

BẢO VỆ DỮ LIỆU CÁ NHÂN TRONG KINH DOANH TRỰC TUYẾN: TỪ QUYỀN RIÊNG TƯ ĐẾN TRÁCH NHIỆM GIẢI TRÌNH

NGUYỄN HỒNG PHƯƠNG

Trường Đại học Luật Hà Nội

Hanoi Law University

Email: littlepea239@gmail.com

Ngày nhận bài: 14/7/2026

Ngày sửa bài: 28/7/2026

Ngày duyệt đăng bài: 14/8/2026

Tóm tắt:

Bảo vệ dữ liệu cá nhân trong kinh doanh trực tuyến đang chuyển từ một vấn đề bảo mật kỹ thuật thành yêu cầu quản trị pháp lý xuyên suốt vòng đời dữ liệu. Bài viết phân tích khung pháp lý Việt Nam, gồm Luật Bảo vệ dữ liệu cá nhân năm 2025, Nghị định số 356/2025/NĐ-CP và Luật Thương mại điện tử năm 2025; đối chiếu kinh nghiệm tại Singapore, Hàn Quốc và Liên minh châu Âu. Trên cơ sở phương pháp phân tích quy phạm, nghiên cứu tình huống và so sánh pháp luật, bài viết nhận diện 4 nhóm rủi ro: sự đồng ý mang tính hình thức; kiểm soát nhân sự và bên xử lý dữ liệu; tệp cookie, công nghệ theo dõi và lập hồ sơ hành vi; chuyển dữ liệu xuyên biên giới. Kết quả nghiên cứu cho thấy trọng tâm hoàn thiện không nên chỉ là tăng chế tài, mà cần chuyển sang mô hình trách nhiệm giải trình có thể kiểm chứng, quản trị dựa trên rủi ro, bảo vệ dữ liệu ngay từ thiết kế và chuẩn hóa trách nhiệm trong toàn bộ chuỗi xử lý dữ liệu.

Từ khóa: dữ liệu cá nhân, kinh doanh trực tuyến, thương mại điện tử, quyền riêng tư, trách nhiệm giải trình

Personal data protection in online business: From privacy to accountability

Abstract:

Personal data protection in online business is evolving from a technical security issue into a legal governance obligation covering the entire data lifecycle. This study examines Vietnam's legal framework under the 2025 Law on Personal Data Protection, Decree No. 356/2025/ND-CP, and the 2025 Law on E-Commerce, while comparing selected experience from Singapore, South Korea, and the European Union. Using doctrinal analysis, case studies, and comparative law, the study identifies four major risk areas: formalistic consent, control of employees and data processors, cookies and behavioral tracking, and cross-border data transfers. It argues that legal reform should not focus solely on stronger sanctions but should promote demonstrable accountability, risk-based governance, data protection by design, and clearer responsibility throughout the entire data-processing chain.

Keywords: personal data, online business, e-commerce, privacy, accountability

1. Đặt vấn đề

Kinh doanh trực tuyến tạo ra một nghịch lý pháp lý đáng chú ý: giao dịch càng thuận tiện thì chuỗi xử lý dữ liệu phía sau càng phức tạp. Một đơn hàng trên nền tảng số có thể phát sinh đồng thời dữ liệu định danh, địa chỉ, thiết bị, lịch sử mua sắm, thanh toán, vị trí và dấu vết hành vi; các dữ liệu này đi qua nền tảng, người bán, đơn vị thanh toán, dịch vụ hậu cần, nhà cung cấp hạ tầng, công cụ phân tích và mạng quảng cáo. Vì vậy, rủi ro không chỉ nằm ở sự có “lộ dữ liệu”, mà xuất hiện ngay từ quyết định thu thập dữ liệu nào, dùng cho mục đích gì, chia sẻ cho ai, lưu bao lâu và dựa trên căn cứ pháp lý nào.

