành Luật Bảo vệ dữ liệu cá nhân năm 2025 đến gần.

2.3.3. Không thống nhất về phạm vi "thông tin cá nhân" và "dữ liệu cá nhân"

Khái niệm "thông tin cá nhân" tại Nghị định số 52/2013/NĐ-CP có phạm vi hẹp hơn, loại trừ một số dữ liệu liên hệ công việc hoặc dữ liệu đã công bố trên phương tiện truyền thông. Ngược lại, Nghị định số 13/2023/NĐ-CP và Luật Bảo vệ dữ liệu cá nhân 2025 mở rộng "DLCN" tới cả dữ liệu có thể xác định hoặc "làm rõ" về một cá nhân khi kết hợp với dữ liệu khác và không loại trừ dữ liệu đã công khai. Do đó, nếu doanh nghiệp chỉ căn cứ Nghị định số 52/2013/NĐ-CP để xác định phạm vi thông tin được bảo vệ (ví dụ, coi dữ liệu công khai trên mạng xã hội không phải DLCN), họ có nguy cơ vi phạm Luật Bảo vệ dữ liệu cá nhân năm 2025, như thiếu căn cứ xử lý (đồng ý/ngoại lệ) hoặc từ chối thực hiện quyền của chủ thể dữ liệu.

Quy định nhiều hình thức cung cấp thông tin trước khi xử lý dữ liệu cá nhân. Nghĩa vụ cung cấp thông tin trước khi thu thập sự đồng ý đều được thể hiện trong nhiều văn bản pháp luật, tuy nhiên, mỗi văn bản lại có cách tiếp cận khác nhau về hình thức thể hiện.

Nghị định số 52/2013/NĐ-CP yêu cầu doanh nghiệp ban hành chính sách bảo vệ thông tin cá nhân, Luật Bảo vệ quyền lợi người tiêu dùng năm 2023 quy định doanh nghiệp phải ban hành Quy tắc bảo vệ thông tin người tiêu dùng. Trong khi đó, Nghị định số 13/2023/NĐ-CP, Luật Bảo vệ dữ liệu cá nhân năm 2025 chỉ yêu cầu thông báo mà không ấn định hình thức thể hiện bằng một tên gọi cụ thể. Hệ quả là doanh nghiệp TMĐT có thể phải ban hành nhiều tài liệu khác tên nhưng nội dung trùng lặp, khó duy trì đồng bộ và dễ mâu thuẫn, gây quá tải thông tin đối với người tiêu dùng.

2.3.4. Thời gian để đáp ứng yêu cầu của chủ thể dữ liệu quá ngắn

Nghị định số 13/2023/NĐ-CP quy định thời hạn 72 giờ để doanh nghiệp thực hiện một số quyền của chủ thể dữ liệu (hạn chế, phản đối, xóa, cung cấp, chỉnh sửa dữ liệu…). Đây là khoảng thời gian ngắn, đặc biệt, khi DLCN được lưu trữ và xử lý trên nhiều hệ thống, đã chia sẻ cho bên thứ ba. Trên thực tế, chỉ riêng việc: xác minh tính hợp pháp của yêu cầu; truy vết nơi dữ liệu đang tồn tại; tổ chức xóa/hủy hoặc điều chỉnh dữ liệu có thể tiêu tốn hầu hết quỹ thời gian theo quy định; chưa kể các trường hợp dữ liệu do đối tác ngoài tổ chức quản lý, làm cho tiến độ thực hiện phụ thuộc vào sự phối hợp của bên nhận dữ liệu. Vì vậy, nguy cơ doanh nghiệp không kịp đáp ứng thời hạn và phát sinh xử phạt là đáng kể nếu không có quy trình, công cụ và thỏa thuận liên kết phù hợp.

