PHÁP LUẬT CHÂU ÂU VỀ CHUYỂN DỮ LIỆU CÁ NHÂN XUYÊN BIÊN GIỚI - GỢI MỞ HOÀN THIỆN PHÁP LUẬT VIỆT NAM

NGUYỄN HOÀNG DIỆU KHÁNH*

Để kiểm soát dòng chảy dữ liệu cá nhân xuyên biên giới, Việt Nam từng bước thiết lập khuôn khổ pháp lý chuyên biệt đối với hoạt động chuyển dữ liệu cá nhân xuyên biên giới. Từ năm 2023, các quy định cụ thể về chuyển dữ liệu cá nhân xuyên biên giới bắt đầu được thiết lập, và đến năm 2025, việc ban hành Luật Bảo vệ dữ liệu cá nhân cùng với nghị định hướng dẫn thi hành đã hoàn thiện khuôn khổ pháp lý, thông qua cơ chế đánh giá tác động và tăng cường trách nhiệm của các bên liên quan. Bài viết phân tích thực trạng pháp luật Việt Nam trong tương quan so sánh với pháp luật Liên minh châu Âu, qua đó, làm rõ các thách thức thực tiễn và gợi mở một số định hướng hoàn thiện pháp luật.

Từ khóa: *Dữ liệu cá nhân; xuyên biên giới; bảo vệ dữ liệu cá nhân; lưu trữ dữ liệu.*

To regulate the flow of personal data across borders, Vietnam has gradually established a specialized legal framework governing such transfers. Since 2023, specific regulations on such transfers have begun to take shape, and by 2025, the promulgation of the Law on Personal Data Protection, together with its implementing decree, has further completed the legal framework through impact assessment mechanisms and enhanced responsibilities of relevant parties. This article analyzes the current state of Vietnamese law in comparison with the European Union's legal framework, clarifying practical challenges and suggesting several directions for legal improvement.

Keywords: *Personal data; cross-border; personal data protection; data storage.*

NGÀY NHẬN: 07/12/2025 NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 20/01/2026 NGÀY DUYỆT: 13/02/2026

DOI: https://doi.org/10.59394/qlnn.361.2026.1442

1. Đặt vấn đề

Trong bối cảnh phát triển mạnh mẽ của công nghệ số và Internet, dòng chảy dữ liệu trở thành "mạch máu" của kinh tế số toàn cầu[1]. Tuy nhiên, cùng với lợi ích kinh tế, dòng chảy dữ liệu này cũng mang theo dữ liệu cá nhân, làm gia tăng nguy cơ xâm phạm quyền riêng tư, suy giảm khả năng kiểm soát của chủ thể dữ liệu. Điều này đặt ra thách thức, đó là làm sao cân bằng lợi ích kinh tế nhưng vẫn bảo đảm quyền riêng tư cá nhân, bảo đảm an ninh quốc gia và bảo vệ chủ quyền quốc gia cũng như chống lại sự giám sát từ nước ngoài. Liên minh châu Âu (EU) là một trong những khu vực đi đầu trong việc thiết lập khuôn khổ pháp lý toàn diện về bảo vệ dữ liệu cá nhân, trong đó Chương V của *Quy định chung về bảo vệ dữ liệu* (GDPR)[2] quy định các điều kiện cho việc chuyển dữ liệu cá nhân ra ngoài EU,

* *NCS của Trường Đại học Kinh tế - Luật, Đại học Quốc gia TP. Hồ Chí Minh*

trên cơ sở bảo đảm mức độ bảo vệ tương đương về thực chất cho chủ thể dữ liệu.

Tại Việt Nam, pháp luật về bảo vệ dữ liệu cá nhân nói chung và chuyển dữ liệu cá nhân xuyên biên giới nói riêng đã có những bước phát triển đáng kể trong thời gian gần đây. Tuy nhiên, các quy định về chuyển dữ liệu cá nhân xuyên biên giới tại Việt Nam còn tương đối mới và đặt ra nhiều thách thức trong quá trình thực thi, nhất là đối với doanh nghiệp và cơ quan quản lý.