Việt Nam đã bước sang một giai đoạn điều chỉnh mới. Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP có hiệu lực từ ngày 01/01/2026; Luật Thương mại điện tử số 122/2025/QH15 và Luật An ninh mạng số 116/2025/QH15 có hiệu lực từ ngày 01/07/2026 (Chính phủ, 2025; Quốc hội, 2025a, 2025b, 2025c). Luật An ninh mạng sau đó được sửa đổi một phần bởi Luật Đầu tư số 143/2025/QH15. Bảo vệ dữ liệu cá nhân vì vậy không còn thể xử lý bằng một điều khoản bảo mật chung hoặc giao riêng cho bộ phận công nghệ thông tin.

Khoảng trống cần làm rõ nằm ở cách chuyển các nguyên tắc pháp lý thành chuẩn quản trị phù hợp với chuỗi kinh doanh trực tuyến nhiều chủ thể. Sự đồng ý trên giao diện số, trách nhiệm với nhà cung cấp, theo dõi hành vi, lập hồ sơ người dùng và chuyển dữ liệu xuyên biên giới đặt ra câu hỏi không chỉ về tính hợp pháp của việc xử lý mà còn về khả năng doanh nghiệp chứng minh đã kiểm soát rủi ro thực chất.

Mục tiêu của bài viết là: (i) làm rõ cơ sở tiếp cận dữ liệu cá nhân vừa gắn với quyền riêng tư vừa có giá trị kinh tế; (ii) đánh giá điểm tiên bộ và điểm nghẽn trong thực thi pháp luật Việt Nam đối với kinh doanh trực tuyến; (iii) rút bài học từ kinh nghiệm quốc tế; và (iv) đề xuất giải pháp theo hướng trách nhiệm giải trình, quản trị dựa trên rủi ro và bảo vệ dữ liệu trong toàn bộ vòng đời xử lý. Đóng góp của nghiên cứu là kết nối các lớp pháp luật hiện hành với kiến trúc quản trị dữ liệu thực tế của doanh nghiệp.

2. Cơ sở lý thuyết và phương pháp nghiên cứu

2.1. Cơ sở lý thuyết

Bài viết dựa trên 3 trụ cột lý luận có quan hệ chặt chẽ, cụ thể là:

Thứ nhất, cách tiếp cận dựa trên quyền. Dữ liệu cá nhân không phải một hàng hóa thuần túy vì thông tin về một con người gắn trực tiếp với đời sống riêng tư, danh tính và khả năng tự quyết của chính cá nhân đó. Việc cá nhân cung cấp số điện thoại, địa chỉ hoặc dữ liệu thanh toán để hoàn thành giao dịch không mặc nhiên làm phát sinh quyền khai thác vô hạn cho doanh nghiệp. Do đó, giá trị thương mại của dữ liệu phải bị giới hạn bởi mục đích hợp pháp, tính minh bạch và quyền của chủ thể dữ liệu.

Thứ hai, lý thuyết trách nhiệm giải trình. Nếu cách tiếp cận truyền thống chủ yếu hỏi doanh nghiệp có tuân thủ một nghĩa vụ cụ thể hay không, trách nhiệm giải trình đòi hỏi doanh nghiệp phải tổ chức hệ thống để chứng minh sự tuân thủ. Trong pháp luật Việt Nam, logic này thể hiện ở việc bên kiểm soát dữ liệu phải xác định mục đích và phương tiện xử lý, lựa chọn bên xử lý phù hợp, thực hiện biện pháp quản lý và kỹ thuật, bảo đảm quyền của chủ thể dữ liệu và chịu trách nhiệm đối với thiệt hại do xử lý gây ra. Đây là nền tảng để nhìn bảo vệ dữ liệu như một chức năng quản trị doanh nghiệp, không chỉ là nhiệm vụ bảo mật.