2.3.5. Trách nhiệm báo cáo sự cố, vi phạm về dữ liệu cá nhân

Như đã phân tích, Nghị định số 52/2013/NĐ-CP và Luật Bảo vệ quyền lợi người tiêu dùng năm 2023 yêu cầu doanh nghiệp báo cáo trong 24 giờ khi xảy ra sự cố tấn công hệ thống gây nguy cơ mất an toàn thông tin, kể cả khi mới dừng ở mức "nguy cơ". Trong bối cảnh các hệ thống TMĐT lớn thường xuyên hứng chịu tấn công, không phải lúc nào doanh

nghiệp cũng có thể đánh giá kịp thời mức độ và khả năng hiện thực hóa rủi ro. Việc thiếu tiêu chí định lượng rõ ràng về "ngưỡng báo cáo", trong khi thời hạn thông báo rất ngắn, dễ tạo gánh nặng tuân thủ. Ngoài ra, quy định hiện hành chưa xác định cụ thể cơ quan tiếp nhận làm cho doanh nghiệp TMĐT lúng túng trong triển khai.

Bên cạnh đó, khi sự cố vi phạm DLCN thực sự xảy ra, doanh nghiệp còn phải báo cáo trong 72 giờ tới cơ quan chuyên trách của Bộ Công an, theo pháp luật bảo vệ DLCN. Như vậy, doanh nghiệp TMĐT có nguy cơ phải thực hiện hai kênh báo cáo với tiêu chí kích hoạt, thời hạn và đầu mối khác nhau, làm tăng độ phức tạp và rủi ro sai sót nếu không có quy trình hợp nhất, tiêu chí phân loại sự cố và cơ chế phối hợp nội bộ/đối tác rõ ràng.

2.3.6. Chưa có quy định về quyền riêng tư theo thiết kế và theo mặc định

Pháp luật hiện hành chưa quy định cụ thể, rõ ràng và ràng buộc nghĩa vụ về quyền riêng tư theo thiết kế và theo mặc định (Privacy by Design/Default) đối với các nền tảng TMĐT quy mô lớn, trong khi chuẩn mực quốc tế (ví dụ, GDPR, Điều 25; ISO/IEC 31700) yêu cầu tích hợp bảo vệ dữ liệu ngay từ kiến trúc và xuyên suốt vòng đời phát triển phần mềm, ứng dụng nói chung và TMĐT nói riêng.

Các quy định pháp luật hiện hành chủ yếu dừng ở nguyên tắc mục đích, tối thiểu hóa và an ninh, chưa đặt ra cơ chế phân tầng rủi ro theo quy mô/ngưỡng xử lý để áp dụng tiêu chuẩn nghiêm ngặt hơn cho hệ sinh thái dữ liệu phức tạp. Đồng thời, chưa có chỉ số đo lường vận hành (KPIs) và bằng chứng quyền riêng tư theo thiết kế/theo mặc định bắt buộc (ví dụ, theo dõi tắt mặc định; cấu hình chia sẻ ở chế độ giới hạn; nhật ký quyết định thiết kế, đánh giá rủi ro khi ứng dụng AI; thời hạn chuẩn để thực hiện quyền), cũng như khung chứng nhận/kỹ thuật chuyên biệt cho TMĐT giúp chuyển hóa yêu cầu pháp lý thành quy trình bắt buộc và tiêu chí giám sát cụ thể.

Hệ quả là nhiều website/ứng dụng không cài đặt cơ chế bảo vệ ngay từ đầu, dẫn đến thu thập quá mức, theo dõi thiếu minh bạch và hạn chế công cụ thực thi quyền; khi bị yêu cầu tuân thủ, doanh nghiệp phải "vá" hệ thống đang vận hành, phát sinh chi phí lớn, gián đoạn hoạt động và rủi ro không đáp ứng được các nghĩa vụ khi xử lý DLCN.

