



Original Article

# Consumer Information Tracking in E-Commerce from A Personal Data Protection Perspective: A Comparative Analysis of Vietnamese and Japanese Legal Frameworks

Phan Thi Thanh Thuy\*

*VNU Vietnam Japan University, Hoa Lac, Ha Noi, Vietnam*

Received 18<sup>th</sup> November 2025

Revised 24<sup>th</sup> January 2026; Accepted 20<sup>th</sup> March 2026

**Abstract:** Amid the rapid growth of the digital economy, e-commerce businesses are increasingly tracking consumer information, essentially by processing behavioural data, to enable personalised marketing and improve business performance. This trend raises legal challenges for the protection of personal data in general and consumer information in particular. Although Vietnamese law has established a basic legal framework for personal data protection and consumer protection, it still lacks direct and specific rules to regulate online consumer-tracking practices. This article examines the current legal landscape governing the protection of consumer information in Vietnamese e-commerce, compares it with the legal framework in Japan, and identifies regulatory gaps as well as the legal mechanisms that should be added to ensure that consumers can conduct transactions in a secure and privacy-preserving manner.

**Keywords:** Consumer information, Consumer tracking, Behavioural data, Personal data.

\* Corresponding author.

*E-mail address:* [phanthuy.law@gmail.com](mailto:phanthuy.law@gmail.com)

<https://doi.org/10.25073/2588-1167/vnuls.4826>

# Hành vi theo dõi thông tin người tiêu dùng trong thương mại điện tử từ góc nhìn bảo vệ dữ liệu cá nhân theo pháp luật Việt Nam và Nhật Bản

Phan Thị Thanh Thủy\*

*Trường Đại học Việt-Nhật, Đại học Quốc gia Hà Nội, Khu Đô thị ĐHQGHN,  
Hòa Lạc, Hà Nội, Việt Nam*

Nhận ngày 18 tháng 11 năm 2025

Chỉnh sửa ngày 24 tháng 01 năm 2026; Chấp nhận đăng ngày 20 tháng 3 năm 2026

**Tóm tắt:** Trong xu hướng phát triển mạnh mẽ của kinh tế số, các doanh nghiệp thương mại điện tử đang ngày càng gia tăng việc theo dõi thông tin người tiêu dùng, bản chất là xử lý dữ liệu hành vi, để phục vụ cho mục tiêu tiếp thị cá nhân khách hàng và tối ưu hóa hiệu quả kinh doanh. Bối cảnh này đang đặt ra những thách thức pháp lý đối với quyền bảo mật dữ liệu cá nhân nói chung và thông tin người tiêu dùng nói riêng. Mặc dù pháp luật Việt Nam đã thiết lập được khung pháp luật nền tảng về bảo vệ DLCN và bảo vệ người tiêu dùng, song vẫn thiếu những quy định mang tính trực tiếp và cụ thể để điều chỉnh hành vi theo dõi người tiêu dùng trực tuyến. Bài báo này phân tích thực trạng pháp luật về bảo vệ thông tin người tiêu dùng trong thương mại điện tử ở Việt Nam, đối chiếu với pháp luật Nhật Bản và chỉ ra những khoảng trống và những cơ chế pháp lý cần được bổ sung để bảo đảm cho người tiêu dùng có những giao dịch an toàn, bảo mật.

**Từ khóa:** Thông tin người tiêu dùng, theo dõi thông tin người tiêu dùng, dữ liệu hành vi, dữ liệu cá nhân.

## 1. Mở đầu

Sự bùng nổ của thương mại điện tử (TMĐT) thông qua các sàn giao dịch TMĐT, website bán hàng, ứng dụng mua sắm và trên các mạng xã hội ở các nước cũng như ở Việt Nam đã thúc đẩy các doanh nghiệp theo dõi một cách có hệ thống các thông tin về người tiêu dùng (NTD), bao gồm thông tin cá nhân, lịch sử truy cập internet, tình trạng giỏ hàng, mua, hủy đơn, các đánh giá, bình luận và những thông tin có liên quan khác.

Hành vi thu thập, lưu trữ và khai thác các thông tin nói trên được hiểu là “theo dõi thông tin NTD” (Consumer information tracking). Theo lý giải của các doanh nghiệp TMĐT, việc

theo dõi thông tin nhằm mục đích xác định nhu cầu và thói quen mua sắm của NTD, từ đó đưa ra những chính sách tiếp thị có tính cá nhân hóa cho từng khách hàng và nhằm tối đa lợi ích của hoạt động kinh doanh [1]. Mặc dù các doanh nghiệp lên tiếng biện hộ vì lợi ích của NTD, song do tính nhạy cảm của các dữ liệu cá nhân (DLCN), hoạt động này cũng làm dấy lên sự lo ngại về việc xâm phạm các quy định về bảo mật thông tin NTD, bảo vệ dữ liệu DLCN thông qua những hành vi thu thập và xử lý trái phép

Ở Việt Nam, đang thiếu sự kết nối trực tiếp giữa các quy định bảo vệ thông tin NTD và bảo vệ DLCN trong quy định của pháp luật hiện hành. Luật Bảo vệ quyền lợi người tiêu dùng

\* Tác giả liên hệ.

Địa chỉ email: phanthuy.law@gmail.com

<https://doi.org/10.25073/2588-1167/vnuls.4826>

(BVQLNTD) năm 2023 đã xác định “thông tin người tiêu dùng bao gồm thông tin cá nhân, thông tin về việc mua và sử dụng hàng hóa, dịch vụ, cùng các thông tin khác liên quan đến giao dịch giữa người tiêu dùng với tổ chức, cá nhân kinh doanh” (Khoản 3 Điều 3), đồng thời yêu cầu các tổ chức, cá nhân thực hiện việc thu thập, lưu trữ, sử dụng, chỉnh sửa, cập nhật, hủy bỏ thông tin của NTD phải được sự đồng ý của NTD và tuân thủ pháp luật (Điều 15). Trong khi đó, các văn bản quy pháp luật mới nhất về bảo vệ DLCN là Luật Bảo vệ DLCN năm 2025 (có hiệu lực kể từ 01/01/2026) và 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 DLCN (NĐ 356/2025/NĐ - CP) cũng không đề cập trực tiếp đến hành vi thu thập và xử lý một cách có hệ thống thông tin NTD vì mục đích kinh doanh và cũng không có giải thích trực tiếp rằng thông tin NTD là một loại dữ liệu đặc thù được pháp luật bảo vệ. Cả luật và nghị định chỉ chia DLCN làm hai loại: “dữ liệu cá nhân cơ bản” và “dữ liệu cá nhân nhạy cảm” và đưa ra danh mục cụ thể từng loại DLCN trong Điều 3 và Điều 4 của NĐ 356/ 2025/ NĐ-CP Theo đó, thông tin NTD bao gồm thông tin cá nhân và thông tin về lịch sử giao dịch trên internet thể hiện xu hướng tiêu dùng có thể được nhận diện theo cả hai loại DLCN cơ bản và DLCN nhạy cảm. Tuy nhiên, việc xác định và xử lý hành vi theo dõi trái phép thông tin NTD không dễ dàng. Để làm rõ vi phạm, các cơ quan chức năng phải “đi vòng” bằng cách chứng minh, giải thích rằng theo dõi trái phép thông tin NTD trong TMĐT chính là theo dõi dữ liệu cơ bản cá nhân qua internet. Từ đó mới có cơ sở cho việc điều tra, xử lý hành vi chính hay hình sự tùy theo mức độ vi phạm.