Thứ ba, quản trị dựa trên rủi ro. Mức độ nghĩa vụ cần gắn với quy mô, tính chất và tác động của hoạt động xử lý. Một nền tảng có hàng triệu người dùng, xử lý dữ liệu vị trí, tài chính hoặc sinh trắc học không thể được đánh giá theo cùng chuẩn với một hộ kinh doanh xử lý vài trăm đơn hàng. Cách tiếp cận này phù hợp với nguyên tắc “bảo vệ dữ liệu ngay từ thiết kế và theo mặc định” của GDPR: bảo vệ dữ liệu phải được tích hợp vào thiết kế hệ thống và cấu hình mặc định, thay vì chỉ bổ sung sau khi sản phẩm đã vận hành (Nghị viện châu Âu và Hội đồng Liên minh châu Âu, 2016).

2.2. Phương pháp nghiên cứu

Bài viết sử dụng phương pháp nghiên cứu định tính. Phương pháp phân tích quy phạm được dùng để đối chiếu Luật Bảo vệ dữ liệu cá nhân năm 2025, Nghị định số 356/2025/NĐ-CP, Luật Thương mại điện

từ năm 2025, Luật Bảo vệ quyền lợi người tiêu dùng năm 2023 và các quy định liên quan. Phương pháp nghiên cứu tình huống được sử dụng đối với Bản án số 63/2022/HS-ST của Tòa án nhân dân tỉnh Hải Dương và các quyết định thực thi của cơ quan bảo vệ dữ liệu Singapore, Hàn Quốc, Pháp. Phương pháp so sánh pháp luật được sử dụng có chọn lọc, thay vì sao chép mô hình nước ngoài. Dữ liệu nghiên cứu giới hạn ở văn bản pháp luật và nguồn có khả năng kiểm chứng đến tháng 8/2026.

3. Kết quả và thảo luận kết quả nghiên cứu

3.1. Khung pháp lý mới

3.1.1. Pháp luật đã xác lập rõ hơn trách nhiệm của các chủ thể xử lý dữ liệu

Điểm tiến bộ lớn của Luật Bảo vệ dữ liệu cá nhân năm 2025 là đặt trách nhiệm pháp lý vào toàn bộ quá trình xử lý, thay vì chỉ tập trung vào việc dữ liệu có bị tiết lộ hay không. Luật phân định vai trò của bên kiểm soát, bên xử lý và chủ thể có liên quan; xác lập nguyên tắc về mục đích, phạm vi, tính cần thiết, an toàn và trách nhiệm giải trình. Với doanh nghiệp trực tuyến, câu hỏi tuân thủ chuyển từ “có giữ bí mật dữ liệu không?” sang “thu thập dữ liệu nào, vì sao, ai được truy cập, chia sẻ cho ai và lưu giữ đến bao giờ?”.

Quy định này đặc biệt quan trọng đối với thương mại điện tử vì dữ liệu thường đi qua nhiều chủ thể: nền tảng, cổng thanh toán, đơn vị giao nhận, hệ thống CRM, tổng đài, nhà cung cấp đám mây và đối tác quảng cáo. Việc thuê ngoài không làm biến mất trách nhiệm của doanh nghiệp đối với dữ liệu khách hàng. Vì vậy, quản trị dữ liệu phải bao gồm phân vai rõ ràng, giới hạn mục đích, kiểm soát truy cập, nghĩa vụ bảo mật, cơ chế xử lý sự cố và việc xóa hoặc hoàn trả dữ liệu khi hợp đồng kết thúc.

Nghị định số 356/2025/NĐ-CP cụ thể hóa yêu cầu về hồ sơ đánh giá tác động, tổ chức bộ phận hoặc nhân sự bảo vệ dữ liệu và các biện pháp thực thi. Cơ chế chuyển tiếp không phải là sự miễn trừ chung: theo Điều 41 Nghị định, doanh nghiệp nhỏ và khởi nghiệp được lựa chọn thực hiện hoặc không thực hiện Điều 21, Điều 22 và khoản 2 Điều 33 của Luật trong 05 năm kể từ ngày Luật có hiệu lực, trừ trường hợp kinh doanh dịch vụ xử lý dữ liệu, xử lý dữ liệu nhạy cảm hoặc có quy mô từ 100.000 chủ thể dữ liệu trở lên. Hộ kinh doanh và doanh nghiệp siêu nhỏ cũng được miễn 3 nhóm nghĩa vụ nêu trên, trừ các ngoại lệ tương tự.