3. Một số kiến nghị hoàn thiện pháp luật về bảo vệ dữ liệu cá nhân trong thương mại điện tử

Từ những bất cập trên, nghiên cứu đề xuất một số kiến nghị nhằm hoàn thiện pháp luật về bảo vệ DLCN nói chung và trong hoạt động TMĐT nói riêng, theo hướng thống nhất, khả thi và phù hợp thực tiễn. Cụ thể:

Thứ nhất, sớm ban hành Luật Thương mại điện tử và văn bản hướng dẫn chi tiết về xử lý DLCN để giảm chồng chéo.

Cần sớm ban hành Luật Thương mại điện tử để quản lý tập trung, thống nhất hoạt động TMĐT (dự thảo Luật đã trình và dự kiến được Quốc hội thông qua vào kỳ họp tháng 11/2025). Để tránh chồng chéo với pháp luật về bảo vệ DLCN, Luật Thương mại điện tử không nên đi sâu điều chỉnh chi tiết các vấn đề về DLCN, mà nên dẫn chiếu và tuân thủ thống nhất theo Luật Bảo vệ dữ liệu cá nhân năm 2025. Luật Thương mại điện tử chỉ nên quy định các ngoại lệ đặc thù phục vụ nhu cầu vận hành TMĐT (nếu thực sự cần thiết), nhưng phải phù hợp nguyên tắc và cơ chế xử lý xung đột pháp luật của Luật Bảo vệ dữ liệu cá nhân năm 2025. Đồng thời, khi Luật Thương mại điện tử có hiệu lực, Nghị định số 52/2013/NĐ-CP, đặc biệt, các quy định về bảo vệ thông tin cá nhân người tiêu dùng, nên chấm dứt hiệu lực để loại trừ trùng lặp.

Cách tiếp cận này sẽ tự động tháo gỡ các mâu thuẫn hiện hành (như sự khác biệt giữa "thông tin cá nhân", "thông tin người tiêu dùng" và "dữ liệu cá nhân"), thống nhất nghĩa vụ minh bạch và hình thức thông báo, giúp doanh nghiệp TMĐT dễ xác định trách nhiệm, xây dựng quy trình xử lý và bảo vệ DLCN hiệu quả, nhất quán.

Thứ hai, kéo dài thời hạn xử lý yêu cầu của chủ thể dữ liệu.

Để doanh nghiệp nói chung và doanh nghiệp TMĐT nói riêng, có đủ thời gian: (i) thẩm tra tính hợp lệ của yêu cầu; định vị dữ liệu trong toàn bộ hệ thống và các bên nhận; đánh giá tác động của việc đáp ứng yêu cầu đối với hệ thống và hoạt động kinh doanh; (ii) tổ chức thực hiện yêu cầu, cần kéo dài thời hạn phản hồi hiện nay. Có thể tham khảo thông lệ: GDPR cho phép phản hồi trong 30 ngày và có thể gia hạn thêm 60 ngày đối với trường hợp phức tạp15; Đạo luật Quyền riêng tư người tiêu dùng của California (CCPA) quy định 45 ngày và có thể gia hạn thêm 45 ngày khi cần, với điều kiện phải thông báo việc gia hạn cho chủ thể dữ liệu16. Bên cạnh đó, cần cân nhắc cơ chế "dừng tính thời hạn" (stop the clock) đối với giai đoạn xác minh danh tính, làm rõ phạm vi yêu cầu hoặc bổ sung thông tin; cách tiếp cận này tương đồng với việc điều chỉnh tại Đạo luật Dữ liệu của Vương quốc Anh, giúp thời hạn phản hồi phản ánh đúng khối lượng công việc thực tế và không bị chủ thể dữ liệu lạm dụng17.

Thứ ba, làm rõ chế độ báo cáo vi phạm về dữ liệu cá nhân.