Trong luật pháp Việt Nam hiện hành cũng như trong các nghiên cứu, vấn đề bảo vệ DLCN đang được tiếp cận chủ yếu ở phương diện chung như quyền riêng tư, an ninh thông tin, ít có nghiên cứu đề cập đến “theo dõi thông tin NTD” trong TMĐT như một vấn đề pháp lý nằm ở giao điểm giữa bảo vệ thông tin NTD và bảo vệ DLCN. Điều này cho thấy sự thiếu hụt trong quy định của pháp luật về xử lý trực tiếp và thích đáng đối với hành vi theo dõi trái phép thông tin

NTD để trục lợi trong kinh doanh.

Trong lĩnh vực điều chỉnh pháp lý đối với hành vi theo dõi thông tin NTD, Đạo luật Bảo vệ Thông tin Cá nhân của Nhật Bản (Act on the Protection of Personal Information - APPI) [2] đang cung cấp một đối chiếu đáng chú ý cho pháp luật bảo vệ DLCN của Việt Nam. APPI là đạo luật trung tâm, điều chỉnh hoạt động thu thập và xử lý thông tin cá nhân và có mục tiêu “bảo vệ quyền và lợi ích của cá nhân, đồng thời bảo đảm việc sử dụng hữu ích thông tin cá nhân cho sự phát triển kinh tế - xã hội số” (Article 1). Việc giám sát thực thi luật được thực hiện bởi một cơ quan độc lập trực thuộc chính phủ là Ủy ban Bảo vệ Thông tin Cá nhân (Personal Information Protection Commission - PPC) (Article 59-74). Việc nghiên cứu kinh nghiệm của pháp luật Nhật Bản trong điều chỉnh hành vi theo dõi NTD để tìm ra những gợi ý phù hợp nhằm sửa đổi bổ sung pháp luật Việt Nam là rất cần thiết.

Bài báo này tập trung vào phân tích bản chất pháp lý của hành vi theo dõi thông tin NTD dưới góc độ bảo vệ DLCN và cách thức pháp luật Việt Nam và Nhật bản điều chỉnh hành vi này để so sánh, đối chiếu và tìm ra các cơ chế pháp lý cần bổ sung trong pháp luật hiện hành nhằm bảo vệ dữ liệu cá nhân của NTD khi tham gia các giao dịch TMĐT; từ đó rút ra những đề xuất, kiến nghị nhằm hoàn thiện pháp luật bảo vệ DLCN. Bài viết cũng tập trung vào đánh giá pháp lý đối với hành vi theo dõi NTD trong mô hình B2C của TMĐT nói chung, mà không mở rộng đến các lĩnh vực đặc thù như ngân hàng, bảo hiểm và tài chính.

## 2. Khái quát về hành vi theo dõi thông tin người tiêu dùng trong thương mại điện tử

### 2.1. Khái niệm và đặc điểm của “hành vi theo dõi thông tin người tiêu dùng”

#### - Khái niệm

Trong thông lệ quốc tế, hoạt động thể hiện một cách xác thực và điển hình nhất “hành vi theo dõi thông tin NTD” chính là các quảng cáo được thiết lập dựa trên các dữ liệu hành vi của

NTD trong môi trường trực tuyến - Gọi tắt là “quảng cáo hành vi” (online behavioural advertising - OBA). Theo các nhà nghiên cứu, OBA là việc các doanh nghiệp bán hàng hóa, cung cấp dịch vụ bằng phương thức TMĐT, phối hợp với các doanh nghiệp công nghệ, công ty quảng cáo theo dõi hành vi trực tuyến (truy cập internet) của NTD và sử dụng thông tin thu thập được để tạo ra và hiển thị quảng cáo có tính cá nhân cao, nhắm tới từng NTD cụ thể, nhằm gia tăng tiêu thụ hàng hóa, dịch vụ. Hành vi trực tuyến rất đa dạng, có thể bao gồm dữ liệu duyệt web, lịch sử tìm kiếm, tiêu thụ phương tiện truyền thông như xem video, dữ liệu sử dụng ứng dụng, mua hàng, phản hồi nhấp chuột vào quảng cáo, nội dung giao tiếp trong email hoặc đăng trên các trang mạng xã hội [3]. Ủy ban Bảo vệ quyền riêng tư Canada (OPC) mô tả OBA là việc theo dõi hoạt động của người dùng trên nhiều trang web và các ứng dụng điện tử và theo thời gian, nhằm đưa ra các quảng cáo được “cá nhân hóa” theo sở thích được suy luận bởi bên theo dõi. OPC cũng chỉ ra rằng các nhà quảng cáo dựa trên hành vi thường sử dụng các thuật toán phức tạp để phân tích dữ liệu thu thập được, xây dựng hồ sơ cá nhân chi tiết của người dùng và phân loại họ theo các nhóm dựa trên sở thích [4]. Hiện tại OBA đang là đối tượng điều chỉnh của Luật Quảng cáo hành vi trực tuyến và Luật Bảo vệ thông tin cá nhân và tài liệu điện tử (PIPEDA) nhằm ngăn chặn và xử lý các chủ thể vi phạm các quy định về bảo vệ DLCN của NTD ở Canada.

Trương tự, Ủy ban Thương mại Liên bang Hoa Kỳ (FTC), giải thích rằng OBA là quảng cáo được xây dựng dựa trên hành vi theo dõi hoạt động trực tuyến của người tiêu dùng trong một khoảng thời gian để đưa ra những quảng cáo nhắm vào sở thích cá nhân của người đó [5].

Từ những nhận định này, có thể đưa ra khái niệm sau: “Hành vi theo dõi thông tin NTD trong TMĐT là việc thương nhân TMĐT cùng các chủ thể có liên quan, thu thập, ghi nhận và phân tích có hệ thống các dữ liệu phát sinh từ hành vi tiêu dùng trực tuyến của người tiêu dùng (truy cập, tìm kiếm, xem sản phẩm, hủy, đặt hàng, thanh toán, đánh giá, bình luận...) trong một khoảng

thời gian nhất định, nhằm phục vụ các mục đích như cá nhân hóa trải nghiệm, gợi ý sản phẩm, quảng cáo nhắm đích, hoặc các quyết định kinh doanh khác”.

- Đặc điểm của hành vi theo dõi theo dõi thông tin NTD

TMĐT là môi trường thuận lợi nhất để các doanh nghiệp triển khai các chiến lược kinh doanh dựa trên các dữ liệu (data-driven business). Tại đó, doanh nghiệp không chỉ phân tích dữ liệu lịch sử NTD để đưa ra quảng cáo tiếp thị mang tính cá nhân, mà còn kết hợp phân tích dự báo và khuyến nghị, sử dụng thuật toán để dự đoán hành vi mua sắm, nhu cầu tồn kho, giá tối ưu và phản ứng của NTD đối với các chiến dịch marketing [6]. Theo D’Annunzio và các cộng sự, nhìn chung, các hành vi theo dõi trực tuyến đều chứa đựng những đặc điểm cốt lõi sau đây [1]:

1) Theo dõi các dữ liệu đa dạng: dữ liệu hành vi được thu thập ở nhiều hoạt động khác nhau của NTD. Chẳng hạn: lịch sử tìm kiếm sản phẩm, giỏ hàng, đơn hủy, đơn đã mua, phương thức thanh toán, các đánh giá, bình luận, tương tác với nội dung tiếp thị.