3.1.2. Thương mại điện tử làm nổi bật tính liên ngành của bảo vệ dữ liệu

Luật Thương mại điện tử năm 2025 có hiệu lực từ ngày 01/07/2026 tạo thêm lớp nghĩa vụ gắn trực tiếp với nền tảng, chủ thể kinh doanh và giao dịch trực tuyến (Quốc hội, 2025). Trong khi Luật Bảo vệ dữ liệu cá nhân cung cấp “luật chơi” chung cho xử lý dữ liệu, pháp luật thương mại điện tử và bảo vệ người tiêu dùng bổ sung yêu cầu về minh bạch giao dịch, trách nhiệm nền tảng, thông tin người bán và cơ chế khiếu nại. Một chính sách bảo vệ dữ liệu chỉ dựa vào một đạo luật đơn lẻ có nguy cơ bỏ sót nghĩa vụ.

Từ góc độ quản trị, doanh nghiệp cần hình thành ma trận tuân thủ liên ngành. Một hoạt động thu thập số điện thoại để gửi khuyến mại có thể đồng thời liên quan đến căn cứ xử lý dữ liệu, quyền phản đối của người tiêu dùng, quy tắc quảng cáo và nghĩa vụ của nền tảng. Nếu mỗi bộ phận chỉ nhìn một văn bản riêng lẻ, doanh nghiệp dễ tạo ra chính sách hợp lệ trên giấy, nhưng không thống nhất với quy trình vận hành thực tế.

3.2. Một số vướng mắc trong thực thi bảo vệ dữ liệu cá nhân trong kinh doanh trực tuyến

3.2.1. Sự đồng ý có nguy cơ hợp pháp về hình thức nhưng không tạo ra quyền kiểm soát thực chất

Trong môi trường số, sự đồng ý dễ trở thành thao tác kỹ thuật hơn là biểu hiện thực chất của quyền tự quyết. Người dùng thường phải chấp nhận một văn bản dài để tiếp tục giao dịch; mục đích cần thiết cho hợp đồng có thể bị gộp với tiếp thị (marketing), phân tích hành vi hoặc chia sẻ cho đối tác. Khi đó, hình thức “đồng ý” vẫn tồn tại nhưng khả năng lựa chọn thực tế của chủ thể dữ liệu bị suy giảm.

Giải pháp không nằm ở việc tăng số lượng hộp kiểm, mà ở thiết kế sự đồng ý có chất lượng: tách mục đích cần thiết và tùy chọn; dùng thông báo nhiều lớp, ngôn ngữ dễ hiểu; cho phép rút lại thuận tiện; và lưu bằng chứng về thời điểm, nội dung, phiên bản thông báo người dùng đã chấp thuận.

3.2.2. *Rủi ro nội bộ và chuỗi nhà cung cấp thường lớn hơn giả định “bị tin tặc (hacker)”*

Bản án số 63/2022/HS-ST ngày 12/12/2022 của Tòa án nhân dân tỉnh Hải Dương là minh họa đáng chú ý về việc dữ liệu khách hàng được tổ chức thành các tệp và đưa vào giao dịch có giá trị. Bản án cho thấy dữ liệu không phải “rác thông tin”; nó có thể trở thành nguồn lợi kinh tế và tạo động cơ chiếm đoạt, sao chép hoặc bán trái phép (Tòa án Nhân dân tỉnh Hải Dương, 2022). Giá trị của vụ án không chỉ nằm ở trách nhiệm của cá nhân bán dữ liệu, mà còn ở câu hỏi hệ thống: tại sao một người có thể truy cập, trích xuất và chuyển dữ liệu ra ngoài với quy mô đáng kể?