2. Pháp luật châu Âu về chuyển dữ liệu cá nhân xuyên biên giới

2.1. Mục tiêu của châu Âu trong bảo vệ dữ liệu cá nhân

EU đóng vai trò quan trọng trong việc định hình khuôn khổ bảo vệ dữ liệu cá nhân trên phạm vi toàn cầu thông qua việc xây dựng một hệ thống pháp luật toàn diện, lấy quyền con người làm trung tâm. Tuy nhiên, việc diễn giải và thực thi bị ảnh hưởng bởi sự phán quyết của Tòa án công lý châu Âu (CJEU). Một bước ngoặt quan trọng trong tiến trình phát triển pháp luật bảo vệ dữ liệu cá nhân của EU là việc thông qua Hiệp ước Lisbon[3], quyền bảo vệ dữ liệu cá nhân lần đầu tiên được hiến định hóa, trở thành quyền cơ bản trong hệ thống pháp luật EU.

GDPR ban hành năm 2017 thay thế cho *Chỉ thị bảo vệ dữ liệu cá nhân* (DPD)[4], đã loại bỏ quyền tùy nghi của các quốc gia thành viên trong quá trình nội luật hóa quy định vào hệ thống pháp luật quốc gia. Theo GDPR, dữ liệu cá nhân được tự do lưu chuyển giữa các quốc gia thành viên EU, nơi các tiêu chuẩn bảo vệ dữ liệu thống nhất. Tuy nhiên, các vấn đề pháp lý phức tạp nảy sinh khi phát sinh nhu cầu chuyển dữ liệu cá nhân sang các quốc gia thứ ba. (Điều 44 - 50) Chương V của GDPR đưa ra các điều kiện cho việc chuyển dữ liệu cá nhân sang nước thứ ba hoặc tổ chức quốc tế. Điều 44 đặt ra nguyên tắc chung là chuyển dữ liệu cá nhân chỉ được thực hiện nếu các điều kiện của Chương V được tuân thủ và dữ liệu tiếp tục được hưởng "mức độ bảo vệ tương đương" với mức được bảo đảm trong EU.

2.2. Điều kiện về chuyển dữ liệu cá nhân xuyên biên giới theo GDPR

Trước khi áp dụng điều kiện để chuyển dữ liệu cá nhân xuyên biên giới tại Chương V GDPR, về mặt pháp lý cần làm rõ:

Một là, phạm vi áp dụng lãnh thổ, đây là một trong những điểm khác biệt quan trọng giữa GDPR và DPD. Điều 3 GDPR thiết lập hai nguyên tắc chính (1) Trường hợp bên kiểm soát dữ liệu hoặc bên xử lý dữ liệu được thành lập trong EU và (2) Trường hợp những chủ thể này không được thành lập trong EU. Theo đó, GDPR có thể được áp dụng đối với các tổ chức đặt trụ sở bên ngoài EU nếu các tổ chức này cung cấp hàng hóa hoặc dịch vụ cho các cá nhân trong EU hoặc tiến hành theo dõi hành vi của họ trong phạm vi EU. Hai án lệ nổi tiếng Google Spain (2014)[5] và Weltimmo (2015)[6] đã đưa ra những giải thích quan trọng về khái niệm "thành lập". Các phán quyết này đã góp phần mở rộng phạm vi áp dụng của pháp luật quốc gia và thẩm quyền tài phán của các quốc gia thành viên EU đối với các hoạt động xử lý dữ liệu diễn ra ngoài lãnh thổ châu Âu.