Khi xảy ra sự cố, quan trọng nhất là tập trung vào việc khắc phục, giảm thiểu tối đa tác động đến hoạt động kinh doanh. Do đó, mặc dù việc thông báo là cần thiết để cơ quan nhà nước kịp thời cung cấp các hỗ trợ nhưng cần tính toán để bảo đảm đơn giản, hiệu quả. Một số đề xuất, gồm: (i) thống nhất ngưỡng báo cáo: chỉ kích hoạt nghĩa vụ báo cáo đối với sự

cố/vi phạm có tác động đáng kể theo tiêu chí định lượng (quy mô dữ liệu, loại dữ liệu nhạy cảm, số lượng chủ thể bị ảnh hưởng, rủi ro quyền và lợi ích,…); (ii) thống nhất mốc thời gian: áp dụng 72 giờ kể từ thời điểm phát hiện sự cố/vi phạm theo Luật Bảo vệ dữ liệu cá nhân năm 2025; mốc 24 giờ là quá ngắn và thiếu khả thi, nhất là khi sự cố rơi vào ngày nghỉ/ngày lễ; (iii) thống nhất đầu mối tiếp nhận: thiết lập cơ chế báo cáo "một cửa" tới cơ quan chuyên trách về bảo vệ dữ liệu; cơ quan này sẽ điều phối với các cơ quan nhà nước liên quan khi cần. Cách làm này giảm trùng lặp báo cáo, rút ngắn thời gian xử lý và nâng cao hiệu quả ứng phó, thay vì buộc doanh nghiệp báo cáo nhiều cơ quan với nhiều khung thời gian như hiện nay.

Thứ tư, bổ sung quy định quyền riêng tư theo thiết kế và theo mặc định trong phát triển phần mềm, ứng dụng thương mại điện tử.

Cần quy định rõ nghĩa vụ này trong văn bản pháp luật, nhằm bảo đảm các doanh nghiệp tích hợp nguyên tắc quyền riêng tư có hệ thống. Việt Nam có thể tham khảo Điều 25 GDPR và Hướng dẫn 4/2019 của Ủy ban Bảo vệ dữ liệu châu Âu (EDPB) về quyền riêng tư theo thiết kế và theo mặc định, gồm yêu cầu chủ động tích hợp các biện pháp kiểm soát quyền riêng tư xuyên suốt vòng đời sản phẩm từ phân tích yêu cầu, thiết kế, thử nghiệm đến triển khai và cập nhật gắn liền với trách nhiệm giải trình18.

Từ góc độ quản trị rủi ro, nên áp dụng cơ chế phân tầng nghĩa vụ, theo đó, các nền tảng TMĐT đạt quy mô lớn hoặc xử lý lượng dữ liệu nhạy cảm vượt ngưỡng nhất định phải thực hiện đánh giá rủi ro bắt buộc đối với tính năng mới và công nghệ mới (như việc ứng dụng, sử dụng AI hoặc blockchain). Đồng thời, duy trì các chỉ số định lượng (KPIs) để đo lường hiệu quả, như tỷ lệ cài đặt chế độ riêng tư mặc định, tỷ lệ tắt theo dõi hoặc thời hạn lưu trữ tối đa.

Bên cạnh đó, cần cân nhắc xây dựng chuẩn mực kỹ thuật và cơ chế chứng nhận phù hợp với thông lệ quốc tế. Việt Nam có thể tham khảo các tiêu chuẩn như ISO/IEC 31700:2023 (Bảo vệ người tiêu dùng - Quyền riêng tư theo thiết kế cho hàng hóa và dịch vụ tiêu dùng), ISO/IEC 27701:2019 (Quản lý thông tin quyền riêng tư)19 hoặc mô hình chứng nhận/đánh dấu tin cậy như Data Protection Trustmark (DPTM) của IMDA Singapore20, nhằm chuẩn hóa quy trình kiểm toán, báo cáo và công bố tuân thủ. Doanh nghiệp phải cung cấp bằng chứng cụ thể (như ma trận mục đích dữ liệu, nhật ký quyết định thiết kế hoặc kết quả thử nghiệm) cho cơ quan chức năng khi có yêu cầu.