Từ góc độ trách nhiệm giải trình, tuyên bố “dữ liệu bị tin tặc lấy” không kết thúc phân tích pháp lý. Cần tiếp tục kiểm tra cơ chế phân quyền, nhật ký truy cập, xác thực đa yếu tố, quản trị tài khoản nghỉ việc, cảnh báo tài xuống bất thường, mã hóa và kiểm thử bảo mật. Nếu các biện pháp cơ bản không được duy trì phù hợp với quy mô và loại dữ liệu xử lý, sự hiện diện của tác nhân tấn công bên ngoài không tự động loại trừ trách nhiệm quản trị.

Bài học cho Việt Nam là nghĩa vụ bảo vệ dữ liệu cần gắn với khả năng dự liệu và phòng ngừa rủi ro. Tiêu chuẩn đối với một nền tảng xử lý hàng triệu hồ sơ và dữ liệu nhạy cảm phải cao hơn một cơ sở kinh doanh nhỏ. Cách tiếp cận dựa trên rủi ro vừa tránh áp đặt đồng loạt, vừa yêu cầu các chủ thể có khả năng gây tác động lớn chứng minh mức kiểm soát tương xứng.

3.2.3. *Tệp cookie (cookie), công nghệ theo dõi (tracking) và lập hồ sơ hành vi là vùng rủi ro pháp lý còn bị đánh giá thấp*

Nhiều doanh nghiệp vẫn mô tả dữ liệu khách hàng chủ yếu bằng họ tên, số điện thoại, thư điện tử và địa chỉ. Trong khi đó, quảng cáo số còn sử dụng tệp cookie, điểm ảnh theo dõi, mã định danh quảng cáo, dấu vết thiết bị và lịch sử truy cập để suy đoán sở thích, khả năng mua hàng hoặc nhóm khách hàng. Khi các tín hiệu này gắn với một cá nhân cụ thể, chúng cần được đưa vào bản đồ xử lý dữ liệu và đánh giá cùng dữ liệu định danh truyền thống.

Kinh nghiệm thực thi của Pháp năm 2025 đặc biệt đáng chú ý. CNIL phạt công ty thuộc SHEIN 150 triệu Euro vì vi phạm quy tắc về tệp cookie, gồm việc đặt công cụ theo dõi khi chưa có sự đồng ý hợp lệ và không thông tin đầy đủ cho người dùng; cùng ngày, CNIL phạt Google 325 triệu Euro liên quan đến quảng cáo trong Gmail và tệp cookie khi tạo tài khoản (Ủy ban Quốc gia về Tin học và Tự do của Pháp, 2025). 2 quyết định cho thấy, bảo vệ dữ liệu không đồng nhất với an ninh mạng: một hệ thống không bị xâm nhập vẫn có thể vi phạm nếu cơ chế thu thập và theo dõi không hợp pháp.

Đối với Việt Nam, tệp cookie, công nghệ theo dõi và SDK của bên thứ ba, cùng mô hình lập hồ sơ, cần được đưa vào kiểm toán pháp lý định kỳ. Doanh nghiệp nên lập danh mục công nghệ theo dõi, phân loại mục đích, xác định bên nhận dữ liệu, thời hạn lưu trữ và cơ chế lựa chọn của người dùng. Chính sách bảo mật chỉ đề cập họ tên, số điện thoại nhưng bỏ qua dữ liệu hành vi sẽ không phản ánh đầy đủ hoạt động xử lý thực tế.

3.2.4. *Dòng dữ liệu xuyên biên giới làm tăng khoảng cách giữa “hợp đồng” và khả năng kiểm soát thực tế*

Kinh doanh trực tuyến thường sử dụng đám mây, hệ thống CRM, công cụ phân tích và quảng cáo đặt tại nhiều quốc gia. Chuyển dữ liệu xuyên biên giới không chỉ là gửi một tệp ra nước ngoài mà có thể phát sinh liên tục qua đồng bộ, sao lưu, hỗ trợ kỹ thuật hoặc truy cập từ xa. Doanh nghiệp cần nhận diện đầy đủ các luồng này để thực hiện nghĩa vụ đánh giá tác động và kiểm soát bên nhận dữ liệu theo pháp luật Việt Nam.