2) Theo dõi liên tục và dài hạn: Hành vi theo dõi không diễn ra một lần, mà kéo dài theo thời gian, bất cứ khi nào NTD có tương tác trực tuyến. Nó cho phép doanh nghiệp xây dựng một “đòng đời tiêu dùng” (customer journey) khá chi tiết của từng người hoặc từng phân khúc.

3) Theo dõi để liên kết và hợp nhất dữ liệu: dữ liệu hành vi của một khách hàng được liên kết từ nhiều nguồn khác nhau như website TMĐT, ứng dụng di động, email, hoặc thậm chí từ nền tảng mạng xã hội (social commerce), từ đó tạo ra hồ sơ tiêu dùng đa kênh.

4) Theo dõi một cách “vô hình”: Các hoạt động theo dõi diễn ra ở tầng kỹ thuật như ghi log, đặt mã theo dõi... nên NTD ít có khả năng nhận biết; nhất là khi thông tin về việc bị theo dõi được “ẩn” trong các điều khoản sử dụng dịch vụ (Terms of Service) khó hiểu, mang tính kỹ thuật cao.

Theo dõi có mục đích lợi ích: Việc theo dõi nhằm mục đích thương mại; các dữ liệu thu thập được dùng để xây dựng hồ sơ, từ đó nhắm

chọn quảng cáo hoặc nội dung phù hợp với sự quan tâm của NTD. Chẳng hạn, ở Việt Nam, các nền tảng TMĐT như Shopee, Tiki... luôn gợi ý cho khách hàng các sản phẩm tương tự với những mức giá khác nhau để lựa chọn.

## 2.2. Mối liên kết giữa hành vi theo dõi người tiêu dùng và bảo vệ dữ liệu cá nhân

Trong pháp luật của nhiều quốc gia hiện nay, dữ liệu về hành vi NTD (Consumer behaviour) trên môi trường số như lịch sử truy cập, tìm kiếm, mua sắm, phản hồi được coi là một dạng DLCN và được điều chỉnh chủ yếu bằng pháp luật bảo vệ DLCN, bên cạnh pháp luật bảo vệ NTD.

Ở Liên minh châu Âu (EU), trong Quy định chung về bảo vệ dữ liệu - General Data Protection Regulation (GDPR) coi việc thu thập, ghi chép, tổ chức, phân tích, sử dụng, trao đổi,... DLCN, bao gồm thông tin NTD, là các hoạt động “xử lý” (processing) và phải tuân thủ một số nguyên tắc cơ bản bao gồm: Giới hạn mục đích (purpose limitation): Dữ liệu chỉ được thu thập cho mục đích rõ ràng, hợp pháp và không được dùng cho mục đích khác nếu không chứng minh được cơ sở pháp lý; Giảm thiểu dữ liệu (data minimisation): Chỉ thu thập những gì “phù hợp, có liên quan và cần thiết”, Minh bạch: Cá nhân phải được thông tin về việc dữ liệu của mình được thu thập và sử dụng như thế nào và An toàn và trách nhiệm giải trình: Bên xử lý phải áp dụng biện pháp bảo mật phù hợp và chịu trách nhiệm chứng minh sự tuân thủ [7]. Từ đó, Cơ quan Bảo vệ Dữ liệu của EU (EDPB) - trực thuộc Ủy ban châu Âu, đã có hướng dẫn và giải thích về “lập hồ sơ” khách hàng (Profiling) là mọi hình thức xử lý dữ liệu cá nhân để đánh giá hoặc dự đoán các khía cạnh về hành vi, sở thích, địa điểm,... của một cá nhân [8]. Quy định này cho phép các cơ quan pháp luật có căn cứ để kết luận rằng theo dõi hành vi thường là bước đầu của quá trình lập hồ sơ thông tin NTD và xử lý đối với những vi phạm ngay từ đầu [9].

Tại Hoa Kỳ, không có một đạo luật cấp liên bang về bảo vệ DLCN thống nhất; mối liên hệ giữa hành vi NTD và DLCN được hình thành

thông qua một mạng lưới quy định về bảo vệ NTD và quyền riêng tư. Ủy ban Thương mại Liên bang (FTC) sử dụng thẩm quyền theo Điều 5 Đạo luật FTC để xử lý các thực tiễn thu thập, theo dõi và chia sẻ dữ liệu người tiêu dùng bị coi là “không công bằng hoặc lừa dối”, trong đó có việc theo dõi trực tuyến và quảng cáo cá nhân hóa trái với cam kết trong chính sách riêng tư của doanh nghiệp [10]. Ở cấp bang, Đạo luật Quyền riêng tư Người tiêu dùng California (CCPA) là ví dụ tiêu biểu cho việc gắn trực tiếp hành vi NTD với khái niệm “thông tin cá nhân”. Theo đó, “Thông tin cá nhân” được giải thích rất rộng, bao gồm cả lịch sử duyệt web, lịch sử mua sắm, tương tác trên internet của NTD. Luật trao cho NTD quyền từ chối (opt-out) khỏi việc “bán” hoặc “chia sẻ” thông tin cá nhân cho mục đích OBA [11].

Từ góc độ so sánh, có thể thấy pháp luật EU và Hoa Kỳ đều có điểm chung là: dữ liệu về hành vi NTD được coi là “dữ liệu cá nhân” và có giá trị kinh tế, được phép sử dụng ở mức độ nhất định để trao đổi trong các giao dịch số, song có những quy tắc nghiêm ngặt để bảo vệ quyền riêng tư, quyền tự chủ và an ninh của NTD. Cùng xu hướng, hầu hết các nước có hoạt động TMĐT phát triển đang dần thiết lập mối liên hệ chặt chẽ giữa bảo vệ DLCN và bảo vệ NTD, coi việc theo dõi hành vi tiêu dùng là một hình thức xử lý DLCN cần được đặt dưới các nguyên tắc minh bạch, đồng ý hay thỏa thuận công bằng và quyền kiểm soát của cá nhân. Nói cách khác, việc kết nối chặt chẽ pháp luật về bảo vệ DLCN và pháp luật bảo vệ NTD sẽ giúp thực thi hiệu quả quyền được bảo vệ thông tin cá nhân, chống lại hành vi thu thập, xử lý trái phép thông tin NTD ở các nước cũng như ở Việt Nam.

## 3. Hành vi theo dõi thông tin người tiêu dùng trong pháp luật Việt Nam

### 3.1. Khung pháp luật có liên quan

Ở Việt Nam, hành vi theo dõi thông tin NTD trong TMĐT tuy chưa được đề cập trực tiếp trong các văn bản quy phạm pháp luật hiện hành,

nhưng đã được “ngụ ý” trong các quy định pháp luật về bảo vệ thông tin NTD, bảo vệ DLCN và quản lý TMĐT.