Cách tiếp cận này không chỉ giảm thiểu tình trạng "vá" hệ thống sau khi phát sinh yêu cầu pháp lý, mà còn nâng cao tính minh bạch, khả năng thực thi quyền của chủ thể dữ liệu và niềm tin thị trường đối với lĩnh vực TMĐT.

Kết luận Bảo vệ DLCN trong TMĐT không chỉ là yêu cầu pháp lý mà còn là yếu tố nền tảng để xây dựng niềm tin của người tiêu dùng, thúc đẩy cạnh tranh bền vững và bảo đảm an ninh quốc gia trong kỷ nguyên số. Phân tích cho thấy hệ thống pháp luật Việt Nam đã có bước tiến quan trọng, song còn tồn tại chồng chéo, khoảng trống và nguy cơ không đồng bộ khi Luật Bảo vệ dữ liệu cá nhân năm 2025 chính thức có hiệu lực. Việc ban hành Luật Thương mại điện tử mới cùng các văn bản hướng dẫn chi tiết và cơ chế thực thi minh bạch, sẽ giúp doanh nghiệp TMĐT định hình chiến lược tuân thủ rõ ràng, giảm rủi ro pháp lý và nâng cao hiệu quả bảo vệ dữ liệu. Đồng thời, tăng cường nhận thức của người tiêu dùng và năng lực quản lý của cơ quan chức năng sẽ là chìa khóa để các quy định pháp luật đi vào thực chất, tạo môi trường TMĐT an toàn, tin cậy và phát triển bền vững./.

Ảnh: Internet

* Bài viết được thực hiện trong khuôn khổ Đề tài nghiên cứu khoa học cấp cơ sở: *"Pháp luật Việt Nam về thương mại điện tử - Thực trạng và giải pháp đáp ứng yêu cầu hội nhập và phát triển trong kỷ nguyên mới"*, Trường Đại học Luật Hà Nội, 2025.

[1]. Vũ Khuê (2025), *Tỷ trọng thương mại điện tử chiếm 2/3 giá trị của nền kinh tế số Việt Nam*, https://vneconomy.vn/ty-trong-thuong-mai-dien-tu-chiem-2-3-gia-tri-cua-nen-kinh-te-so-viet-nam.htm, truy cập ngày 19/11/2025.

[2]. Cisco (2024), *Cisco 2024 Consumer Privacy Survey Report*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf, truy cập ngày 19/11/2025.

[3]. Nguyễn Thành Minh Chánh, Vương Thị Thu Thùy, Trương Ngọc Bảo Nhi và Trịnh Võ Minh Luật (2024), *Bảo vệ quyền riêng tư, dữ liệu cá nhân của người tiêu dùng trong thương mại điện tử*, https://tapchitoaan.vn/bao-ve-quyen-rieng-tu-du-lieu-ca-nhan-cua-nguoi-tieu-dung-trong-thuong-mai-dien-tu12105.html, truy cập ngày 19/11/2025.

[4]. Xa Kiều Oanh, Nguyễn Phạm Thanh Hoa (2025), *So sánh pháp luật EU và Việt Nam về bảo vệ dữ liệu cá nhân của người tiêu dùng khi mua sắm trực tuyến và khuyến nghị cho Việt Nam*, https://phapluatphattrien.vn/so-sanh-phap-luat-eu-va-viet-nam-ve-bao-ve-du-lieu-ca-nhan-cua-nguoi-tieu-dung-khi-mua-sam-truc-tuyen-va-khuyen-nghi-cho-viet-nam-d4178.html, truy cập ngày 19/11/2025.

[5]. Khoản 5 Điều 2 Luật Bảo vệ dữ liệu cá nhân năm 2025.