Hợp đồng với nhà cung cấp nước ngoài chỉ bảo vệ thực chất khi đi kèm khả năng giám sát. Doanh nghiệp cần quyền nhận thông tin về nhà thầu phụ, tiêu chuẩn bảo mật, sự cố, vị trí dữ liệu, cơ chế xóa hoặc hoàn trả dữ liệu và việc thay đổi hạ tầng. Chuỗi cung ứng công nghệ càng dài, nghĩa vụ thẩm định và theo dõi nhà cung cấp càng quan trọng.

3.3. *Kinh nghiệm quốc tế*

Các vụ việc quốc tế được lựa chọn cho thấy cơ quan quản lý không chỉ nhìn vào số lượng bản ghi bị lộ

mà còn xem xét cách tổ chức đã quản trị rủi ro trước và sau sự cố. Singapore nhấn mạnh biện pháp bảo vệ hợp lý, kiểm soát truy cập và khắc phục; GDPR đặt trách nhiệm giải trình và bảo vệ dữ liệu ngay từ thiết kế thành nguyên tắc quản trị; Pháp kiểm soát mạnh việc sử dụng tệp cookie (Nghị viện châu Âu và Hội đồng Liên minh châu Âu, 2016; Ủy ban Quốc gia về Tin học và Tự do của Pháp, 2025; Ủy ban Bảo vệ dữ liệu cá nhân Singapore, 2025).

Ngày 11/6/2026, Ủy ban Bảo vệ thông tin cá nhân Hàn Quốc (PIPC) công bố quyết định xử lý Coupang và Công ty Dịch vụ Hoàn thiện đơn hàng Coupang (CFS). Đối với Coupang, PIPC áp dụng tổng mức phạt hành chính 624,681 tỷ won và phạt tiền 16,8 triệu won; đối với CFS, PIPC áp dụng khoản phạt 248 triệu won. PIPC kết luận sự cố của Coupang làm lộ dữ liệu cá nhân của khoảng 37,55 triệu người, đồng thời xác định thêm vi phạm về thu thập dữ liệu hoạt động trực tuyến không có căn cứ pháp lý phù hợp (Ủy ban Bảo vệ thông tin cá nhân Hàn Quốc, 2026). Điều đáng chú ý là hai nhóm trách nhiệm tồn tại song song: bảo vệ hệ thống khỏi truy cập trái phép và bảo đảm tính hợp pháp của chính hoạt động thu thập, sử dụng dữ liệu. Đầu tư mạnh cho an ninh mạng không thể “bù” cho một mô hình khai thác dữ liệu vượt quá căn cứ pháp lý.

Đối với Việt Nam, bài học phù hợp không phải là sao chép mức phạt, mà là xây dựng chuẩn đánh giá dựa trên rủi ro và bằng chứng. Quy mô dữ liệu, tính nhạy cảm, mức độ theo dõi hành vi và khả năng tác động đến số đông cần ảnh hưởng trực tiếp đến yêu cầu về tổ chức, công nghệ, kiểm toán và giám sát nhà cung cấp.

3.4. Kiểm nghị hoàn thiện pháp luật và nâng cao hiệu quả thực thi

Thứ nhất, cụ thể hóa trách nhiệm giải trình theo mô hình quản trị vòng đời dữ liệu. Hướng dẫn thực thi nên xác định bộ bằng chứng tối thiểu có khả năng kiểm tra, gồm bản đồ dữ liệu và mục đích xử lý, căn cứ pháp lý, ma trận quyền truy cập, thời hạn lưu giữ, nhật ký xử lý yêu cầu của chủ thể dữ liệu, hồ sơ đánh giá tác động và kế hoạch ứng phó sự cố. Trọng tâm không phải tăng giấy tờ mà tạo khả năng chứng minh tuân thủ.