Luật BVQLNTD năm 2023 quy định thông tin NTD bao gồm thông tin cá nhân, thông tin về mua và sử dụng hàng hóa, dịch vụ và các thông tin khác liên quan đến giao dịch giữa NTD với tổ chức, cá nhân kinh doanh - Quy định này có thể hiểu là nhóm dữ liệu được tạo ra khi NTD tham gia TMĐT. Luật cũng thiết lập quyền được bảo mật thông tin của NTD (Khoản 1 Điều 4) và cấm tổ chức, cá nhân kinh doanh tiết lộ, cung cấp thông tin NTD cho bên thứ ba nếu không có sự đồng ý (Điều 18). Trước đó, Nghị định 52/2013/NĐ-CP về thương mại điện tử đã có quy định nghĩa vụ của chủ sở hữu website TMĐT, sàn TMĐT, trong đó có yêu cầu bảo mật thông tin khách hàng, xây dựng chính sách bảo mật, chỉ sử dụng thông tin NTD đúng mục đích đã công bố và không được cung cấp cho bên thứ ba nếu không được đồng ý (Điều 69, 70, 71 và 72). Nghị định 85/2021/NĐ-CP sửa đổi, bổ sung một số điều của Nghị định 52, làm rõ hơn trách nhiệm của sàn TMĐT đối với thông tin hàng hóa, thông tin người bán và cơ chế giám sát (Điều 16 NĐ 85/2021/NĐ-CP), nhưng vẫn chưa có quy định riêng về theo dõi và khai thác dữ liệu hành vi của NTD.

Luật Bảo vệ DLCN năm 2025 khẳng định bảo vệ DLCN là một quyền cơ bản và thiết lập hệ thống nguyên tắc, quyền và nghĩa vụ mang tính ổn định hơn. Theo Khoản 6 Điều 2, mọi hành vi thu thập, ghi, lưu trữ, sửa đổi, sử dụng, tiết lộ, xóa, hủy DLCN đều là “xử lý dữ liệu cá nhân” (Khoản 7, Điều 2). Luật liệt kê 07 nhóm hành vi bị nghiêm cấm liên quan đến DLCN (xử lý trái phép, mua bán trái phép, tiết lộ dữ liệu... (Điều 7); Cá nhân chủ thể dữ liệu có quyền được thông tin, quyền đồng ý, quyền rút lại đồng ý, quyền phản đối xử lý cho mục đích tiếp thị trực tiếp (Điều 9, 10 và 11). Các quy định này chính là nền tảng pháp lý trực tiếp buộc các doanh nghiệp phải tuân thủ các quy định về theo dõi và dùng dữ liệu hành vi cho mục đích quảng cáo, gởi ý sản phẩm (Điều 24 đến Điều 30). Nghị định 356/2025/NĐ-CP hướng dẫn thi hành Luật bảo vệ DLCN 2025 đã thiết lập tương đối đầy đủ các

đặt ra nguyên tắc, quy trình và cách thức xử lý DLCN, quyền của chủ thể dữ liệu và trách nhiệm của bên kiểm soát, bên xử lý dữ liệu (Điều 5, 6 và 7 của NĐ 356/2025/NĐ-CP) Như vậy, căn cứ vào các quy định của pháp luật hiện hành, việc thương nhân kinh doanh TMĐT và các chủ thể có liên quan ghi nhận lịch sử truy cập, lịch sử mua hàng, hành vi tìm kiếm, đánh giá... của NTD hoàn toàn có thể coi là một chuỗi hoạt động xử lý DLCN của NTD.

Trong các luật có liên quan khác, yêu cầu bảo vệ DLCN chỉ được đề cập đến một cách khái quát và nguyên tắc. Chẳng hạn, Luật An ninh mạng 2018 yêu cầu doanh nghiệp cung cấp dịch vụ trên không gian mạng phải thực hiện biện pháp bảo vệ thông tin cá nhân, bí mật kinh doanh của người dùng và có trách nhiệm phối hợp với cơ quan chức năng khi có hành vi xâm phạm an ninh mạng, lộ lọt dữ liệu (Điều 26 và Điều 41). Luật Giao dịch điện tử 2023 điều chỉnh mọi giao dịch thực hiện bằng phương tiện điện tử, tạo khuôn khổ pháp lý tổng quát cho giao dịch trực tuyến, tuy không đi sâu vào DLCN nhưng khẳng định giá trị pháp lý của dữ liệu, chứng từ điện tử và nghiêm cấm việc lợi dụng giao dịch điện tử xâm phạm đến lợi ích quốc gia, dân tộc, an ninh quốc gia, trật tự, an toàn xã hội, lợi ích công cộng, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân (Khoản 1 và 3 Điều 6). Gần đây nhất, Luật TMĐT năm 2025 (có hiệu lực từ 01/7/2026) chủ yếu tập trung vào quản lý nhà nước đối với TMĐT và trách nhiệm của các chủ thể tham gia TMĐT, trong đó có trách nhiệm bảo mật, mà không tập trung vào các quy định cụ thể về bảo vệ thông tin NTD trong giao dịch TMĐT.

Về tổng thể, có thể nói Việt Nam đã hình thành một khung pháp luật đa tầng bao gồm các luật, các nghị định và các văn bản hướng dẫn, tác động trực tiếp hoặc gián tiếp tới việc theo dõi thông tin NTD trong TMĐT, song vẫn cần có sự kết nối trực tiếp và chặt chẽ giữa bảo vệ thông tin NTD và DLCN của NTD.

### 3.2. Cách thức pháp luật điều chỉnh hành vi theo dõi trong thương mại điện tử

Mặc dù không dùng thuật ngữ “theo dõi

thông tin NTD” hay “dữ liệu hành vi”, các quy định pháp luật hiện hành đã điều chỉnh khá rõ các bước cốt lõi của hành vi này, thông qua các chế định về thu thập - sử dụng - chia sẻ dữ liệu cá nhân trong môi trường TMĐT.

3.2.1. Yêu cầu công bố mục đích và có sự đồng ý khi thu thập và sử dụng dữ liệu hành vi

Luật Bảo vệ DLCN 2025 và NĐ 356/2025/NĐ-CP đều yêu cầu việc xử lý DLCN phải có mục đích cụ thể, hợp pháp và thông báo trước cho chủ thể dữ liệu; đồng thời giới hạn việc sử dụng dữ liệu cho mục đích khác nếu không có cơ sở pháp lý bổ sung. Điều này có nghĩa là: khi sản, ứng dụng TMĐT theo dõi lịch sử xem sản phẩm, giỏ hàng, thời gian truy cập, đánh giá... để phục vụ quảng cáo nhắm đích, phân tích hành vi, thì mục đích này phải được công bố rõ trong chính sách bảo mật hoặc điều khoản sử dụng; đồng thời doanh nghiệp phải có căn cứ đồng ý hoặc căn cứ pháp lý khác để xử lý [12].

Tương tự, từ góc nhìn bảo vệ NTD, Luật Bảo vệ NTD 2023 quy định tổ chức, cá nhân kinh doanh chỉ được thu thập, sử dụng thông tin người tiêu dùng khi được sự đồng ý và phải thông báo rõ mục đích; không được sử dụng trái với mục đích đã thông báo, không được cung cấp cho bên thứ ba nếu không có sự đồng ý, trừ trường hợp pháp luật quy định (Khoản 3 Điều 18). Như vậy, hành vi “theo dõi” NTD trong TMĐT về bản chất chính là việc thu thập và sử dụng dữ liệu hành vi cá nhân. Pháp luật hiện hành điều chỉnh hành vi này thông qua yêu cầu về mục đích, đồng ý và minh bạch.