[6]. *Hợp nhất Luật An ninh mạng và Luật An toàn thông tin mạng*, https://hvctcand.bocongan.gov.vn/nha-nuoc-va-phap-luat/hop-nhat-luat-an-ninh-mang-va-luat-an-toan-thong-tin-mang-7514, truy cập ngày 19/11/2025.

[7]. Lê Huỳnh Phương Chinh, Ngô Thị Khánh Linh (2025), *Thực trạng bảo vệ dữ liệu cá nhân trong thương mại điện tử và một số kiến nghị*, https://tapchinganhang.gov.vn/thuc-trang-bao-ve-du-lieu-ca-nhan-trong-thuong-mai-dien-tu-va-mot-so-kien-nghi-16137.html, truy cập ngày 19/11/2025.

[8]. Điều 11, Điều 13 Nghị định số 13/2023/NĐ-CP.

[9]. Điều 6 GDPR.

[10]. Khoản 4 Điều 70 Nghị định số 52/2013/NĐ-CP; Điều 17 Luật Bảo vệ dữ liệu cá nhân năm 2025.

[11]. Nghị định số 15/2020/NĐ-CP (được sửa đổi, bổ sung năm 2025) và Nghị định số 98/2020/NĐ-CP (được sửa đổi, bổ sung năm 2025).

[12]. Nguyễn Thị Thu Hằng (2019), *Bàn về vấn đề bảo vệ thông tin cá nhân của người tiêu dùng trong thương mại điện tử*, Tạp chí Khoa học Pháp lý, Trường Đại học Luật TP. Hồ Chí Minh, Số 2, tr. 18 - 25; Đoàn Quỳnh Thương (2020), Hoàn thiện pháp luật thương mại điện tử Việt Nam trong bối cảnh thực thi Hiệp định Thương mại điện tử ASEAN 2019, Tạp chí Luật học, Trường Đại học Luật Hà Nội, Số 12, tr. 85 - 99.

[13]. Theo Điều 99 GDPR, Quy định này có hiệu lực từ ngày 24/5/2016 và được áp dụng kể từ ngày 25/5/2018, sau thời gian chuyển tiếp 02 năm kể từ ngày có hiệu lực.

[14]. DLA Piper (2025), *Data protection laws in Thailand*, https://www.dlapiperdataprotection.com/index.html?t=law&c=TH, truy cập ngày 19/11/2025.

[15]. Điều 12 GDPR.

[16]. California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5, truy cập ngày 27/11/2025.

[17]. Chính phủ Vương quốc Anh (2025), *Data (Use and Access) Act factsheet: UK GDPR and DPA*, https://www.gov.uk/government/publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa, truy cập ngày 27/11/2025.

[18]. EDPB (2019), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, truy cập ngày 27/11/2025.

[19]. Tổ chức Quốc tế về Tiêu chuẩn hóa - ISO, *ISO/DIS 31700(en)Consumer protection - Privacy by design for consumer goods and services*, https://www.iso.org/obp/ui/#iso:std:iso:31700:dis:ed-1:v1:en, truy cập ngày 28/11/2025.

[20]. Cơ quan Phát triển Truyền thông và Thông tin Singapore - IMDA, *Data Protection Trustmark Certification*, https://www.imda.gov.sg/-/media/imda/files/programme/dptm/dptm-information-kit.pdf, truy cập ngày 28/11/2025.

TÀI LIỆU THAM KHẢO

1. Vũ Khuê (2025), *Tỷ trọng thương mại điện tử chiếm 2/3 giá trị của nền kinh tế số Việt Nam*, https://vneconomy.vn/ty-trong-thuong-mai-dien-tu-chiem-2-3-gia-tri-cua-nen-kinh-te-so-viet-nam.htm, truy cập ngày 19/11/2025.

2. Cisco (2024), *Cisco 2024 Consumer Privacy Survey Report*, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf, truy cập ngày 19/11/2025.