Thứ hai, chuẩn hóa nghĩa vụ hợp đồng trong chuỗi xử lý dữ liệu. Cần có hướng dẫn tối thiểu đối với thỏa thuận giữa bên kiểm soát và bên xử lý về chỉ dẫn xử lý, bảo mật, nhà thầu phụ, hỗ trợ quyền của chủ thể dữ liệu, thông báo sự cố, kiểm toán và xóa hoặc hoàn trả dữ liệu. Chuẩn hợp đồng giúp doanh nghiệp nhỏ dễ tuân thủ hơn, hạn chế tình trạng điều khoản “bảo mật thông tin” quá chung chung.

Thứ ba, làm thực chất cơ chế đồng ý và minh bạch. Cần hướng dẫn rõ việc trình bày thông báo nhiều lớp; tách mục đích cần thiết khỏi tiếp thị, phân tích hoặc chia sẻ tùy chọn; không thiết kế giao diện gây áp lực lựa chọn; và bảo đảm rút lại sự đồng ý đơn giản như khi đưa ra. Với hoạt động lập hồ sơ có tác động đáng kể, doanh nghiệp cần giải thích rõ cách thức vận hành, mục tiêu và hệ quả đối với người dùng.

Thứ tư, bổ sung chuẩn quản trị đối với tệp cookie, công nghệ theo dõi, hoạt động lập hồ sơ (profiling) và ứng dụng trí tuệ nhân tạo. Trọng tâm nên là nhận diện công nghệ theo dõi, phân loại mục đích, hạn chế thu thập không cần thiết, đánh giá tác động đối với hoạt động lập hồ sơ có rủi ro và cung cấp lựa chọn thực chất cho người dùng. Những công nghệ không thiết yếu cho giao dịch không nên mặc nhiên được coi là thành phần kỹ thuật trung tính.

Thứ năm, xây dựng cơ chế hỗ trợ tuân thủ theo rủi ro và quy mô. Bên cạnh cơ chế chuyển tiếp cho doanh nghiệp nhỏ và khởi nghiệp, cần phát triển bộ mẫu, danh mục kiểm tra (checklist), tiêu chí phân tầng rủi ro và hướng dẫn thực hành cho hộ kinh doanh, người bán trên mạng xã hội và doanh nghiệp vừa và nhỏ. Hỗ trợ tuân thủ càng rõ thì chi phí pháp lý càng giảm mà không phải hạ thấp chuẩn bảo vệ dữ liệu.

Thứ sáu, tăng hiệu quả ứng phó sự cố theo hướng phối hợp và hậu kiểm dựa trên bằng chứng. Doanh nghiệp cần quy trình thống nhất để phân loại sự cố, cô lập rủi ro, bảo toàn chứng cứ, đánh giá phạm vi ảnh hưởng, thông báo theo quy định và khắc phục nguyên nhân gốc. Cơ quan quản lý nên ưu tiên đánh giá không chỉ thời điểm báo cáo mà cả chất lượng chuẩn bị trước sự cố và mức độ khắc phục sau sự cố.

4. Kết luận

Bảo vệ dữ liệu cá nhân trong kinh doanh trực tuyến không còn là một nghĩa vụ ngoại vi của hoạt động số. Dữ liệu vừa là đầu vào của năng lực cạnh tranh, vừa gắn chặt với quyền riêng tư và an toàn của người tiêu dùng; chính sự kết hợp này khiến quản trị dữ liệu trở thành một vấn đề pháp lý cốt lõi của doanh nghiệp. Khung pháp luật Việt Nam có hiệu lực trong năm 2026 đã tạo bước chuyển quan trọng khi xác lập rõ hơn vai trò của các chủ thể xử lý, trách nhiệm hợp đồng, biện pháp quản lý, kỹ thuật và mối quan hệ với thương mại điện tử.

Tuy nhiên, thách thức lớn nhất nằm ở khoảng cách giữa văn bản và kiến trúc vận hành thực tế. Sự đồng ý có thể chỉ mang tính hình thức; chuỗi nhà cung cấp làm phân tán quyền kiểm soát; tệp cookie và hoạt động lập hồ sơ tạo ra dòng dữ liệu ít được nhìn thấy; và sự cố có thể bắt nguồn từ quản trị nội bộ chứ không chỉ từ tấn công tinh vi. Các vụ việc tại Singapore, Hàn Quốc và Pháp củng cố một thông điệp chung: trách nhiệm pháp lý ngày càng được đánh giá bằng khả năng dự liệu, phòng ngừa, phát hiện và khắc phục.