3.3.2. Chính sách bảo mật và nghĩa vụ thông tin với người tiêu dùng

Luật Bảo vệ DLCN 2025 và NĐ 356/2025/NĐ-CP yêu cầu thương nhân, tổ chức sở hữu website TMĐT, sàn TMĐT phải xây dựng cơ chế bảo vệ thông tin cá nhân của NTD, bao gồm: công bố công khai chính sách bảo mật, phạm vi và mục đích sử dụng thông tin, thời gian lưu trữ, chủ thể được tiếp cận thông tin, biện pháp bảo mật,... và có cơ chế để NTD kiểm tra, cập nhật, điều chỉnh thông tin của mình. Luật Bảo vệ QLNTD 2023 cũng quy định trong các giao dịch từ xa, giao dịch trên nền tảng số, bên

kinh doanh phải cung cấp thông tin đầy đủ, dễ hiểu về cách thức thu thập, lưu trữ, sử dụng thông tin NTD. Những trường hợp vi phạm có thể bị xử lý theo pháp luật về bảo vệ NTD và pháp luật xử phạt vi phạm hành chính. Mặc dù đã có quy định cụ thể, trên thực tế, nhiều nghiên cứu, khảo sát đã chỉ ra rằng chính sách bảo mật của nhiều sàn TMĐT vẫn được diễn đạt nặng về kỹ thuật và khó hiểu đối với đa số NTD, khiến cơ chế “thông tin đầy đủ” và “đồng ý thực chất” khó được thực thi [13].

3.2.3. Quyền của người tiêu dùng - chủ thể dữ liệu đối với dữ liệu hành vi

Theo NĐ 13/2023 và Luật BVDLCN 2025, chủ thể dữ liệu có các quyền cơ bản: quyền được thông tin, quyền truy cập, quyền yêu cầu sửa, xóa dữ liệu, quyền hạn chế hoặc phản đối xử lý dữ liệu cho một số mục đích nhất định, trong đó có mục đích tiếp thị trực tiếp. Luật BVQLNTD 2023 cũng đã công nhận quyền của NTD trong bảo vệ DLCN thông qua những quy định về nghĩa vụ của doanh nghiệp, cá nhân kinh doanh trong thu thập, xử lý và sử dụng thông tin NTD (Điều 15, 16, 17 và 18).

Trên lý thuyết, nếu áp dụng đầy đủ các nghĩa vụ của doanh nghiệp, cá nhân kinh NTD có quyền yêu cầu doanh nghiệp TMĐT ngừng dùng dữ liệu hành vi của mình cho quảng cáo hành vi, gợi ý sản phẩm hoặc chuyển cho bên thứ ba. Tuy nhiên, nhiều nghiên cứu thực tiễn cho thấy NTD ở Việt Nam chưa có thói quen và khả năng thực sự để sử dụng các quyền này; một phần do thiếu thông tin, một phần do doanh nghiệp thiết kế giao diện và quy trình thực hiện không thân thiện, khó hiểu và khó áp dụng [14].

3.2.4. Nghĩa vụ đánh giá tác động xử lý dữ liệu và bảo đảm an ninh mạng của doanh nghiệp

NĐ 356/2025/NĐ-CP yêu cầu các bên kiểm soát dữ liệu phải lập hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, đặc biệt khi xử lý dữ liệu với quy mô lớn, đối tượng nhạy cảm hoặc rủi ro cao, và gửi cho cơ quan chuyên trách bảo vệ DLCN (Điều 5, 6, 7 và 8). Luật An ninh mạng 2018 đặt ra nghĩa vụ bảo đảm an toàn thông tin cá nhân trên không gian mạng, phòng ngừa, ngăn chặn hành vi lộ, lọt, mua bán trái phép dữ liệu cá nhân,

trong đó có dữ liệu của khách hàng trên sàn TMĐT (Điều 16, 17).

Luật bảo vệ DLCN 2025 đặt ra yêu cầu về lập hồ sơ đánh giá tác động xử lý DLCN và cập nhật hồ sơ (Điều 21 và 22). Chiếu theo quy định của luật và cụ thể hóa tại Điều 9 của NĐ 356/2025/NĐ-CP, hoạt động theo dõi và phân tích dữ liệu hành vi NTD của các sàn TMĐT lớn, đặc biệt là sàn TMĐT xuyên biên giới, đều thuộc diện phải đánh giá tác động xử lý dữ liệu do tính “quy mô lớn” và “rủi ro cao” đối với quyền bảo mật DLCN. Tuy nhiên, cho đến nay, có rất ít công bố chính thức về tình trạng các doanh nghiệp TMĐT ở Việt Nam thực hiện nghĩa vụ đánh giá tác động xử lý dữ liệu [15].

### 3.3. Khoảng trống pháp lý trong điều chỉnh hành vi theo dõi người tiêu dùng

Tính đến đầu năm 2026, Việt Nam đã có khung pháp luật quy định tương đối đầy đủ ở cấp độ nguyên tắc và bước đầu tiếp cận các chuẩn mực quốc tế liên quan đến điều chỉnh hành vi theo dõi thông tin NTD, bao gồm Luật Bảo vệ DLCN 2025, NĐ 356/2025/NĐ-CP, Luật BVQLNTD 2023, Luật Giao dịch điện tử 2025, các nghị định về TMĐT,... Tuy nhiên, vẫn còn nhiều khoảng trống làm hạn chế hiệu quả tác động của pháp luật đến hành vi theo dõi thông tin NTD.

Thứ nhất, pháp luật không cung cấp khái niệm và không có các quy định trực tiếp về “dữ liệu hành vi” hoặc các giải thích về “theo dõi”, “lập hồ sơ”, “quảng cáo hành vi” như một dạng xử lý thông tin cá nhân có tính rủi ro cao và đặc thù, cần cơ chế bảo vệ đặc biệt. Do đó, hành vi “theo dõi thông tin NTD”, mặc dù rất phổ biến trong TMĐT, vẫn chưa được nhận diện rõ ràng và cụ thể. Vẫn còn thiếu sự liên kết và giải thích thống nhất và rõ ràng giữa khái niệm “thông tin NTD” và “dữ liệu cá nhân” cũng như mức độ bảo vệ DLCN của NTD mua sắm trực tuyến. Hệ quả là hành vi theo dõi thông tin NTD chỉ được điều chỉnh gián tiếp thông qua các quy định chung về DLCN; cũng chưa có tiêu chuẩn riêng để đánh giá về “giới hạn chấp nhận được” của việc theo dõi này [16].