3. Nguyễn Thành Minh Chánh, Vương Thị Thu Thùy, Trương Ngọc Bảo Nhi và Trịnh Võ Minh Luật (2024), *Bảo vệ quyền riêng tư, dữ liệu cá nhân của người tiêu dùng trong thương mại điện tử*, https://tapchitoaan.vn/bao-ve-quyen-rieng-tu-du-lieu-ca-nhan-cua-nguoi-tieu-dung-trong-thuong-mai-dien-tu12105.html, truy cập ngày 19/11/2025.

4. Xa Kiều Oanh, Nguyễn Phạm Thanh Hoa (2025), *So sánh pháp luật EU và Việt Nam về bảo vệ dữ liệu cá nhân của người tiêu dùng khi mua sắm trực tuyến và khuyến nghị cho Việt Nam*, https://phapluatphattrien.vn/so-sanh-phap-luat-eu-va-viet-nam-ve-bao-ve-du-lieu-ca-nhan-cua-nguoi-tieu-dung-khi-mua-sam-truc-tuyen-va-khuyen-nghi-cho-viet-nam-d4178.html, truy cập ngày 19/11/2025.

5. Hợp nhất Luật An ninh mạng và Luật An toàn thông tin mạng, https://hvctcand.bocongan.gov.vn/nha-nuoc-va-phap-luat/hop-nhat-luat-an-ninh-mang-va-luat-an-toan-thong-tin-mang-7514, truy cập ngày 19/11/2025.

6. Lê Huỳnh Phương Chinh, Ngô Thị Khánh Linh (2025), *Thực trạng bảo vệ dữ liệu cá nhân trong thương mại điện tử và một số kiến nghị*, https://tapchinganhang. gov.vn/thuc-trang-bao-ve-du-lieu-ca-nhan-trong-thuong-mai-dien-tu-va-mot-so-kien-nghi-16137.html, truy cập ngày 19/11/2025.

7. Nguyễn Thị Thu Hằng (2019), *Bàn về vấn đề bảo vệ thông tin cá nhân của người tiêu dùng trong thương mại điện tử*, Tạp chí Khoa học Pháp lý, Trường Đại học Luật TP. Hồ Chí Minh, Số 2.

8. Đoàn Quỳnh Thương (2020), *Hoàn thiện pháp luật thương mại điện tử Việt Nam trong bối cảnh thực thi Hiệp định Thương mại điện tử ASEAN 2019*, Tạp chí Luật học, Trường Đại học Luật Hà Nội, Số 12.

9. California Consumer Privacy Act of 2018, https://leginfo.legislature.ca.gov/faces/codes_ displayText.xhtml?division=3.&part=4.& lawCode=CIV&title=1.81.5, truy cập ngày 27/11/2025.

10. Chính phủ Vương quốc Anh (2025), *Data (Use and Access) Act factsheet: UK GDPR and DPA*, https://www.gov.uk/government/ publications/data-use-and-access-act-2025-factsheets/data-use-and-access-act-factsheet-uk-gdpr-and-dpa, truy cập ngày 27/11/2025.

11. EDPB (2019), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, https://www.edpb.europa. eu/sites/default/files/files/file1/edpb_ guidelines_201904_dataprotection_by_ design_and_by_default_v2.0_en.pdf, truy cập ngày 27/11/2025.

12. Tổ chức Quốc tế về Tiêu chuẩn hóa - ISO, *ISO/DIS 31700(en)Consumer protection - Privacy by design for consumer goods and services*, https://www.iso.org/obp/ui/#iso:std:iso:31700:dis:ed-1:v1:en, truy cập ngày 28/11/2025.

13. Cơ quan Phát triển Truyền thông và Thông tin Singapore - IMDA, *Data Protection Trustmark Certification*, https://www.imda.gov.sg/-/media/imda/files/programme/dptm/dptm-information-kit.pdf, truy cập ngày 28/11/2025.