Hai là, xác định trường hợp nào cấu thành chuyển dữ liệu cá nhân xuyên biên giới, CJEU đã giải quyết việc xác định như thế nào là "chuyển" một cách cụ thể tại một trong những án lệ đầu tiên về bảo vệ dữ liệu, đó là án lệ Lindqvist năm 2003[7]. Đến Điều 44 GDPR, chuyển dữ liệu cá nhân xuyên biên giới được hiểu là bất kỳ việc chuyển dữ liệu cá nhân nào (đang được xử lý hoặc dự kiến sẽ được xử lý sau khi chuyển) sang một quốc gia thứ ba hoặc một tổ chức quốc tế. Tuy nhiên, tương tự như DPD, GDPR không đưa ra định nghĩa trực tiếp về thế nào là "chuyển dữ liệu quốc tế", thế nào là "quốc gia thứ ba".

Sau khi xác định phạm vi áp dụng; trường hợp cấu thành chuyển dữ liệu cá nhân xuyên biên giới, các điều kiện cụ thể tại Chương V sẽ được áp dụng. Theo đó, pháp luật EU phân biệt giữa các hoạt động chuyển dữ liệu mang

tính hệ thống, thường xuyên và các hoạt động chuyển dữ liệu mang tính ngẫu nhiên, không lặp lại. Các cơ chế này vốn đã được đặt nền móng từ Điều 25 và Điều 26 DPD và tiếp tục được phát triển, hoàn thiện dưới khuôn khổ của GDPR, bao gồm:

(1) Việc chuyển dữ liệu cá nhân có thể diễn ra không có giới hạn chỉ khi quốc gia, vùng lãnh thổ hoặc tổ chức quốc tế bảo đảm mức độ bảo vệ dữ liệu cá nhân ở mức "đầy đủ" thông qua Quyết định về tính đầy đủ trong bảo vệ dữ liệu cá nhân.

(2) Việc chuyển dữ liệu ra khỏi EU là được cho phép nếu bên chuyển dữ liệu áp dụng các biện pháp bảo vệ phù hợp, được phát triển theo DPD nhằm "bù đắp cho việc thiếu vắng bảo vệ dữ liệu" ở các quốc gia dữ liệu được chuyển đến, bao gồm một công cụ ràng buộc pháp lý và có hiệu lực thi hành giữa các cơ quan công quyền: (1) Các điều khoản hợp đồng mẫu (SCC) là các điều khoản mẫu được phê chuẩn trước bởi Ủy ban châu Âu (EC) thông qua một quy trình kiểm tra luật định hoặc được DPA của một quốc gia thành viên EU thông qua để bảo vệ dữ liệu. (2) Quy định ràng buộc (BCR) được phê duyệt bởi DPA, là các chính sách bảo vệ dữ liệu cá nhân được các công ty thành lập ở EU tuân thủ để chuyển dữ liệu cá nhân ra bên ngoài EU trong một nhóm các công ty trong cùng hoạt động kinh doanh cam kết. (3) So với DPD, GDPR cũng đưa ra hai biện pháp bảo vệ thích hợp mới cho việc chuyển dữ liệu cá nhân, đó là Quy tắc ứng xử (COC) và cơ chế Chứng nhận. Ngoài ra, dữ liệu cá nhân cũng được chuyển ra khỏi EU trong trường hợp có công cụ pháp lý ràng buộc có hiệu lực thi hành giữa các cơ quan công quyền ở EU và các nước thứ ba.

(3) Trong trường hợp không thể dựa vào một quyết định công nhận mức độ bảo vệ đầy đủ và việc thiết lập các biện pháp bảo đảm thích hợp là không khả thi, việc chuyển dữ liệu cá nhân ra khỏi EU có thể được thực hiện trên cơ sở một trong các ngoại lệ được quy định tại khoản 1 Điều 49 GDPR. Tuy nhiên, đây chỉ là cơ chế mang tính ngoại lệ và tạm thời, vì các ngoại lệ này không cung cấp bất kỳ cơ chế bảo vệ bổ sung nào cho cá nhân có dữ liệu được chuyển giao.