Thứ hai, vấn đề “đồng ý thực chất” của chủ thể DLCN và mức độ “minh bạch” của chủ thể theo dõi trong TMĐT còn là điểm hạn chế lớn. Nhiều doanh nghiệp thường gộp nhiều mục đích xử lý như cung cấp dịch vụ, lưu trữ lịch sử, quảng cáo, chia sẻ với đối tác,... vào cùng một điều khoản chấp nhận, thể hiện bằng một nút “đồng ý” hoặc “chấp nhận” duy nhất. Mặc dù cả Luật BVQLNTD 2025 và Luật BVQLNTD 2023 đều quy định rằng chủ DLCN, có quyền từ chối việc cho doanh nghiệp dùng dữ liệu hành vi cho quảng cáo, gợi ý sản phẩm hoặc chia sẻ với bên thứ ba, song hầu như các doanh nghiệp không cung cấp cơ chế riêng cho NTD thực hiện quyền này; cùng một thực tế là NTD hầu như không đọc hoặc không hiểu được đầy đủ các điều khoản về bảo mật. Vụ việc Zalo ra yêu cầu người dùng hoặc phải đồng ý cho doanh nghiệp này theo dõi thông tin và chuyển dữ liệu cho bên thứ ba hoặc phải chấm dứt việc sử dụng dịch vụ, xảy ra vào cuối tháng 12/2025, là một minh chứng điển hình cho hành vi xâm phạm nghiêm trọng quyền được bảo mật DLCN của NTD. Theo quyết định xử phạt của Ủy ban Cảnh tranh Quốc gia, VNG, công ty chủ sở hữu của Zalo, có những vi phạm nghiêm trọng pháp luật bảo vệ DLCN, gồm không cho người dùng lựa chọn phạm vi cung cấp thông tin, không cho từ chối sử dụng dữ liệu cho quảng cáo, và đưa điều khoản không hợp lệ vào điều kiện giao dịch chung [17]. Có thể thấy rằng, “đồng ý hình thức” là có, nhưng “đồng ý thực chất” vẫn là thách thức; đặc biệt trong bối cảnh hành vi theo dõi, xử lý thông tin NTD được doanh nghiệp sắp đặt để “tước đoạt” quyền tự chủ của NTD một cách chủ ý (như trường hợp Zalo) hoặc mang tính kỹ thuật cao làm cho NTD khó quan sát, nhận biết.

Thứ ba, việc giám sát thực thi pháp luật vẫn là khâu yếu. Theo Luật BVQLNTD và NĐ 356/2025/NĐ-CP, mô hình giám sát phối hợp được thực hiện bởi cơ quan chuyên trách là các đơn vị thuộc Bộ Công an và Bộ Thông tin và Truyền thông như đã từng quy định trong Nghị định số 13/2023/NĐ-CP về bảo vệ DLCN (đã hết hiệu lực và bị thay thế bởi NĐ 356/2025/NĐ-CP). Mặc dù DLCN được hai cơ quan chuyên trách thuộc hai bộ khác nhau phối hợp bảo vệ,

song các nghiên cứu về thực trạng bảo vệ NTD trong TMĐT gần đây cho thấy tình trạng lộ, lọt dữ liệu, bán dữ liệu khách hàng, gọi điện, nhắn tin, quảng cáo nhắm đích vẫn tràn lan vẫn diễn ra. Thực trạng này cho thấy khoảng cách lớn giữa quy định và thực thi [13].

#### **4. Hành vi theo dõi thông tin người tiêu dùng trong pháp luật Nhật Bản**

##### *4.1. Khung pháp luật về bảo vệ dữ liệu cá nhân tại Nhật Bản*

Ở Nhật Bản, Đạo luật về bảo vệ thông tin cá nhân (Act on the Protection of Personal Information - APPI) ban hành năm 2003 là đạo luật trung tâm, điều chỉnh hầu như mọi vấn đề về DLCN khu vực tư, trong đó có TMĐT. APPI đã được sửa đổi nhiều lần để cập nhật các ảnh hưởng của công nghệ số đối với thông tin cá nhân. Trong lần sửa đổi gần nhất năm 2021 (có hiệu lực 01/4/2022) [2], APPI có mục tiêu tiệm cận các chuẩn mực của EU để đạt “quyết định tương đương” (adequacy) về hiệu lực với GDPR trong khuôn khổ hợp tác giữa EU và Nhật Bản về bảo vệ thông tin cá nhân [18]. Việc thực thi APPI được giám sát bởi Ủy ban Bảo vệ Thông tin Cá nhân (PPC) - một cơ quan trung ương độc lập, có thẩm quyền ban hành hướng dẫn, thanh tra, ra lệnh khắc phục và xử phạt hành chính [19].

Về phạm vi áp dụng, APPI có hiệu lực cả bên ngoài lãnh thổ: các doanh nghiệp nước ngoài vẫn phải tuân thủ APPI nếu xử lý DLCN của cá nhân cư trú tại Nhật Bản liên quan đến việc cung cấp hàng hóa, dịch vụ (ví dụ nền tảng TMĐT xuyên biên giới phục vụ khách hàng Nhật Bản). APPI thể hiện hai mục tiêu chính: i) Bảo vệ thông tin cá nhân và bảo vệ quyền cá nhân và phục vụ mục tiêu phát triển kinh tế - xã hội số; ii) Nâng chuẩn hiệu lực pháp lý của APPI để hiệu lực tương đương với GDPR của EU [20]. Trong bối cảnh TMĐT phát triển, APPI được coi là nền tảng pháp luật chính để điều chỉnh việc thu thập, phân tích và chia sẻ dữ liệu hành vi của NTD ở Nhật Bản. Các đạo luật khác về viễn thông, an ninh, các quy định chuyên ngành và hướng dẫn của các

hiệp hội ngành nghề (như Hiệp hội Quảng cáo Tương tác Nhật Bản - JIAA) đóng vai trò bổ trợ.

##### *4.2. Cách thức APPI điều chỉnh hành vi theo dõi thông tin người tiêu dùng*

Nghiên cứu về APPI có thể thấy điểm mấu chốt giúp đạo luật này liên kết chặt chẽ giữa thông tin cá nhân và hành vi theo dõi thông tin NTD với DLCN chính là cách định nghĩa, giải thích và phân loại dữ liệu.

4.2.1. Sự kết nối giữa “thông tin cá nhân” với “thông tin liên quan tới cá nhân”.

Theo APPI, “Thông tin cá nhân” (personal information) là thông tin của một cá nhân còn sống, có thể nhận diện người đó (họ tên, địa chỉ, số điện thoại, ID thành viên, địa chỉ email gắn với cá nhân,...); còn “Dữ liệu cá nhân” (personal data): là thông tin cá nhân được lưu trữ trong cơ sở dữ liệu số, có thể tìm kiếm. APPI sửa đổi năm 2020 đã bổ sung một khái niệm có tính liên kết chặt chẽ và tính viện dẫn cao là “Thông tin liên quan tới cá nhân” (Personally Referable Information - PRI) để chỉ những thông tin vốn có liên quan đến một cá nhân, nhưng sau khi được xử lý thì không còn là “thông tin của một cá nhân cụ thể”. Chẳng hạn những thông tin về lịch sử duyệt web, sử dụng dịch vụ, mã cookie, ID thiết bị,... [2]. Khái niệm PRI được đưa vào chính là để buộc các dịch vụ sử dụng dữ liệu hành vi có được từ theo dõi thông tin NTD phải chịu sự điều chỉnh của APPI [21].