Vì vậy, hướng hoàn thiện phù hợp cho Việt Nam là chuyển từ “tuân thủ bằng tài liệu” sang “tuân thủ có thể kiểm chứng”: quản trị dữ liệu theo vòng đời, dựa trên rủi ro; hợp đồng hóa trách nhiệm trong toàn chuỗi xử lý; bảo vệ dữ liệu ngay từ thiết kế và theo mặc định; và xây dựng cơ chế hỗ trợ tuân thủ theo quy mô. Khi đó, bảo vệ dữ liệu trở thành hạ tầng của niềm tin số và lợi thế cạnh tranh bền vững ■

TÀI LIỆU THAM KHẢO:

Chính phủ. (2025). Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân.

Nghị viện châu Âu và Hội đồng Liên minh châu Âu (European Parliament and Council). (2016). Quy định (EU) 2016/679 - Quy định chung về bảo vệ dữ liệu (General Data Protection Regulation - GDPR). Công báo Liên minh châu Âu (Official Journal of the European Union), L 119, 1-88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Quốc hội. (2023). Luật số 19/2023/QH15: Luật Bảo vệ quyền lợi người tiêu dùng, ban hành ngày 20/6/2023.

Quốc hội. (2023). Luật số 20/2023/QH15: Luật Giao dịch điện tử, ban hành ngày 22/6/2023.

Quốc hội. (2025). Luật số 91/2025/QH15: Luật Bảo vệ dữ liệu cá nhân, ban hành ngày 26/6/2025.

Quốc hội. (2025). Luật số 116/2025/QH15: Luật An ninh mạng, ban hành ngày 10/12/2025.

Quốc hội. (2025). Luật số 122/2025/QH15: Luật Thương mại điện tử, ban hành ngày 10/12/2025.

Quốc hội. (2025). Luật số 143/2025/QH15: Luật Đầu tư, ban hành ngày 11/12/2025.

Tòa án Nhân dân tỉnh Hải Dương. (2022). Bản án số 63/2022/HS-ST ngày 12/12/2022 về tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông. Công công bố bản án, quyết định của Tòa án nhân dân. <https://congboaban.toaan.gov.vn/3ta1107435t1cvn/>

Ủy ban Bảo vệ dữ liệu cá nhân Singapore (Personal Data Protection Commission - PDPC). (2025). Vi phạm nghĩa vụ bảo vệ của Marina Bay Sands Pte Ltd (Breach of the Protection Obligation by Marina Bay Sands Pte Ltd). <https://www.pdpc.gov.sg/organisations/regulations-decisions/enforcement-decisions/breach-of-the-protection-obligation-by-marina-bay-sands-pte-ltd>

Ủy ban Bảo vệ thông tin cá nhân Hàn Quốc (Personal Information Protection Commission - PIPC). (2026). Thông cáo báo chí về quyết định xử lý Coupang và các công ty liên kết do làm lộ và vi phạm quy định về thông tin cá nhân, ngày 11/6/2026. <https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=12171>

Ủy ban Quốc gia về Tin học và Tự do của Pháp (Commission Nationale de l'Informatique et des Libertés - CNIL). (2025a). Quyết định xử phạt Shein về việc đặt tệp cookie khi chưa có sự đồng ý. <https://www.cnil.fr/en/cookies-placed-without-consent-shein-fined-150-million-euros-cnil>

Ủy ban Quốc gia về Tin học và Tự do của Pháp (Commission Nationale de l'Informatique et des Libertés - CNIL). (2025b). Quyết định xử phạt Google về quảng cáo và tệp cookie trong Gmail. <https://www.cnil.fr/en/cookies-and-advertisements-inserted-between-emails-google-fined-325-million-euros-cnil>