2.3. Án lệ Schrems I, II

Việc áp dụng các quy định của GDPR trên thực tế không thể tách rời vai trò giải thích của CJEU. Các án lệ Schrems I và Schrems II[8] đã trở thành những mốc then chốt, không chỉ làm rõ nội hàm của cơ chế chuyển dữ liệu xuyên biên giới mà còn tái định hình cách hiểu về tiêu chuẩn "mức độ bảo vệ tương đương" và trách nhiệm của các chủ thể tham gia chuyển dữ liệu cá nhân xuyên biên giới. Cả hai phán quyết đều thể hiện sự không hài lòng của châu Âu đối với các thực tiễn giám sát ngoại quốc của Hoa Kỳ được tiết lộ qua Edward Snowden[9].

Chẳng hạn khi tòa án tuyên Safe Habour[10] vô hiệu năm 2015 tại Schrems I, các công ty thực hiện chuyển dữ liệu từ EU sang Mỹ căn cứ vào Safe Habour bỗng nhiên bị mất đi căn cứ hợp lệ cho việc chuyển dữ liệu cá nhân ra khỏi EU. Trước tình huống này, Nhóm công tác Điều 29 và EC đã đưa ra hướng dẫn riêng cho các doanh nghiệp về cách để vẫn có thể chuyển dữ liệu sang Hoa Kỳ. Theo Schrems I, công cụ chuyển dữ liệu cá nhân SCC vẫn có hiệu lực. Vì vậy, EC phải thỏa thuận với các công ty nói trên, cho phép 3 tháng thời gian ân hạn, theo đó EC sẽ không truy cứu hay xử phạt và các công ty phải sử dụng khoản thời gian này để thực hiện các chính sách tuân thủ bổ sung. EC cũng phải thực hiện đàm phán một thỏa thuận mới với chính quyền Mỹ, trở thành Privacy Shield[11] sau này.

Sau khi Safe Harbor vô hiệu, Facebook dựa vào SCC để chuyển dữ liệu từ EU tới Hoa Kỳ, vì vậy Max Schrems đã thay đổi khiếu nại của mình và toàn bộ quá trình khiếu kiện bắt đầu lại. Cụ thể, vào cuối năm 2015, Maximillian Schrems tiếp tục thách thức việc Facebook sử dụng SCC để chuyển dữ liệu cá nhân của công dân EU sang Hoa Kỳ với lập luận rằng cơ chế này không bảo đảm đầy đủ

các quyền của chủ thể dữ liệu EU. Theo Schrems, việc chuyển dữ liệu như vậy vi phạm GDPR và rộng hơn là pháp luật EU về bảo vệ dữ liệu cá nhân. Theo đó, thuôn khổ EU - Hoa Kỳ Privacy Shield đã bị CJEU tuyên vô hiệu trong phán quyết Schrems II năm 2020. CJEU đã kết luận, Privacy Shield không bảo đảm mức độ bảo vệ "về cơ bản tương đương" đối với dữ liệu cá nhân được chuyển nhượng sang Hoa Kỳ vì không thể khắc phục được sự thiếu hụt các hạn chế và biện pháp bảo vệ cần thiết trong luật pháp Hoa Kỳ đối với sự can thiệp do quyền tiếp cận dữ liệu cá nhân của các cơ quan giám sát Hoa Kỳ trong bối cảnh an ninh quốc gia và bảo vệ pháp lý hiệu quả đối với những sự can thiệp đó.

3. Gợi mở cho Việt Nam

Với mục tiêu chuyển đổi số, Việt Nam đang xây dựng một khuôn khổ pháp lý toàn diện và chuyên biệt hơn cho việc bảo vệ dữ liệu cá nhân. Khung pháp lý của Việt Nam đối với hoạt động chuyển dữ liệu cá nhân xuyên biên giới được định hình rõ nét thông qua Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ sau đó được kế thừa, luật hóa và nâng cấp trong *Luật Bảo vệ dữ liệu cá nhân* năm 2025 và Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành *Luật Bảo vệ dữ liệu cá nhân* năm 2025 có hiệu lực từ ngày 01/01/2026.