Như vậy, về mặt lý luận, hoạt động theo dõi hành vi NTD trên nền tảng TMĐT đều nằm trong phạm vi điều chỉnh của APPI: hoặc với tư cách “thông tin cá nhân” hoặc “thông tin liên quan tới cá nhân”. Bên cạnh APPI, Luật Viễn thông sửa đổi năm 2023 cũng đưa ra quy định về chuyển giao thông tin người dùng cho bên thứ ba, áp dụng cho các nền tảng trực tuyến lớn (mạng xã hội, dịch vụ nội dung, công cụ tìm kiếm,...), trong đó có yêu cầu cao hơn về minh bạch và trong nhiều trường hợp phải có sự đồng ý trước khi chia sẻ dữ liệu theo dõi.

Dưới tác động của APPI, Hiệp hội Quảng cáo Tương tác Nhật Bản (JIAA) đã ban hành Bộ

hướng dẫn về quảng cáo hành vi trực tuyến (OBA), yêu cầu doanh nghiệp: (1) Thông báo rõ ràng cho người dùng rằng dữ liệu duyệt web, tương tác trực tuyến đang được dùng để gắn quảng cáo; (2) Cung cấp cơ chế từ chối rõ ràng để người dùng dễ sử dụng. Trong thực tiễn, các nền tảng TMĐT bán lẻ Nhật Bản (Rakuten, Amazon Japan, các chuỗi bán lẻ có kênh online như Nitori, Aeon,...) đều công bố chính sách bảo vệ thông tin cá nhân trên cơ sở viện dẫn APPI, trong đó có nội dung về thu thập lịch sử mua hàng, lịch sử xem sản phẩm,... để gợi ý sản phẩm và quảng cáo, đồng thời cam kết tuân thủ quy định về cung cấp thông tin cho bên thứ ba [22].

#### 4.2.2. Quyền của người tiêu dùng Nhật Bản khi bị theo dõi hành vi trực tuyến

APPI quy định một loạt quyền của cá nhân có liên quan trực tiếp tới hành vi theo dõi NTD bao gồm: Quyền yêu cầu sàn TMĐT giải thích việc sử dụng dữ liệu lịch sử mua hàng, lịch sử tra cứu của họ cho mục đích quảng cáo, gợi ý sản phẩm (Article 33); Quyền yêu cầu ngừng cung cấp dữ liệu hành vi cho bên thứ ba như công ty quảng cáo, nền tảng phân tích dữ liệu (Article 34); Quyền gửi khiếu nại lên PPC nếu doanh nghiệp tiếp tục sử dụng dữ liệu bất chấp yêu cầu (Article 35) [2]. Tuy nhiên, việc chưa có chế định “đặt tên thẳng” các hành vi như theo dõi hành vi, lập hồ sơ, quảng cáo hành vi... cũng để lại một số vùng xám, nhất là trong các mô hình phân tích dữ liệu nâng cao.

Tóm lại, nhìn từ góc độ bảo vệ DLCN, pháp luật Nhật Bản đã bước khá xa trong việc nhận diện và xử lý hành vi theo dõi thông tin NTD, gắn chúng với chế độ bảo vệ DLCN thông qua chế định “thông tin cá nhân” và “thông tin liên quan tới cá nhân” và thiết lập cơ chế đồng ý và quyền yêu cầu ngừng cung cấp cho bên thứ ba.

### 5. Một số gợi ý về điều chỉnh pháp luật đối với hành vi theo dõi thông tin người tiêu dùng ở Việt Nam

Từ sự thành công của đạo luật APPI 2020 của Nhật Bản, các nhà lập pháp Việt Nam có thể

tham khảo được một số kinh nghiệm hữu ích trong việc xác lập những quy định điều chỉnh hành vi theo dõi NTD trong TMĐT, đó là:

Thứ nhất, Luật BVDLCN 2025 cần bổ sung những giải thích mang tính kết nối, hỗ trợ giữa khái niệm “thông tin cá nhân” và “dữ liệu cá nhân”. Mặc dù có nội hàm gần gũi, nhưng các khái niệm này đang nằm tách biệt trong hai riêng là Luật BVNTD 2023 và Luật BVDLCN 2025 và đang tạo ra một “con đường vòng” - Khi xử lý hành vi theo dõi trái phép thông tin NTD, cơ quan chức năng phải lập luận rằng đó chính là xâm phạm DLCN.

Thứ hai, cần bổ sung khái niệm “dữ liệu hành vi” với ý nghĩa là những thông tin ghi lại mọi tương tác của người dùng trên website, ứng dụng hoặc kênh số... để đưa ra quy định chung về cơ chế thu thập, sử dụng, chia sẻ dữ liệu cá nhân nói chung và thông tin NTD trong TMĐT nói riêng. Từ đó thiết lập cơ chế pháp lý đặc thù cho theo dõi thông tin NTD và quảng cáo dựa trên hành vi.

Thứ ba, để điều chỉnh các dữ liệu hành vi, Luật BVDLCN nên bổ sung khái niệm “thông tin liên quan đến cá nhân” trong môi trường trực tuyến, bao gồm lịch sử duyệt web, cookies, lịch sử sử dụng dịch vụ... vag những thông tin có liên quan khác, để có chế độ kiểm soát chuẩn xác và hiệu quả đối với hành vi theo dõi NTD trong TMĐT.

Thứ tư, cần thiết lập các cơ chế để đảm bảo quyền của NTD được thực hiện một cách thực chất. Cụ thể, có những quy định về chuẩn minh bạch của bên xử lý dữ liệu và cơ chế để thực hiện sự “đồng ý thực chất” của NTD. Pháp luật cũng cần yêu cầu doanh nghiệp TMĐT phải thể hiện trong chính sách bảo mật công khai theo hướng tách bạch giữa việc cung cấp dịch vụ mua bán với đề nghị theo dõi thông tin khách hàng. Doanh nghiệp xử lý thông tin phải cơ chế từ chối theo dõi (opt-out) riêng để khách hàng lựa chọn, chẳng hạn cung cấp nút “Đồng ý”, “Từ chối” hoặc “Tùy chọn” rõ ràng để NTD phân biệt được khi sử dụng.

Thứ năm, nên đánh giá kỹ lưỡng và tiến tới thành lập một cơ quan bảo vệ DLCN độc lập trực

thuộc Chính phủ làm đầu mối tập trung và là nơi chịu trách nhiệm giám sát việc thực thi pháp luật bảo vệ DLCN. Cơ quan chuyên trách này cần có thẩm quyền hướng dẫn, thanh tra theo rủi ro, tiếp nhận khiếu nại nhanh, và áp dụng chế tài đủ sức răn đe đối với các vi phạm.