Về phạm vi áp dụng, dữ liệu cá nhân được bảo vệ là các dữ liệu cá nhân trên môi trường điện tử, là dữ liệu số và cả dữ liệu được xử lý trên môi trường vật lý. Quy định về phạm vi áp dụng tại Điều 1 *Luật Bảo vệ dữ liệu cá nhân* năm 2025 cho thấy, sự kết hợp giữa nguyên tắc lãnh thổ truyền thống và bước đầu thừa nhận hiệu lực ngoài lãnh thổ của pháp luật bảo vệ dữ liệu. *Luật* đã mở rộng sang các chủ thể nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động xử lý dữ liệu cá nhân của công dân Việt Nam. Khác với GDPR, phạm vi áp dụng được xây dựng dựa trên bản thân hoạt động xử lý dữ liệu và mối liên hệ thực tế với cá nhân tại EU, không phụ thuộc vào quốc tịch: phạm vi áp dụng quy định tại *Luật Bảo vệ dữ liệu cá nhân* năm 2025 vẫn được xác lập chủ yếu dựa trên quốc tịch, tình trạng cư trú và điều kiện hành chính của chủ thể dữ liệu.

Về xác định cấu thành hoạt động chuyển dữ liệu cá nhân xuyên biên giới. Theo *Luật Bảo vệ dữ liệu cá nhân* năm 2025, các trường hợp được coi là "chuyển dữ liệu cá nhân xuyên biên giới" được quy định tại khoản 1 Điều 20. So với GDPR, quy định của Việt Nam có phạm vi bao quát tương đối rộng khi điều chỉnh không chỉ việc "chuyển" dữ liệu theo nghĩa truyền thống mà cả trường hợp dữ liệu cá nhân được xử lý trên nền tảng đặt ở nước ngoài, dù dữ liệu không bị chuyển giao vật lý. Cách tiếp cận này phản ánh xu hướng quản lý chặt chẽ hơn đối với hoạt động xử lý dữ liệu cá nhân liên quan đến chủ thể dữ liệu trong nước trong bối cảnh kinh tế số.

Về điều kiện chuyển dữ liệu cá nhân xuyên biên giới, *Luật Bảo vệ dữ liệu cá nhân* năm 2025 xác định nghĩa vụ lập hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới của bên chuyển dữ liệu là yêu cầu trung tâm trong mô hình quản lý. Vai trò của cơ quan chuyên trách bảo vệ dữ liệu cá nhân trong việc đánh giá hồ sơ cũng được trao quyền rõ trong việc đánh giá và kết luận hồ sơ đạt hoặc không đạt yêu cầu trong thời hạn nhất định, yêu cầu hoàn thiện hồ sơ khi cần thiết cũng như áp dụng các biện pháp xử lý trong trường hợp không tuân thủ. Điều này cho thấy, mô hình quản lý của Việt Nam đã dịch chuyển từ hậu kiểm thuần túy sang cơ chế kiểm soát chặt chẽ hơn, kết hợp giữa nghĩa vụ đánh giá bắt buộc và yếu tố tiền kiểm có điều kiện.

Khung pháp lý về chuyển dữ liệu cá nhân xuyên biên giới của EU và Việt Nam mặc dù cùng hướng tới các mục tiêu chung như bảo vệ quyền con người, quyền riêng tư cá nhân và lợi ích kinh tế, song hai hệ thống pháp luật có sự khác biệt rõ rệt.

Thứ nhất, pháp luật EU mà trung tâm là GDPR được xây dựng trên quan điểm xem bảo vệ dữ liệu cá nhân là một quyền cơ bản của con người, nhấn mạnh quyền tự chủ và quyền kiểm soát thông tin của cá nhân. Trong khi đó, pháp luật Việt Nam tuy ngày càng chú trọng bảo vệ quyền riêng tư và quyền của chủ thể dữ liệu nhưng vẫn đặt trọng tâm lớn vào các mục tiêu bảo vệ an ninh quốc gia, chủ quyền dữ liệu và quản lý nhà nước đối với không gian số với mức độ can thiệp tương đối sâu của cơ quan nhà nước vào hoạt động xử lý và chuyển dữ liệu.

Thứ hai, EU áp dụng mô hình đa tầng cho điều kiện chuyển dữ liệu cá nhân xuyên biên giới. Ngược lại, Việt Nam vẫn chưa cung cấp các tiêu chí pháp lý rõ ràng để đánh giá mức độ bảo vệ tương đương tại quốc gia tiếp nhận cũng như chưa hình thành các công cụ chuyển dữ liệu mang tính chuẩn hóa. Pháp luật Việt Nam áp dụng mô hình tiền kiểm có điều kiện, thông qua hồ sơ đánh giá tác động.

Trên cơ sở các kết quả phân tích, một số định hướng nhằm hoàn thiện pháp luật Việt Nam về chuyển dữ liệu cá nhân xuyên biên giới được gợi mở cho Việt Nam như sau: (1) Nghiên cứu xây dựng và ban hành bộ điều khoản hợp đồng chuẩn phù hợp, do cơ quan có thẩm quyền ban hành hoặc phê duyệt, nhằm tạo công cụ pháp lý thống nhất cho hoạt động chuyển dữ liệu. (2) Khuyến khích các tập đoàn đa quốc gia hoạt động tại Việt Nam xây dựng và đăng ký các quy tắc nội bộ ràng buộc để điều chỉnh việc chuyển dữ liệu cá nhân trong cùng một nhóm công ty, đặc biệt trong bối cảnh dữ liệu được chuyển đến các chi nhánh ở nước ngoài.

4. Kết luận

Phân tích so sánh khung pháp lý bảo vệ dữ liệu cá nhân của Việt Nam và EU cho thấy, sự khác biệt rõ nét về triết lý, mức độ hoàn thiện cũng như cơ chế thực thi. Để hướng tới một hệ thống bảo vệ dữ liệu hiệu quả, Việt Nam cần tiếp tục học hỏi kinh nghiệm của EU trong bảo vệ quyền lợi của chủ thể dữ liệu trong bối cảnh toàn cầu hóa và chuyển dữ liệu cá nhân xuyên biên giới ngày càng phổ biến. Việc hoàn thiện này không chỉ giúp bảo đảm quyền riêng tư cá nhân mà còn góp phần tạo dựng niềm tin, thúc đẩy phát triển kinh tế số bền vững và hội nhập quốc tế sâu rộng hơn❐

Chú thích:

1. Francesca Casalini & Javier Lopez-Gonzalez (2019). *Trade and cross-border data flows.* OECD Trade Policy Papers, Số 220, OECD Publishing, Paris, tr. 8, 2019, (PDF) Trade and Cross-Border Data Flows.

2. Regulation (EU). 2016/679 *General Data Protection Regulation.* 2016 OJ L119/1.

3. *Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C 306/1*, có hiệu lực ngày 01/12/2009.

4. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995]* OJ L 281/31.

5. *Case C-131/12, Google Spain SL v. Agencía Española de Protección de Datos (AEPD),* 2014 E.C.R. 317.

6. Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, 2015 E.C.R. 639.

7. Case C-101/01. *Criminal proceedings against Bodil Lindqvist,* EU:C:2003:596. CJEU.

8. Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18) EU:C:2020:559.

9. T*he Schrems II judgment of the Court of Justice and the future of data transfer regulation.* https://www.europeanlawblog.eu, truy cập ngày 18/12/2025.

10. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

11. *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided* by the EU–US Privacy Shield [2016] OJ L 207/1.