## 6. Kết luận

Theo dõi thông tin NTD trong TMĐT về bản chất là một chuỗi hoạt động xử lý DLCN và của các doanh nghiệp tham gia TMĐT và có liên quan, nhằm mục đích nhận diện và phân loại NTD, phục vụ cho mục tiêu tối ưu hóa hoạt động kinh doanh của doanh nghiệp. Ở một mức độ nhất định, đây là hoạt động có lợi cho cả doanh nghiệp và NTD, thúc đẩy nền kinh tế số phát triển. Song, nếu hoạt động này không được tiến hành một cách minh bạch, công khai, phù hợp với pháp luật, và có sự đồng ý của NTD, và có sự kiểm soát chặt chẽ việc chuyển dữ liệu cho bên thứ ba, sẽ tạo ra nhiều rủi ro cho NTD. Tham khảo pháp luật bảo vệ thông tin cá nhân và DLCN của Nhật bản cho thấy, về cơ bản, Việt Nam đã thiết lập được những quy định pháp luật bảo vệ DLCN của NTD, song vẫn cần được hoàn thiện theo hướng bổ sung những quy định trực tiếp về hoạt động theo dõi thông tin cá nhân NTD, về thu thập và xử lý dữ liệu hành vi cũng như cơ chế minh bạch và có sự đồng thuận thực chất của NTD để kết nối pháp luật bảo vệ NTD với pháp luật bảo vệ DLCN. Để pháp luật được thực thi hiệu quả, cũng nên cân nhắc việc thiết lập một cơ quan chuyên trách về bảo vệ DLCN để thực hiện việc giám sát việc thực thi pháp luật bảo vệ DLCN, thực hiện chức năng thanh tra và giải quyết khiếu nại, tố cáo đối với các vi phạm.

## Tài liệu tham khảo

- [1] A. D'Annunzio et al, Ad Networks and Consumer Tracking, Management Science, Vol. 66, No. 11, 2019 at <https://doi.org/10.1287/mnsc.2019.3481> (accessed on: July 25<sup>th</sup>, 2025).
- [2] Article 6, Act on the Protection of Personal Information (APPI) (The 2021 Amendment) tại <https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en> (accessed on: July 25<sup>th</sup>, 2025).
- [3] Z. Borgesius, F. J.a., Improving Privacy Protection in the Area of Behavioural Targeting, Alphen aan de Rijn, the Netherlands: Kluwer Law International, 2015.
- [4] Office of the Privacy Commissioner, Guidelines on Privacy and Online Behavioural Advertising, [https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl\\_ba\\_1112/](https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/) (accessed on: August 15<sup>th</sup>, 2025).
- [5] T. Reuter, Glossary: Online Behavioral Advertising tại: <https://uk.practicallaw.thomsonreuters.com/4-503-6290?contextData> (accessed on: August 15<sup>th</sup>, 2025).
- [6] B. Marcinkowski et al, Data-Driven Business Model Development - Insights from the Facility Management Industry, Journal of Facilities Management (2021) 19 (2): pp. 129- 49.
- [7] EU, Chapter 2 of General Data Protection Regulation (GDPR) tại <https://gdpr-info.eu/> (accessed on: July 25<sup>th</sup>, 2025).
- [8] EU, EDPB response to the European Commission on Article 15 DMA Consumer Profiling Reports, tại [https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-european-commission-article-15-dma-consumer\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-european-commission-article-15-dma-consumer_en) (accessed on: August 15<sup>th</sup>, 2025).
- [9] H. M. Quân et al, Pháp luật Liên minh châu Âu về bảo vệ dữ liệu cá nhân trong hoạt động thương mại điện tử, Tạp chí Ngân hàng, <https://tapchinganhang.gov.vn/phap-luat-lien-minh-chau-au-ve-bao-ve-du-lieu-ca-nhan-trong-hoat-dong-thuong-mai-dien-tu-16769.html> (accessed on: December 5<sup>th</sup>, 2025).
- [10] Data Protection Law in the US, <https://www.dlapiperdataprotection.com/?c=US> (accessed on: December 5<sup>th</sup>, 2025).
- [11] California Consumer Privacy Act (CCPA) sửa đổi năm 2020 và 2023.
- [12] N. T. Long et al, "Thông báo và đồng ý" trong thu thập, xử lý dữ liệu cá nhân, Tạp chí Kiểm sát Online, tại <https://kiemsat.vn/thong-bao-va-dong-y-trong-thu-thap-xu-ly-du-lieu-ca-nhan-65250.html> (accessed on: September 5<sup>th</sup>, 2025).
- [13] L. H. P. Chinh et al, 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 (accessed on: July 25<sup>th</sup>, 2025).
- [14] D. L. Phuong et al, Bảo vệ dữ liệu cá nhân trong hoạt động giao dịch thương mại điện tử: Kinh nghiệm của một số quốc gia trên thế giới và kiến nghị cho Việt Nam, Tạp chí Luật sư Việt Nam Online, <https://lsvn.vn/ba-o-ve-du-lieu-ca-nhan-trong-hoa-t-do-ng-giao-di-ch-thuong-ma-i-die-n-tu-kinh-nghie-m-cu-a-mo-t-so-quo-c-gia-tren-the-gio-i-va-kie-n-nghi-cho-vie-t-nam-1686710508-a131590.html> (accessed on: July 25<sup>th</sup>, 2025).
- [15] N. Đ. Hùng, Hướng dẫn các bước đánh giá tác động xử lý dữ liệu cá nhân, Tạp chí Luật sư Việt Nam online, <https://lsvn.vn/huong-dan-cac-buoc-danh-gia-tac-dong-xu-ly-du-lieu-ca-nhan-a162293.html> (accessed on: December 5<sup>th</sup>, 2025).
- [16] X. K. Oanh et al, 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, Tạp chí Pháp luật và Phát triển Online, <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> (accessed on: September 5<sup>th</sup>, 2025).
- [17] D. Hải, Zalo và TikTok bị phạt, dữ liệu cá nhân của người dùng sẽ xử lý ra sao? tại <https://vnexpress.net/zalo-va-tiktok-bi-phat-du-lieu-ca-nhan-cua-nguoi-dung-se-xu-ly-ra-sao-5009531.html> (accessed on: December 5<sup>th</sup>, 2025).
- [18] F. Y. Wang, Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-JAPAN GDPR Adequacy Agreement, Harvard Journal of Law & Technology, Volume 33, Number 2; Spring 2020 tại: <https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf?utm> (accessed on: November 18<sup>th</sup>, 2025).
- [19] <https://www.ppc.go.jp/en/aboutus/commission/> (accessed on: November 18<sup>th</sup>, 2025).
- [20] L. X. Tùng, Bảo vệ dữ liệu cá nhân tại Nhật Bản thông qua Đạo luật về bảo vệ thông tin cá nhân và một số khuyến nghị đối với Việt Nam, Tạp chí Nghiên cứu Lập pháp, <https://lapphap.vn/Pages/TinTuc/210586/Bao-ve-du-lieu-ca-nhan-tai-Nhat-Ban-thong-qua-dao-luat-ve-bao-ve-thong-tin-ca-nhan-va-mot-so-khuyen-nghi-doi-voi-Viet-Nam.html> (accessed on: July 25<sup>th</sup>, 2025).
- [21] Amendments to the Act on the Protection of Personal Information, tại: [https://www.aplawjapan.com/application/files/5816/3339/3524/Newsletter\\_AS\\_016.pdf?](https://www.aplawjapan.com/application/files/5816/3339/3524/Newsletter_AS_016.pdf?) (accessed on: September 5<sup>th</sup>, 2025).
- [22] Chính sách bảo vệ dữ liệu cá nhân của AEON Viet Nam tại <https://corp.aeon.com.vn/chinh-sach-cua-aeon/chinh-sach-bao-ve-du-lieu-ca-nhan/> và Chính sách bảo mật của NITORI Việt Nam tại <https://www.nitori.com.vn/vi/pages/privacy-policy> (accessed on: December 5<sup>th</sup>, 2025).